BIC / BUSINESS INFORMATION COALITION

B2B MARKETING & DATA PROTECTION COMPLIANCE IN EUROPE

A Practical Guide from
the Business Information Coalition

Version 1: 2023
Version 2: 2025

TABLE OF CONTENTS

01.
EXECUTIVE SUMMARY

Six key guidelines to help you comply

1. Think about the expectations of the recipient
2. Be clear and transparent
3. Apply GDPR and national ePrivacy laws: consent or opt-out
4. Enable compliance with easy to use preference tools and great customer service
5. Use data governance and data quality to support compliance
6. Ask the right questions when you buy personal data

Key Messages

- ☐ Business 2 Business (B2B) marketing enables businesses to grow and extend into new markets.
- ☐ Personal data is any information that relates to an individual, directly or indirectly.
- ☐ Personal data is used during B2B marketing and this means B2B marketing must comply with two laws in Europe:
    - ☐ The General Data Protection Regulation (GDPR) and
    - ☐ Country-specific ePrivacy law that covers direct marketing, including email, phone and text. It is important to understand the laws in each country you want to market in.
- ☐ It is feasible to undertake compliant B2B marketing in Europe. Use the six key messages to help design your compliance program.
- ☐ It is important to recognise the low risk profile of the personal data generally used in B2B. There are also steps you can take to ensure the risk remains low.

  You don't always need consent for B2B marketing:
    - ☐ In some countries you can rely on a lawful basis under GDPR called legitimate interests and offer an opt out.
    - ☐ You may need to rely on consent in some countries and this consent must meet the standard in the General Data Protection Regulation.
- ☐ There may be different rules for email, text, and phone marketing.
- ☐ You must put processes in place to promptly respond to requests from people who want to exercise their rights under GDPR.

02.
INTRODUCTION

How B2B marketing helps businesses grow, personalise communications and reach into new markets

B2B marketing is an essential operation that helps businesses grow, identify, engage and sell to new corporate customers.

B2B marketing needs to reach professionals with a range of roles in a company - all ultimately related to building influence, reaching decision makers and closing deals. B2B marketing can be delivered via multiple channels - email, text, phone, website or social media, as well as offline methods such as postal marketing. The most common mechanism is email but an effective strategy will often use many channels in combination.

Data is integral to the planning, execution and measurement of B2B marketing. This data will include personal data - information about professionals, such as contact details and enriched profiles - to help guide the marketing process. The growth of the internet and digital technologies means that there is more information about customers than ever before.

Companies using B2B marketing will collect their own data and maintain Customer Relationship Management (CRM) systems but will often also seek to use third-party data services to enrich their data.

This Guidance is not a comprehensive guide to all aspects of general data protection compliance. It is focused on the specific compliance implications for B2B marketing. We have included some links to general guidance at the end of the document.

What the Guidance covers and how it can help

B2B data is focused on professional activity and should present a low risk in terms of privacy intrusion and the expectations of the people the data is about. But B2B data is still about people and must be managed with care and diligence to ensure trust, confidence and compliance.

This guidance document (the Guidance) has been developed to help businesses engage in B2B marketing that complies with European data protection and ePrivacy laws.

There can be misunderstandings about the risks of using personal data for B2B marketing in Europe. It can also appear daunting when first planning the steps needed.

This Guidance has a key message—businesses **can** undertake compliant B2B marketing in Europe, including use of third-party data services.

This document takes you through the practical steps to compliance. It covers the requirements that apply across the EU under the General Data Protection Regulation (GDPR) and the additional requirements on direct marketing that are set out in national ePrivacy laws. It guides you through general principles to specific scenarios.

The Guidance is underpinned by six key messages set out below. They highlight the foundational considerations that should underpin your compliance approach for B2B marketing in Europe. It also reinforces how good compliance and data governance go hand-in-hand with trust and confidence in B2B marketing.

Who is the Guidance for?

This Guidance is for any business undertaking B2B marketing in Europe, particularly those planning to use third-party data services.

The Guidance will particularly help people in the following roles:

- Procurement teams assessing third-party data services that will be used for B2B marketing.
- B2B third-party data services discussing European law and regulation with current and prospective customers.
- Chief Privacy Officers and Data Protection Officers.
- Chief Marketing Officers.

This Guidance does not constitute formal legal advice and businesses should always make their own assessment of legal compliance and seek their own specific legal advice when needed.

What countries does the Guidance cover?

The Guidance considers all 27 European Union (EU) Member States, plus the three European Economic Area (EEA) countries: Norway, Liechtenstein and Iceland. It also includes Switzerland as they are part of the EU single market, and the UK given its previous EU membership. The Guidance uses a collective term 'European countries' to describe the overall group.

How the Guidance was developed

The Guidance was developed during 2022, with the input and support of members of the Business Information Coalition ("BIC").

The development of the Guidance was led by Steve Wood, Director of PrivacyX Consulting and former Deputy Commissioner at the Information Commissioner's Office (the Data Protection regulator for the UK).

The Guidance will be reviewed regularly and the BIC welcomes feedback about the content.

The Guidance was reviewed and updated in February 2025, following consultation with BIC Members. The updates to the guidance include new content about AI, new FAQs, a new checklist, recent enforcement cases, and expanded worked examples. The guidance also now contains some additional information about compliance in Canada and Australia, though the core focus remains on Europe.

A companion training slide deck was also developed in February 2025 and is available to use alongside the guidance. Please contact BIC for a copy.

About the Business Information Coalition

The Business Information Coalition ("BIC") is a coalition of like-minded, B2B companies focused on making sure that business contact information is treated fairly by regulators.

The BIC gives companies that promote business information a collective voice and facilitates the pooling of intelligence and resources among its members, making it a low-cost yet effective advocacy tool for businesses of all sizes.

The BIC recognizes that business information is non-sensitive in nature and fundamental to the economy at-large and B2B commerce, and recognizes that the right to research, process, analyse, use, and transfer non-private business information should not be infringed or unduly burdened.

BIC members are listed in Annex D below.

03.
B2B MARKETING COMPLIANCE: KEY GUIDELINES

These messages help reinforce the positive case for compliance and how to enable trust and confidence in the B2B marketing you undertake in Europe.

Companies should plan compliance 'by design'. Think about these six key messages when developing your marketing strategy, system design or procuring third-party services. They can also support conversations with peers and managers about compliance and risk.

01. **Think about the expectations of the recipient**

02. **Be clear and transparent**

03. **Apply GDPR and national ePrivacy laws: onsent or opt-out**

04. **Enable compliance with easy to use preference tools & great customer service**

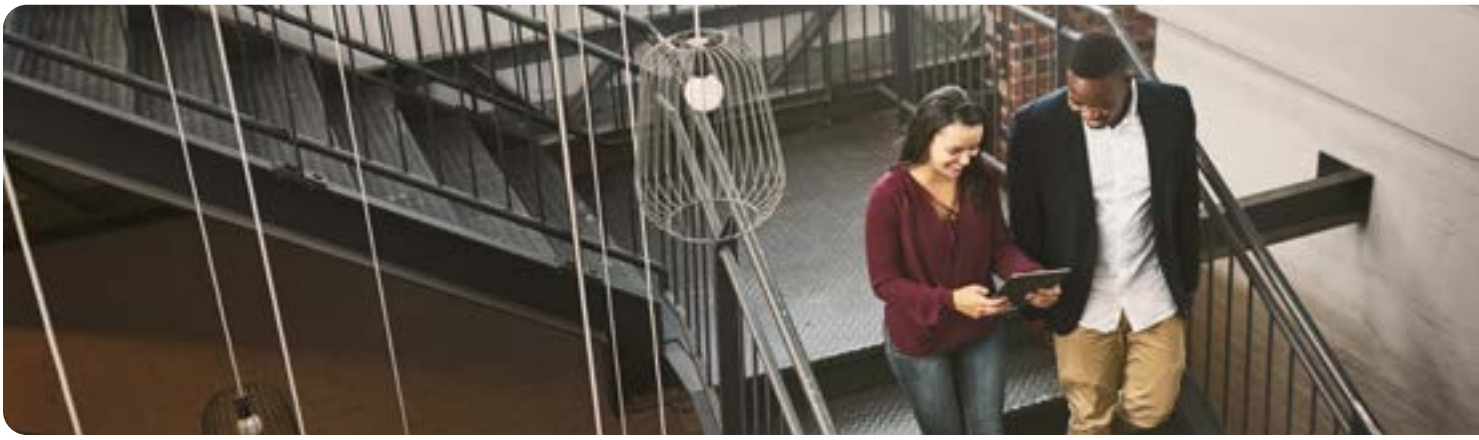
05. **Use data governance and data quality to support compliance**

06. **Ask the right questions when you buy personal data**

04.

DATA PROTECTION AND EPRIVACY LAW:

THE LEGAL FRAMEWORKS REGULATING B2B MARKETING ACROSS EUROPE



When undertaking B2B marketing in Europe companies need to comply with **two different pieces of legislation**.

(1) You need to comply with general data protection law. For most European countries this is called the **General Data Protection Regulation (GDPR)**. This law covers principles and rights related to personal data. If you are using personal data you need to comply. Countries in Europe, but not in the EU, also have similar laws.

(2) In addition, EU countries also have specific laws covering direct marketing. In the EU, the **2002 ePrivacy Directive** requires member states to have a law in place that covers B2B marketing, but leaves them some discretion on the wording and implementation of their national law. This has created the situation where specific requirements differ between countries. The Guidance helps you navigate this. Countries in Europe, but not in the EU, have similar laws.

You will need to demonstrate compliance with both laws and people can complain about use of their personal data under either or both laws.

05.
GDPR OVERVIEW

EU GDPR and UK GDPR Background

The General Data Protection Regulation (GDPR) applies across all 27 EU member states. It is designed to harmonize EU law on data protection. It came into full effect in 2018. The EU has a long-standing culture of data protection and has had data protection law for over 25 years.

The UK also retained GDPR as UK law (with some minor changes), when it completed its full exit from the EU in 2020. The other non-EU countries covered by this Guidance also have laws that replicate or are close to GDPR.

At the time of updating this Guidance (February 2025) a proposed UK Data Protection Bill was before the UK Parliament, but not passed into law. None of the proposed changes will significantly impact B2B marketing. Please check the UK Government website to follow progress. The bill is likely to pass later in 2025.

Switzerland, Liechtenstein, Norway and Iceland also have laws that closely follow the GDPR.

The GDPR aims to both enable use and protect personal data, and has been designed for a digital connected economy and society. It enables people to be informed about what happens to their data and exercise their rights over it, unless a legitimate exception applies. The GDPR also aims to create trust and confidence in how personal data is used, which can enable and support business growth. As a result, GDPR provides the conditions for businesses to use data, as well as what can't be done.

GDPR refers to the use of personal data as **processing**.

The principles in Article 5 GDPR are the cornerstones of compliance. Companies should think about how these principles relate to good data governance. For example, effective B2B marketing must be supported by accurate data and removal of data when it is no longer needed. We explain in more detail below (in Section 6) how they apply to direct marketing.

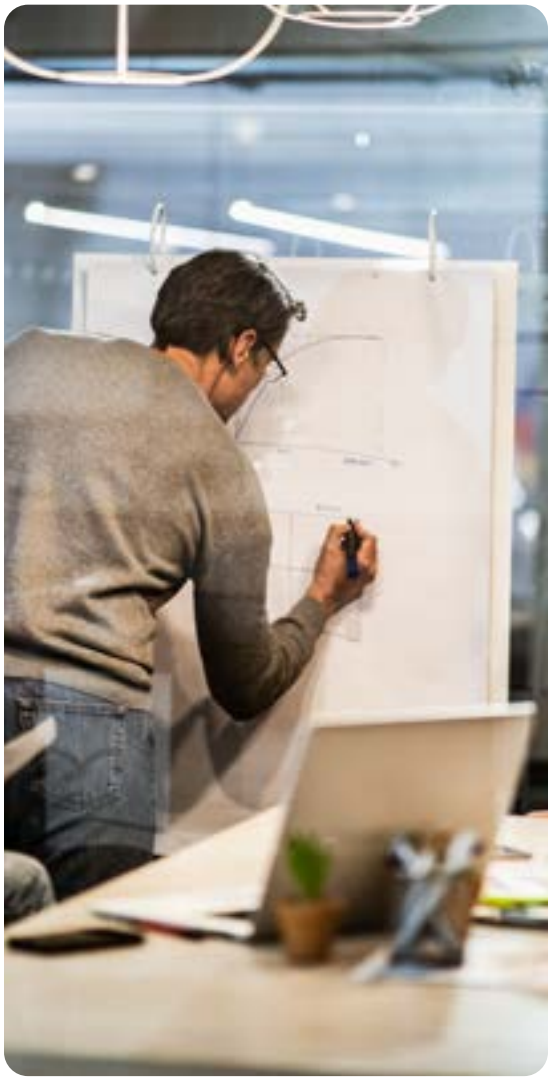
A controller processing personal data must have a lawful basis under GDPR. There are six listed under Article 6. The most likely bases for a commercial company undertaking B2B marketing are legitimate interests or consent. We discuss further below and how this must interact consistently with the ePrivacy laws that exist at national level on direct marketing.

Personal data, such as health information, race and sexuality, is defined as special category data. There are further requirements and conditions to process this data and the most relevant condition is explicit consent. The risks related to non compliance are also higher. It is recommended that special category data is not used in B2B marketing.

Territorial scope

The GDPR will apply if your business is established in the EU (or UK). It will also apply if your business is based outside the EU (or UK) if your personal data processing *'relates to the offering of goods or services to those individuals or to the monitoring of data subjects' behaviour'*.

A transaction or payment does not have to take place for it to relate to the offering of goods or services.



Controller and processor

The GDPR assigns responsibilities for compliance. A **controller** has the responsibility for demonstrating compliance with GDPR.

A **controller** makes the decisions about purposes for using personal data and how this happens.

A **processor** is acting under the instructions of the **controller** in how personal data is processed. A processor must provide guarantees to the controller that the personal data will be protected and only usedin accordance with GDPR.

A **processor** may also use a **sub-processor**, if a contract is also put in place.

The relationships between each entity must be governed by a contract or another form of binding agreement. The European Commission has produced standard contract terms for controller-processor, that can be used and added to a broader contract.

This can be important in B2B marketing as businesses often use the services of third parties. Here are a few examples to illustrate the roles:

B2B example

Scenario 1. Single controller. ABC company gathers personal data about existing and prospective customers in its own CRM system. It gathers this information from its sales reps and conferences it hosts itself, and uses this to target B2B marketing. It does not buy any personal data. ABC Company is a controller.

Scenario 2. Two separate controllers. Company XYZ gathers its own personal data and also buys personal data from a third-party vendor, Company 123. It combines all of the data for B2B marketing. Company XYZ is a controller for the combined data set. Company 123 is a separate controller for the personal data in its own data set. They both have to demonstrate their compliance with the GDPR.

Scenario 3. Controller - processor. Company ABC uses a third-party service, Company 456, to manage its digital B2B marketing communications, including email automation and controls for marketing preferences. Company ABC loads some of its personal data into Company 456's systems to enable emails to be sent. ABC makes the decisions about when to send information and how it is managed on the system. Company ABC is a controller, Company 456 is a processor.

Accountability under GDPR

Controllers must also demonstrate accountability in their compliance with GDPR. A number of provisions in the GDPR require controllers to do this - for example, completing a data protection impact assessment for high risk processing or implementing a data protection by design process. The GDPR also requires records of processing to be kept.

Whilst not a formal requirement, investing in privacy management programs, involving training and awareness, can also embed good accountability practice throughout the company. Companies should consider what accountability measures work best for their business.

You can take a risk based approach to accountability. For B2B marketing this means you can evidence the level of privacy intrusion or data harm that the activity represents, evidenced by the professional and public focus of the data collected. This must be done in your specific circumstances. This should enable a proportionate approach to compliance and if the risk profile is kept low a data protection impact assessment need not be required for B2B marketing.

Transfers of personal data to third countries

If personal data is transferred to a third country (outside the EU, UK or other European country) controllers must consider whether adequate protection is provided for the data. This is most straightforward when the EU or UK have deemed that third country adequate. For example, Japan is deemed adequate. Personal data can be transferred to such countries with no additional safeguards. You can find a list of the countries who have been deemed adequate on the European Commission website.

For other third countries, for example Australia and India, no such decisions are in place. The controller must then implement safeguards to ensure the protections for the personal data are 'essentially equivalent' in the third country. The most common safeguard is a set of 'standard contractual clauses' (SCCs) - between the controller and the importing entity in the third country. The European Commission has published SCCs on its website, as has the Information Commissioner's Office in the UK.

The so-called 'Schrems II' ruling by the Court of Justice in the EU (2020) has also clarified the additional protections controllers must use when using safeguards such as SCCs. The Court's judgment found that the controller must also assess the impact of national security and law enforcement bodies accessing data when transferred to the third country importer. The ruling also struck down the EU-US Privacy Shield, which enabled free flows of personal data between EU and US companies who signed up to the Shield.

Undertaking such as an assessment can be burdensome, but for B2B data it is important to recognize the lower risk profile of the data and whether the receiving entity is likely to be subject to national security or law enforcement access. There is further guidance available from the European Data Protection Board and on Data Protection Authority websites.

In July 2023, a new EU Adequacy decision was issued on the EU - US Data Privacy Framework. allowing companies under the Framework to transfer personal data from the EU to the US. Protections related to national security and law enforcement access to personal data in the US have also extended to cover companies using SCCs as well. Companies should continue to monitor this area as further legal challenges are possible. The UK Government has also issued a decision recognizing the Data Privacy framework.

Localization options

The legal uncertainty and compliance requirements for data transfers under GDPR have led some companies to consider the benefits of localizing data within the EU. This is **not** a requirement of the law but a solution some have sought to the challenges.

For example, some multinational companies with establishments in the EU and other third countries have chosen to have EU servers, rather than store data in the other servers operated by the company. Companies are also seeking to use processors in the EU as well, to avoid challenges. For example, selecting EU based cloud services or hosted e-marketing services. This is a decision based on balancing costs, legal risk and other business planning considerations.

> **HOWEVER, EVEN IF LARGE SCALE SANCTIONS ARE LESS LIKELY FOR B2B MARKETING YOU SHOULD CONSIDER THE RISK OF REPUTATIONAL DAMAGE FROM ANY ACTION, INCLUDING RELATED TO INDIVIDUAL COMPLAINTS.**

GDPR Enforcement

The GDPR is enforced by independent data protection authorities (DPAs) in each country. They have the power to fine up to 10M euro or 2% of worldwide annual turnover for lower-level infringement and up to 20M euro or 4% for the more serious level. DPAs can also issue orders that can stop controllers processing personal data. Individuals can also submit complaints.

Whilst there have been fines of several hundred million Euros for large multinational companies since GDPR commenced there have been very few cases of action being taken for B2B marketing. DPAs are bound to consider the levels of risk and harm before issuing a sanction and the risk profile of B2B data will be relevant to this.

However, even if large-scale sanctions are less likely for B2B marketing you should consider the risk of reputational damage from any action, including related to individual complaints.

In France, the data protection authority (the CNIL) fined FORIOU 310,000 euros for using data supplied by data brokers for commercial prospecting purposes, without making sure the individuals concerned had given their valid consent (2024).

In Belgium the Data Protection Authority fined a B2B data broker €20,000 for unlawfully collecting and disclosing a data subject's email address, and other GDPR infringements. In particular, the DPA held that the processing was not justified by the controller's legitimate interest under GDPR (2025).

Most DPAs provide guidance on their websites about compliance and we have included some examples below.

06.

GDPR AND B2B MARKETING IN PRACTICE

GDPR: defining personal data in B2B marketing

Personal data is any information that relates to an individual, directly or indirectly. For example, a name identifies someone directly, a national identity number can be used to identify someone indirectly.

There is no distinction made between whether the information is publicly available or not. If you collect information about people from a public source like a website, this is still personal data.

General business information about a company you engage with (or want to) is not personal data, unless that business is a sole trader (a one-person business that is not incorporated).

If you are sending B2B marketing communications to an email address that does not relate to a person, then GDPR won't apply. E.g to sales@ABCcompany.com

What types of personal data are likely to be used in B2B marketing?

Considering the current industry practice, the following are regularly used for GDPR compliant B2B marketing:

- ☐ Name
- ☐ Current employer
- ☐ Role or title
- ☐ Department
- ☐ CV information
  Such as: **I.** *Employment history,* **II.** *Education history,* **III.** *Professional certifications,* **IV.** *Publications*
- ☐ Business email
- ☐ Business HQ address
- ☐ Office address
- ☐ Direct business phone
- ☐ Business mobile phone
- ☐ Business related social media
- ☐ IP address, collected when individual users visit websites or apps

Companies undertaking B2B marketing are also likely to maintain a 'free text' notes field to record additional information about their interaction with individuals and the individual's interests. This information is also likely to be personal data if related to the individual. The recommended approach is therefore to treat all such records as personal data.

Much of this information is publicly available or can be found on other sources such as business cards. While this cannot immediately validate GDPR compliance, it is important to note that the risk profile is likely to be low. The information should not significantly intrude on privacy. This lower risk can be used to guide B2B compliance and a more straightforward use of resources to comply.

Businesses should seek to implement policies and guidelines for staff who collect, procure or use personal data, to ensure that the data retains a low risk profile.

GDPR and the data lifecycle

The requirements of GDPR can all relate to the data lifecycles that most digital businesses will follow:

- Generation
- Collection
- Processing
- Storage
- Management
- Analysis
- Visualization
- Interpretation

GDPR principles

There are six principles in Article 15 of the GDPR, plus an overarching principle of accountability. You must demonstrate compliance against all of them unless an exemption applies. It is very unlikely an exemption will be relevant for B2B activity. We cover the most relevant principles to B2B in the sections below.

1. Fair, lawful and transparent
2. Purpose limitation - do not re-use in a manner that is incompatible with the original purpose
3. Data minimization
4. Accurate and up to date
5. Storage limitation
6. Appropriate security - integrity and confidentiality
7. Accountability

Fairness and data minimization principles in B2B marketing

The first principle in the GDPR states that personal data must be processed lawfully, fairly and transparently. We will deal with lawfulness and transparency later in the guide.

Fairness is an important concept to consider related to B2B marketing and helps you focus on the expectations of individuals. It helps you manage risk. The concept helps you to think about the perspective of the individual and step into their shoes.

Personal data may be collected from many sources: automated collection from websites, surveys, conference information and press releases. The data above can also be procured from third-party services. You must be able to justify the personal data collection as necessary and proportionate to your business purpose and meet the data minimization principle.

You must have checks and questions built into your processes to assess this. Excessive personal data collection will infringe GDPR. You should also ensure automated or manual scraping from websites and apps complies with the terms and conditions applicable to the service. Collecting in breach of these terms is likely to be unfair, as well as unlawful.

When thinking about fairness and B2B marketing the most crucial aspect is likely to be the types of data you hold and the level of intrusiveness posed.

Is your B2B data processing within the reasonable expectations of the individual?

If the personal data you hold stays focused on professional information that is commonly known or could be found publicly, you can be more confident it's use can stay within their expectations.

You must think about how your privacy notice sets expectations about how you will use their personal data. A 'no surprises' approach should guide you.

Some key issues to consider about fairness:

- ☐ Make sure you can justify profiling or inferred data as within reasonable expectations - the categories you use are based on professional activity.
- ☐ Think carefully about using additional information from outside the professional sphere e.g hobbies, personal social media accounts.

Key Message
Think about the expectations of the recipient

Spotlight on Artificial Intelligence

AI and GDPR

In the data protection context, Artificial Intelligence (AI) can be defined as 'the theory and development of computer systems able to perform tasks normally requiring human intelligence' (taken from UK ICO guidance).

The potential for AI's effective use in direct marketing is vast. Activities already using AI include those listed below:

- ☐ Audience targeting
- ☐ Lead generation
- ☐ Personalization
- ☐ Customer behavioral analysis
- ☐ Competitor insights
- ☐ Ad-tech/ Pay Per Click (PPC) advertising
- ☐ Intelligent advertising design
- ☐ Search engine optimization
- ☐ Social media listening
- ☐ Email subject line crafting
- ☐ Predictive marketing
- ☐ Chatbots
- ☐ Customer support
- ☐ Content generation
- ☐ Intelligent website audits
- ☐ Market / trend analysis
- ☐ Augmented assistance

As costs of using artificial intelligence (AI) fall, companies may also choose to use algorithms to infer that a person can be placed in a particular category of customer or other AI supported methods to improve segmentation and targeting. This process would be regarded as profiling under GDPR and the output would also be personal data. Fairness is an important principle when using inferred data. A key consideration is to ensure that inferences are related to business categorizations or professional interests and can be justified as necessary and proportionate. It may be possible to conduct such profiling under the GDPR lawful basis of legitimate interests, rather than consent.

Using AI to generate automated calls will need to comply with any laws that set specific rules for recorded calls, for example you may need specific consent from the individual to receive these calls.

Some companies may wish to use Generative AI to draft emails, other marketing communications or analyze summaries of information related to existing or potential customers. You will need to consider whether such uses of AI involve the processing of personal data – this could be in the training or fine tuning of the AI model and whether the personal data will be processed in the prompts or outputs.

The risks under GDPR of using AI for B2B are likely to be lower than for B2C marketing but you will need to consider the specific risks of your use on a case-by-case basis.

If your uses of AI for B2B m arketing involve personal data you should consider the following GDPR compliance considerations:

- Address your role as a controller or a processor under GDPR, and the contractual provisions and due diligence you may need to have in place
- Assess what personal data is necessary for your objectives – do you need to use it?
- The risks of unfairness or bias on individuals – you should consider different types of bias that could occur across the development and deployment process. For example, automation bias - where human users routinely rely on the output generated by a decision-support system and stop using their own judgement or stop questioning whether the output might be wrong.
- Compliance with the GDPR principles, in particular purpose limitation and data minimization
- Compliance with the GDPR accuracy principle - if you do use an AI system to make inferences about people, the personal data you process to train your models or their outputs must be up-to-date and remain so. You also need to ensure that the system is sufficiently statistically accurate for your purposes. (see UK ICO guidance for more detail on AI and accuracy).
- Assess whether personal data processing is high risk, and if you are required to conduct a data protection impact assessment under the GDPR
- How you may enable data subject rights such as the right to erasure in the AI system
- What due diligence you may need to undertake with third party AI providers
- What information should you provide about your use of AI, and the implications, in your privacy notice?

For more information about GDPR and AI please see the UK ICO guidance the EDPB Opinion on AI models.

In 2025 The Federation of European Data and Marketing (FEDMA) published the Ethical AI-Powered Marketing Charter. The Charter is designed to guide organizations and companies with clear and actionable standards for the responsible development and use of AI in data-driven marketing. The Charter outlines ethical principles to guide AI deployment, ensuring transparency, fairness, and accountability.

The EU AI Act

In 2024 the EU passed the Artificial Intelligence Act, a world-first in terms of a new law governing the risks of developing and deploying AI from a product safety perspective. The most stringent areas of the law, such as requirements for conformity testing, are focused on high-risk systems and it seems unlikely that any uses of AI in a B2B context will fall into this category. AI use in areas such as HR and recruitment may fall within the high-risk category.

The EU AI Act also allocates regulatory responsibilities between providers and deployers. If you are deploying an AI solution from a provider, you should consider the information they are required to make available under the transparency rules in the Act.

Other AI systems are considered low risk. These AI systems will be subject only to limited transparency obligations where they interact with individuals.

A detailed guide to compliance with the AI Act is beyond the scope of this guidance. Please see the European Commission's website for more information.

GDPR and personal data collection: Transparency Requirements

Providing privacy information is a key component for data protection law and is applicable to B2B marketing. Most businesses do this using a privacy notice.

Telling people what you will do with their personal data helps build trust and confidence in your brand and explains how you respect their data protection rights.

The requirements for transparency and privacy are set out in Articles 13 and 14 GDPR.

All B2B marketing using personal data must comply with these requirements.

Article 13 covers the requirements for when you collect information **directly** from a person. For example, a customer goes onto your website and registers to download a brochure. You should provide a privacy notice at the point of registration explaining how you will use the personal data, including for B2B purposes. You will also provide the list of other information set out in Article 13, including their rights related to the data, such as rectification and objection.

If you are sharing personal data with third parties GDPR requires you to provide details of who you are sharing the data with - you can tell people the names of organizations or the categories that they fall within; choose the option that is most meaningful or practicable.

Article 14 covers the requirements for when you receive personal data **indirectly**. For example, you procure a dataset from a third-party. You must provide a privacy notice to the individuals in the dataset within one month or at the time of your first communication. Many companies often refer to this as an 'Article 14 notification'. It is possible that someone could object about how you propose to use their data. We explain more about how to respond to these requests below.

Key things to remember about transparency and GDPR:

All B2B marketing emails should include an unsubscribe link and clear identification of the sender.

Keep your privacy information clear and simple. Make sure the key messages are prominent and easy to see. While your legal department will want to review your privacy notice, make sure your notice does not use unnecessary complex 'legal' language.

Do not confuse transparency and consent. While you may also want to seek consent for personal data processing when you provide a privacy notice, don't confuse the two. Transparency helps ensure consent is informed. But as explained below, under GDPR you may not always want to use consent as your lawful basis.

This means that you do not always need to ask the individual to consent to the privacy notice. You may wish to rely on legitimate interest as your GDPR basis for processing, if the national e-privacy regime is opt-out. You will still need to provide a privacy notice, but consent will not be necessary.

Key Message
Be clear and transparent

Purpose limitation and sharing data

This GDPR principle requires you to consider the compatibility of using personal data against the original purpose. If you are purchasing personal data the original purpose of collection, and what people were told, should be clear.

The ICO, the UK data protection regulator, sets out the following factors you can consider for compatibility:

- ☐ Any link between your original purpose and the new purpose;
- ☐ The context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;`
- ☐ The nature of the personal data e.g., is it particularly sensitive;
- ☐ The possible consequences for individuals of the new processing; and
- ☐ Whether there are appropriate safeguards - e.g. encryption or pseudonymisation.

Read the ICO guidance in more detail.

It is particularly important to think about compatibility if you are planning to share or sell data you use for B2B marketing to another third-party.

GDPR and Data Accuracy

GDPR also requires organizations to ensure personal data is accurate and up-to-date. This data quality principle is also intrinsic to wider data governance.

Here are some key points of good practice that will enable compliance with the principle.

In larger data sets, with 10,000s or 100,000s of individual records, it can be important to ensure data is accurate for B2B marketing purposes.

Names can be easily duplicated and information misdirected if they are not recorded against database rules that support a long-term approach to consistency. Companies with large databases of personal data used for B2B may create web-based systems where people can submit information for correction via forms or propose edits to records.

Make sure you have effective processes in place to manage and check data accuracy - responding to correction requests and matching and checking data when data is combined during enrichment.

Key Message
Use data governance and data quality to support compliance

GDPR and Data Retention

GDPR requires organizations to keep personal data for no longer than is necessary. But the law does not set explicit retention time periods, you have to determine the period based on your own circumstances.

Your company may want to keep personal data related to business contacts for many years. Long-term business relationships can span years and even decades. A business can retain an interest in a customer for many years as well. You should record and justify your B2B personal data retention based around your business needs. Does the time period seem reasonable? - how would you explain and justify it to someone?

It is also reasonable to take account of evidence and data about the time period that average careers last, and in certain industries.

You should also consider whether retention is related to the use and value of different data types. You may not need to keep IP address information as long as certain contact details.

On the other side of the consideration, think about the costs of data storage and risk of holding data sets for long periods.

Your business should have a personal data retention policy and schedule for categories and data types that can be consistently applied across the organization.

Good Practice
Your database or CRM should support automated deletion periods, including for different elements of the dataset.

Getting your data governance right can drive your compliance. It makes good business sense to have an effective lifecycle of personal data and only store what is necessary. Holding unnecessary data is also a cyber security risk.

Key Message
Use data governance and data quality to support compliance

On the other side of the consideration, think about the costs of data storage and risk of holding data sets for long periods.

Your business should have a personal data retention policy and schedule for categories and data types that can be consistently applied across the organization.

Securing personal data

While personal data used in B2B marketing is not the most sensitive, it is still important that you use appropriate security measures to protect it. It is also a vital business asset you want to secure. Article 32 GDPR sets out how you must scale your approach with measures according to risk.

You must consider the security of B2B through all points of its lifecycle, including when you use a third-party data processor, such as a cloud service. You must cover data security in a contract with a processor.

If you enable customers to login into your systems to update their records this could be a further risk area where security safeguards must be considered, such as authentication. Poorly secured access to update a record could also enable access to other connected systems if not effectively designed.

There is extensive guidance and support available on information security for trusted vendors. Companies with extensive personal assets should also consider validating their security against external schemes such as an ISO standard.

You will also need to report data breaches to your relevant data protection authority within 72 hours unless you can determine that it does not pose a risk to individuals. Breaches that constitute a high risk should be notified directly to the affected individuals.

Validating data: checking that B2B data you purchase are compliant

As explained earlier in the guide, companies will often use data from third-party services to enrich their datasets or use specialist targeting services.

This guide makes clear that you **can** use third-party data for B2B marketing in compliance with GDPR. This must include providing information to people in accordance with GDPR Article 14.

The third-party data you procure will often be compiled from many sources such as websites, apps, professional social networks, surveys, email contact signatures, conference attendance data and official company registration information.

Good Practice
The company providing the data should explain how the personal data supplied complies with the GDPR. They should provide you with the following information or you should ask for it.

- The steps they have taken to notify individuals under Articles 13 or 14 of GDPR, depending on whether the vendor has collected the personal data themselves or also purchased the personal data
- The types of sources they used to compile the data. They may not wish to explain in detail every source where they have a diverse set and complex set of sources, but information should be enough to give you confidence that the collection is fair and within people's expectations.
- The data governance the vendor applies to ensure accuracy and a data lifecycle approach in terms of collection, review, retention and deletion.
- If the vendor has used consent, what reassurance can they provide that they maintain records of consent?
- If they rely on legitimate interest, what reassurance can they provide about their approach and records they keep?
- Will the vendor pass on objections or other requests related to rights?

In asking these questions you also need to recognize that some aspects of the vendor's business model will be commercially confidential.

A number of data protection authorities have produced guidance about using publicly available information for marketing:

- The ICO (UK) has produced this guidance about using it for B2B marketing.
- The CNIL (France) has produced guidance on the reuse of publicly available online data for commercial canvassing purposes.

From access to deletion: Individual rights under GDPR

The GDPR also provides the following rights, to enable individuals to control and manage their data:

- Right to access (Article 15)
- Right to rectification (Article 16)
- Right to erasure (Article 17)
- Right to restriction (Article 18)
- Right to data portability (Article 20)
- Right to object, including automated decision making (Articles 21 & 22)

It is best to think about responding to requests as customer service, not just basic compliance. This can increase trust and confidence in your approach to B2B marketing and your overall brand. Conversely, your reputation would be damaged if you did not respond effectively to a request to amend personal data for accuracy or deletion

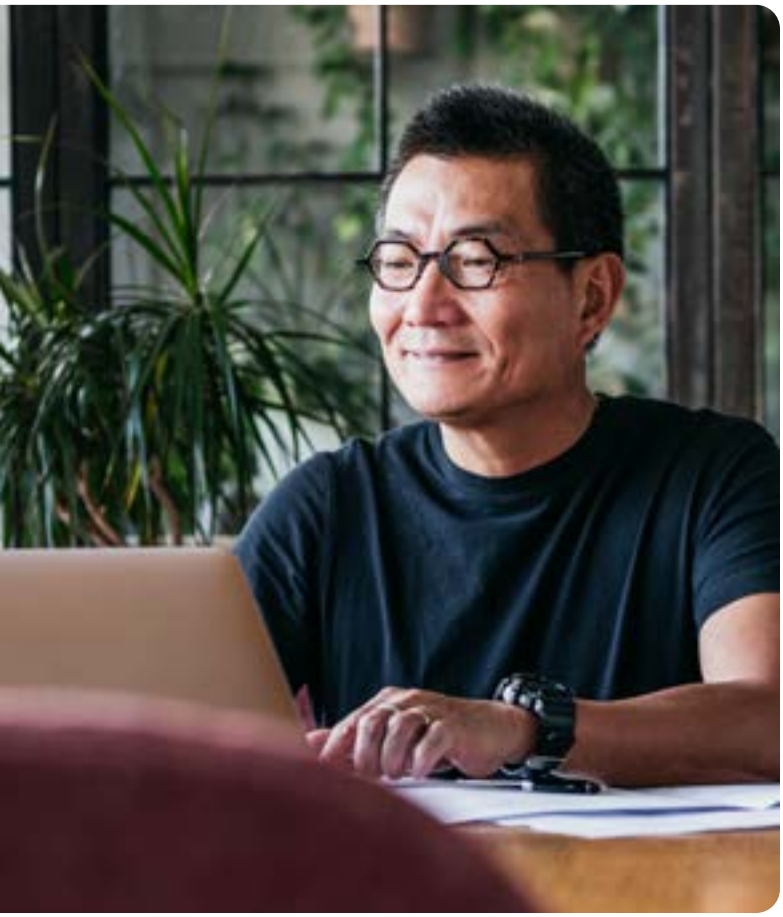
A GDPR rights request may sometimes come when you have issued an Article 14 notification.

Good Practice
Where it is feasible, in terms of cost and scale, you should consider offering digital tools via your website or app to allow people to execute their rights without human intervention.

If people are unhappy with how you have responded to their request they can complain to the Data Protection Authority in the European country where you are established.

The right of access. It is beyond the scope of this guide to cover this right in detail but it is important to have processes in place to respond to data subject access requests. You must respond within one month, but you can extend to two months for complex cases.

As well as providing the person a copy of their personal data, they are also entitled to other information about how you use their personal data, such as the purposes of the processing and the categories of personal data concerned. The full detail is contained in Article 15 GDPR.



Good Practice

There are steps that can make data subject rights compliance more straightforward, depending on scale and costs of your business operation.

- ☐ Consider automating access and personal data requests, such as deletion, to B2B related via web-based access and log-in.
- ☐ Provide an online form for people to complete if they wish to make a data subject rights request. This makes the process consistent.
- ☐ Ensure you have a clear inventory on where all personal data related to B2B is held, so that internal processes can specify how searches can be executed.
- ☐ Electronically log and monitor the management of requests, to ensure and evidence compliance.
- ☐ Ensure staff are trained to spot subject access requests in other correspondence and in telephone contact.

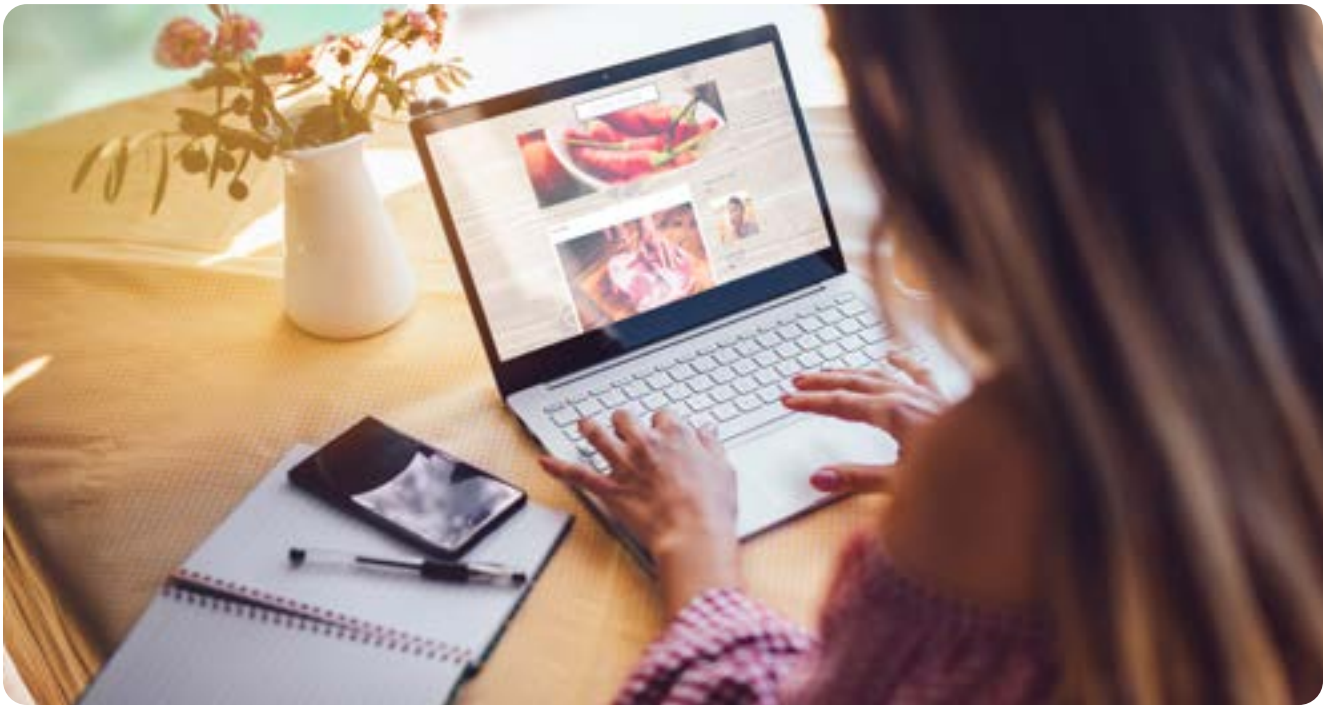
The right to rectification is relevant to B2B marketing. People may want to request corrections where the information you hold about them is incorrect. As above you can consider whether automation is possible to help streamline the process.

The right to object could be exercised by someone if they no longer wish to receive marketing. They could also object to other uses of personal data, including selling or sharing of personal data with third parties. In many cases placing a clear link in emails to opt-out should address the concern the person has. But it is important to remember that people may also object to other forms of marketing e.g. telephone.

The text of GDPR (article 21.2) is explicit that the right to object to direct marketing is absolute and there are no exceptions available.

Good Practice

You should use database suppression to ensure objections to marketing are recorded. People may sometimes only object to certain forms; for instance they could object to phone but not email. This means that you do not close off all marketing opportunities. It is also important that suppressions work across all relevant marketing systems in your company.



The right to erasure allows people to request deletion of their personal data. The GDPR makes clear this must be done without undue delay. You must delete the personal data when consent is withdrawn or it is no longer necessary for you to use it. People may also request that data is deleted when they object to marketing.

Make sure deletions take place across all relevant systems.

Right to restriction. In some circumstances people may request that you restrict the use of their personal data rather than delete it. This could be in circumstances where it is clear it needs to be kept for other purposes e.g in relation to a legal claim.

There is very little evidence of people using their right to data portability in relation to B2B marketing so we have not covered it in this guide.

Key Message

Enable compliance with easy to use preference tools and great customer service

Key Message

Ask the right questions when you buy data

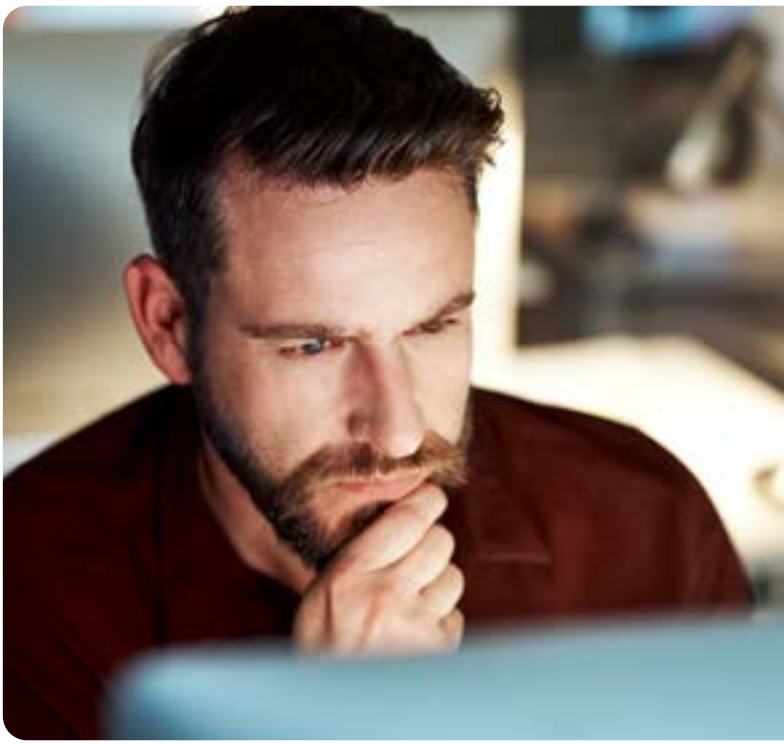
07.

EPRIVACY DIRECTIVE AND NATIONAL LAWS

Overview

As explained above, there are two pieces of legislation related to B2B marketing compliance in Europe - GDPR and national ePrivacy laws.

The EU's 2002 ePrivacy Directive required member states to implement national level laws on direct marketing. Policy makers in Europe decided that more specific rules are required for direct marketing, they cover the following channels: email, text, live telephone calls, automated calls and fax.



Solicited vs Unsolicited Marketing

A solicited message is one that is actively requested. If someone specifically asks you to send them some information, you can do so without worrying about the ePrivacy rules (although you must still say who you are, display your number when making calls, and provide a contact address).

An unsolicited message is any message that has not been specifically requested. So even if the customer has 'consented' to receiving marketing from you, it still counts as unsolicited marketing.

The ePrivacy rules apply to unsolicited marketing messages. This does not make unsolicited marketing unlawful. You can still send unsolicited digital marketing messages as long as you comply with the rules.

Postal marketing is not covered by ePrivacy law. It must still be compliant with GDPR. This means that you should still respect any objections in line with Article 21.2 GDPR.

These ePrivacy laws do not use a definition of personal data but instead focus on the concept of subscribers. The laws then distinguish whether subscribers are natural persons or corporate.

A corporate subscriber generally refers to a non-individual (i.e., a legal entity such as a company, public body, or other organization) that subscribes to a publicly available electronic communications service provider (for telephone, internet, etc.). Corporate subscribers in turn then allocate email addresses to their employees e.g. john.smith@zoominfo.com, and these addresses in turn would be considered corporate subscriber addresses.

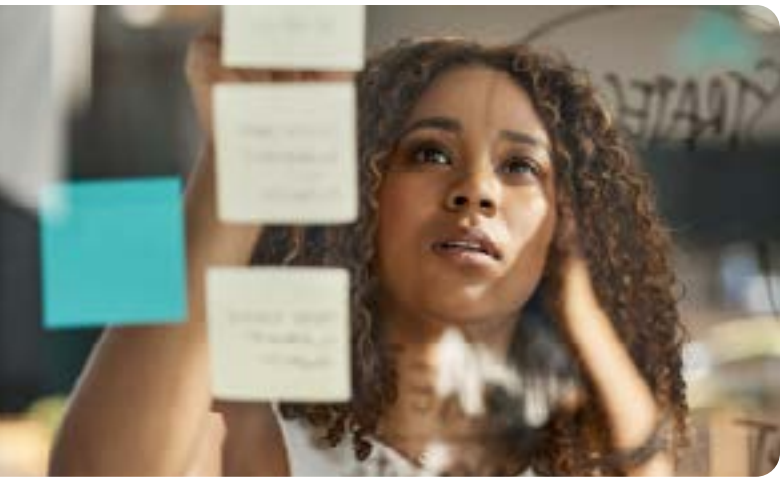
An individual subscriber is essentially a private individual who subscribes to a publicly available electronic communications service e.g. john.smith@gmail.com. In many EU Member States, individual subscribers can extend to include sole traders or partnerships where individuals act in a personal capacity.

The ePrivacy directive contains more detailed direction for national laws on Business to Consumer (B2C) marketing.

On B2B, it says that national legislation must sufficiently protect *"the legitimate interests of subscribers other than natural persons with regard to unsolicited communications."*.

Generally, unsolicited marketing to natural persons requires opt-in, corporate subscribers maybe out-out or opt-in.

Good Practice
These differences are important and you should think about designing your digital systems for B2B marketing so that you can record country specific information against individual records.



Enforcement of the national level direct marketing laws is the responsibility of data protection authorities in most European countries, though in a small number of countries the national telecoms regulator is responsible. The thresholds for fines are lower than GDPR, generally in the range of several hundred thousand euro or pounds.

We have listed all the European laws on direct marketing, as they relate to B2B, in the table in Annex A. We also draw out some particular country examples below.

It is helpful to think of the national e-privacy laws in Europe under three different categories for email and text:

Opt-out means that no consent is required as long as people can opt-out of receiving email or text marketing using a link or other mechanism.	*Croatia, Estonia, Finland, France, Hungary, Ireland, Latvia, Portugal, Slovenia, Sweden, United Kingdom*
Single opt-in requires one consent. Consent under Privacy laws must meet the GDPR standard.	*Belgium, Bulgaria, Czech Republic, Denmark, Iceland, Italy, Lithuania, Luxembourg, Netherlands, Norway, Poland, Romania, Slovakia, Spain*
Double opt-in requires consent and a further confirmation message to be sent.	*Austria, Germany, Greece, Switzerland*

There is also a useful map showing this in Annex B below.

In 'double opt-in' countries, alternative ways to market, other than email and text, are normally more important. We detail some of these options below. B2B marketing is still feasible in those countries, though your channel strategy may have to be adjusted.

Key Message
Understand e-privacy national law: consent or opt-out

The three categories are broad indications and you must still consider particular requirements in each national law.

There are specific rules for telephone marketing as well and they are explained below.

What is direct marketing and how does it differ from other business communications?

Whilst it will often be obvious, you should check that there is a common understanding of 'direct marketing communication' within your business.

Example: In the UK it is defined in law as: "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".

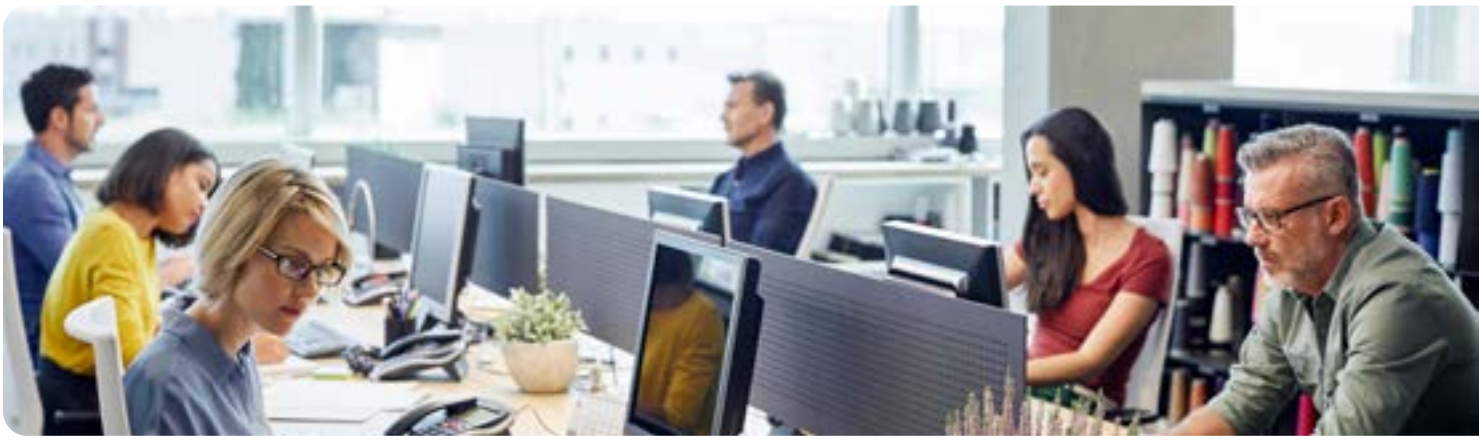
Why is this important?

Because sometimes businesses will send different types of communications using personal data that may not be classed at direct marketing.

For example: emails containing urgent service messages need not be classed as direct marketing or emails notifying the recipient of the processing of their personal data in compliance with GDPR. We recommend that direct marketing is not combined with these messages.

08.
MANAGING THE GDPR AND E-PRIVACY LAWS

TOGETHER IN E-MARKETING



This section addresses one of the most misunderstood aspects of B2B marketing.
This is because you will need to consider **the GDPR and national level e-Privacy laws** and ensure you are consistent in your approach to both.

You will therefore need to often consider national level laws and guidance.

Our table in Annex A will be a useful reference point.

Key points to remember:

Under GDPR you must have a lawful basis to process personal data: while there six possible bases listed under Article 6 of the GDPR, - the most relevant to B2B marketing will be either consent or legitimate interests.

There are other lawful bases under GDPR such as when personal data processing is necessary for the performance of a contract with the data subject. It is unlikely B2B marketing can be undertaken under this lawful basis as guidance from data protection authorities has indicated that it will be challenging for controllers to demonstrate that marketing is “necessary” for the performance of a contract.

When to use legitimate interests

- You may be using B2B data for purposes outside the scope of B2B electronic marketing, for example in postal campaigns or to enrich your first party data.
- Under some national ePrivacy laws you may be able to undertake B2B email or telephone marketing without consent. Though you will need to provide an opt-out mechanism and may need to check national 'do not call' registries.
- In this situation it is recommended that you rely on legitimate interests for GDPR compliance.

When to use consent

- When ePrivacy laws require that you obtain consent and opt-in for B2B marketing, this should also be your lawful basis under GDPR.
- Guidance from regulators has been clear that there should be consistency in use of consent between the two regimes.
- Consent under Privacy laws must meet the standard in the General Data Protection Regulation.
- Guidance from regulators has also indicated that it will generally be unfair to switch a lawful basis under GDPR from consent to legitimate interests, as this will be unfair to the data subject.

How to rely on the GDPR legitimate interests provision

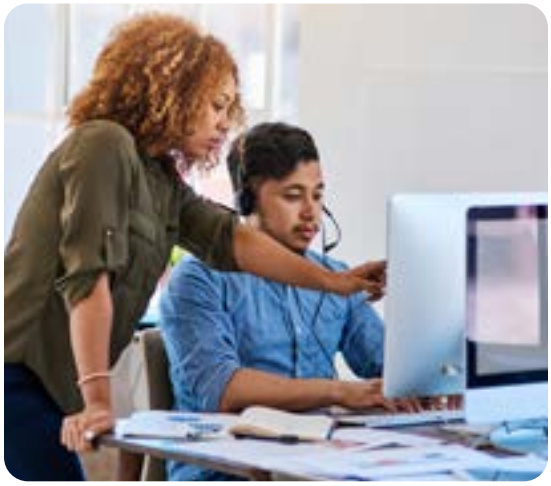
Recital 47 of GDPR states that *"the processing of personal data for direct marketing purposes may be regarded as carried out for legitimate interest."*.

This provides **an indication** that you should be able to rely on the provision but you must assess the particular circumstances of what your company is planning to do. We have also noted that the risk profile of using personal data for B2B marketing is generally low. This can also play into the assessment.

You can find more about legitimate interests in this guidance from the ICO, the UK Data Protection Regulator. The guidance states that use of legitimate interests is: *"likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact"*.

There are three tests to satisfy:

1. Identify a legitimate interest; you will need justify your business interest inconducting B2B marketing
2. Show that the processing is necessary to achieve it – you will need to consider how to explain your use of the personal data for B2B marketing and why you can't use other less intrusive methods (e.g. non personal data contacts to support the marketing).
3. Balance it against the individual's interests, rights and freedoms – you should consider what impact the personal data processing will have, safeguards you will put in place (e.g. how the opt out will work, screening against suppression lists, mechanism to ensure contact preferences are respected) and why this use will be within reasonable expectations of people.



You should record your decision to rely on legitimate interests. This is often called a legitimate interest impact assessment (LIA). The UK or ICO has made a template available on its website. Alternatively, the Data Protection Network also provides a template.

How to use consent

Consent under GDPR and ePrivacy laws must be freely given, specific and informed. This means that you must be clear that the consent covers B2B marketing, you cannot make consent to marketing part of a wider condition e.g. access to a service, if this unfairly gives someone no choice. You must also be careful not to bundle the consent with different processing, where the individual would expect them to be separate choices.

Consent also means providing control and allowing withdrawal of consent. For email marketing this means an opt-out link should be provided in all marketing emails. The principle is that it should be as easy to withdraw consent as it is to provide it.

Some national ePrivacy laws that require consent allow for an exception when a prior relationship is in place, this is often called a soft opt-in or prior relationship exception. The ePrivacy Directive allows this under certain conditions:

- An email address that was obtained from the individual in connection with a prior sale of goods/services.
- An email address that is used to market similar goods/services.
- The individual has not opted out of such use.
- When the email address is collected and each time it is used, the individual is told that they can opt out at any time.

How long can consent last for? – there is no set time limit provided for in the GDPR or ePrivacy laws and you should consider how long it is reasonable for the consent to last for in the context of the relationship with the data subject and what information you provide them. As noted above it is possible to consider the likely longevity of business relationships when considering what is reasonable.

Good Practice

You should also make sure you have a record of consent and date it was provided. Use digital preference tools to make opt-out a straightforward and user friendly process. The UK ICO recommends consent records should cover:

- Who consented: the name of the individual, or other, identifier (e.g. online user name, session ID).
- When they consented a copy of a dated document, or online records that include a timestamp, or, for oral consent, a note of the time and date which was made at the time of the conversation.
- What they were told at the time, a master copy of the document or data capture form containing the consent statement in use at the time, along with any separate privacy policy or other privacy information, including version numbers and dates matching the date consent was given.
- If consent was given orally, your records should include a copy of the relevent document or data capture form.
- Whether they have withdrawn consent, and if so, when.

Exceptions for B2B marketing in national ePrivacy Laws

Some national regimes have general provisions that are opt-in and require consent for B2C marketing but contain exceptions for B2B. For example:

In France, consent not is required if (1) the marketed product/service is related to the individual's profession and (2) at the time the email address/phone number was collected, the individual was informed their information would be used for marketing purposes, and given an opportunity to opt-out.

In the UK emails to corporate subscribers are not covered by the requirements of ePrivacy law.

In Belgium there is no exception for B2B but emails can be sent without consent if there is a "prior relationship". This will mean that marketing to existing and previous customers will not require consent. This could be recorded in your database.

There are other variants of these exceptions you will need to check in the relevant national legislation.

Double opt-in

Germany has a binding court ruling that double opt in is needed. This means that an additional confirmation of consent (e.g via follow up email) is needed. While not formally binding, regulators in Greece and Austria have also set out an expectation that double opt in should be used.

Email or text marketing using third-party data may be less cost effective in these countries.

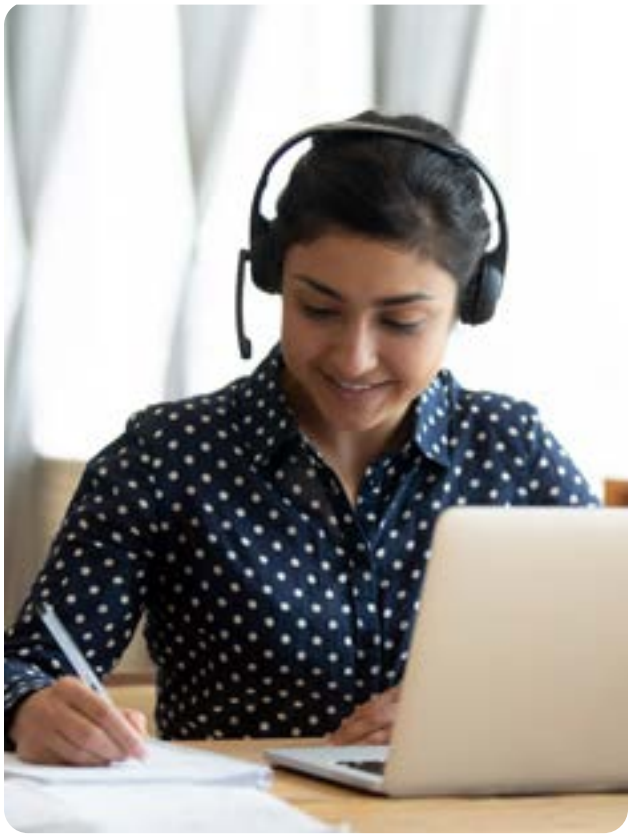
But, B2B marketing in these countries is feasible. In these countries companies can still use third-party data to guide a precision approach but may need to use a different strategy utilizing other channels such as phone and traditional mail. It can also inform offline approaches such as in-person marketing at conferences. The example in section 8 below illustrates how B2B marketing can be undertaken in Germany.

Key Messages

Understand GDPR and national law: consent or opt-out

Enable compliance with easy to use preference tools and great customer service

Making B2B marketing telephone calls: additional rules



Marketing calls are also subject to specific rules in national ePrivacy laws. You will need to consult the table in Annex A to see the different rules country by country.

There are separate legal provisions for live calls and recorded calls (sometimes called automated or robo-calls)

- → A live call is where a person makes the call in real time and speaks to someone using a phone system.
- → A recorded call has no human involvement; an automated system connects the call and then plays a recorded message.
- o It is often possible to make live B2B marketing calls without consent in many European countries.
- o In European countries, specific consent for recorded calls is always required.

It is therefore important that sales and marketing teams are always aware of the different requirements.

Country example: in the UK B2B live calls without consent are possible, but recorded B2B calls require consent.

The general steps you will need to take to ensure live B2B marketing calls are compliant are the following:

- ☐ Ensure you have considered national requirements to check whether a telephone number is registered against a 'do not call' registry. You can link this information to your database records. Many third-party vendors will offer a data service that pre-screens their database against these lists.
- ☐ Respond to requests for phone numbers to be opted out.
- ☐ You must display your number and clearly identify who is calling.
- ☐ You still need to comply with the GDPR requirements set out above on a lawful basis and transparency. If you do not seek consent you should rely on legitimate interests.

Details of the websites for do not call registries in Europe are contained in Annex C.

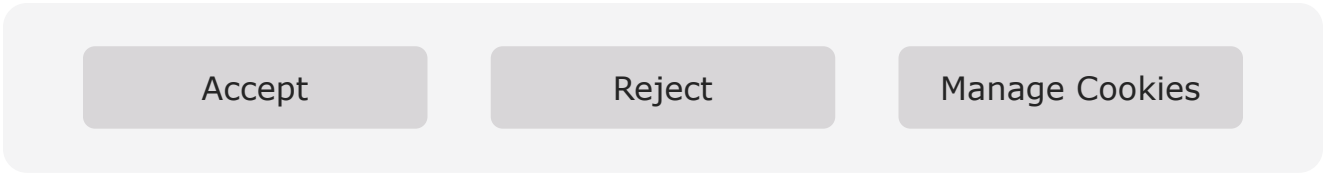
Using cookies - ePrivacy law requirements

National ePrivacy laws also contain requirements related to the use of cookies.

Cookies are used by websites and apps, they remember information about users. They do this by placing a cookie on their device. This can enable the use of features such as shopping carts, behavioral advertising and statistical tools to measure use of the website or app (e.g. Google Analytics).

You must get consent for cookies unless they are strictly essential for the operation of the service. Regulatory guidance indicates that this would include shopping cart features but not behavioral advertising or measurement tools.

Consent is generally gathered via a ‘pop-up’ when the user enters the website or app. Guidance from regulators is clear that this must contain a balanced accept or reject option. You can also allow people to manage their cookies settings via a further button. See below for an example:



It is also possible within the law to set a cookie so that users do not need to consent on each visit.

This guidance is only a summary and you should also consult the more detailed guidance available from the EDPB or national DPA. The UK ICO guidance is one example.

IP addresses may also be collected as part of your cookie process. If you collect IP addresses you should also treat this personal data under GDPR, as it is likely some of the addresses will relate to personal devices, such as a mobile phone. You must make this clear in your privacy policy. For example, you may collect an IP address when a customer completes a web form. We also noted the retention considerations in the section above.

There has been considerable enforcement action from EU and UK Data Protection Authorities related to cookie compliance – focused on whether there is a balanced accept/reject consent mechanism and ensuring that cookies are not placed on the user’s device before consent is given. These have not yet focused on B2B activity but could do in future as the sweeps undertaking by data protection authorities are automated and cover 1000s of websites or apps.

In B2C context, the French DPA, the CNIL, issued a €10 million fine on Yahoo for depositing cookies on data subject’s devices without prior consent and for not taking due account of the right to withdraw consent. The CNIL also issued the online advertising group Criteo with a €40 million fine for violations relating to cookie consent (both in 2023).

In the UK, the ICO undertook a sweep of the top 200 websites in 2024 and plans to sweep the top 1000 in 2025 and will follow up with action to ensure compliance. Action so far has included public reprimands.

09.

GDPR AND EPRIVACY WORKED EXAMPLES

UK, GERMANY, SPAIN, EU-WIDE, FRANCE, AND ITALY

We will now bring together the key points into a series of worked examples.

You can also consult Annex A for more detail on other countries.

Worked example: B2B email marketing in the UK
Legitimate interest and opt-out

- ☐ ABC company wants to undertake B2B marketing in the UK for the first time.
- ☐ ABC has decided to purchase third-party personal data from a vendor to use in its marketing campaign.
- ☐ ABC undertakes due diligence to understand the nature of the personal data it is purchasing to ensure the dataset was processed in accordance with the principles in Article 5 of **UK GDPR**. It finds that it can rely on legitimate interests under Article 6 of the **UK GDPR** to conduct the marketing.
- ☐ ABC sends marketing emails with clear opt-out links in the message, to comply with the **UK Privacy and Electronic Communications Regulations**.
- ☐ The marketing email also contains a **UK GDPR** Article 14 notification, for those recipients whose details were sourced in the dataset. *(ABC has the choice to do this within one month of acquiring the personal data or at the time of the first marketing communication).*
- ☐ ABC swiftly responds to any to any objections following the Article 14 notification.

Worked example: B2B marketing in Spain
Consent based and single opt-in, using third-party data

- ☐ XYZ company wants to undertake B2B marketing in Spain.
- ☐ The data the third party vendor provides is based on the user consenting to their data being used by the B2B companies named in the privacy notice.
- ☐ XYZ relies on consent under **GDPR**.
- ☐ XYZ sends an Article 14 notification to all the contacts in the database.
- ☐ It responds to any objections following the Article 14 notification.
- ☐ XYZ subsequently sends marketing emails, including clear opt-out details.

Worked example: B2B marketing in Germany
Using third-party data

- ☐ Company123 wants to undertake B2B marketing in Germany.
- ☐ It decides to purchase third-party data from a vendor.
- ☐ 123 sends an Article 14 notification to all the contacts on the list bought from the vendor.
- ☐ It responds to any objections following Article 14 notification.
- ☐ The company decides to use the new dataset to focus on telephone marketing, This is possible because implied consent is required for this form of marketing under **German ePrivacy law**. Implied consent is met if the individual could reasonably be expected to be interested in the product or service.
- ☐ 123 records a justification of why the selected contacts would meet this test. They rely on legitimate interests under **GDPR**.
- ☐ 123 also responds to any objection to the telephone calls and adds supressions to their database.
- ☐ 123 decides to focus their email campaign on existing customers, as under German ePrivacy law you can send marketing emails without consent if there is a prior relationship. 123 have marked this in their database. They rely on legitimate interests under GDPR.
- ☐ 123 also uses the purchased dataset to target in-person contacts at an upcoming industry conference. They rely on legitimate interests under GDPR.

Worked example: B2B marketing in the EU
Data collection in house

- ☐ Company456 operates across the EU and wants to avoid a country-by-country approach.
- ☐ Company456 collects personal data about customers from its website query form, business cards, and other information collected from sales reps.
- ☐ The website form contains a privacy notice to comply with Article 13 and consent opt-in for B2B marketing, by phone, email and text.
- ☐ Company456 decides to limit marketing to only opted-in data across the EU, so that it meets the standard of most European countries in a single process.
- ☐ The company seeks a further opt-in for customers from Austria, Germany, Greece, and Switzerland.

B2B Marketing in France
Using the B2B exception

- ☐ Company789 wants to undertake an email marketing campaign in France to focus on acquiring new customers.
- ☐ Company789 decides to purchase third-party data from a vendor to use in its marketing campaign.
- ☐ Company 789 undertakes due diligence to assess the compliance of personal dataset it has purchased to ensure that the individuals have received information about how the data will be used for B2B marketing and they had the ability to opt-out.
- ☐ Company789 can filter the purchased dataset by the profession of the contacts contained and is assured that marketing sent is relevant to the recipient's profession.
- ☐ It finds that it can rely on legitimate interests under Article 6 of the GDPR to conduct the marketing **and** rely on the B2B exception in the **French ePrivacy law**.
- ☐ It sends marketing emails with clear opt-out links in the message, to comply with the French ePrivacy Law.
- ☐ The marketing email also contains a **GDPR** Article 14 notification, for those recipients whose details were sourced in the dataset. (Company789 has the choice to do this within one month of acquiring the personal data or at the time of the first marketing communication).
- ☐ It swiftly responds to any to any objections in response to the Article 14 element of their communication.

B2B marketing in Italy
Using the prior relationship/soft opt in exception

- ☐ Company789 wants to undertake an email marketing campaign in Italy and target customers it has an existing relationship with.
- ☐ Company789 uses personal data from its CRM system, the system has a field indicates that the customers have previously purchased Company 789's products and services.
- ☐ Company789 ensured a privacy notice was provided to the customers, the products and services are similar to the ones previously purchased and an opt out was available at the time the customer provided their details.
- ☐ Company789 sends its marketing emails with a clear unsubscribe option to enable opt out.

10.

FREQUENTLY ASKED QUESTIONS

Q. **Which data protection laws cover B2B marketing in Europe?**

A. If you undertake B2B marketing in the EU or UK you will need to comply with the General Data Protection Regulation (GDPR) and also ensure that you comply with the national ePrivacy laws in each country where you undertake marketing.

Q. **Is an individual's business email address or telephone number personal data under GDPR?**

A. Yes, this will be classed as personal data under GDPR and your use of the data must comply with GDPR.

Q. **Could I get fined if my B2B marketing activities breach GDPR or a national ePrivacy law?**

A. Yes, under GDPR you could get fined up to 4% of global turnover, but there is no evidence since GDPR came into force that B2B marketing infringements will receive fines at the highest level. You could also get fined separately under national ePrivacy laws in Europe. The fines under these laws are lower than GDPR, for example in the UK the cap is currently £500,000.

Q. **Do I still need to comply with GDPR or ePrivacy laws if the contact details I have collected are already in the public domain? (such as on a website)?**

A. Yes, you must still comply, the public domain status of the data does not exempt you from compliance.

Q. **Is contacting people to conduct market research classed as direct marketing under GDPR and national ePrivacy laws?**

A. No, contacting people to conduct genuine market research is not direct marketing. However, if your market research messages include promotional material, or if the research is ultimately being carried out for you or others to send direct marketing to the individuals involved, then it will be considered to be direct marketing and the applicable rules must be followed.

Q. **Do I need comply with the GDPR transparency requirements if I have purchased the contact details from a third party?**

A. Yes, you must still provide this information and within one month.

Q. **Can I use consent under a national ePrivacy law and legitimate interests under GDPR?**

A. No, you should ensure that GDPR and ePrivacy are aligned e.g. you should use consent under both laws. You can use legitimate interests under GDPR if an ePrivacy exception to consent applies.

Q. **Do individuals have any rights in relation to their business contact details?**

A. Yes, the rights given to individuals under the GDPR apply but the lawful basis under which you have gathered their data will impact the rights they can exercise.

11.
CHECKLIST

- ☐ We have a record of the personal data we use for marketing purposes
- ☐ We have a data protection policy that enables our company to comply with the GDPR principles and the lifecycle of data management – from collection to deletion
- ☐ We have assessed the national ePrivacy requirements for each European Country where we conduct B2B marketing
- ☐ We provide effective privacy notices for personal data we collect directly and personal data we purchase from third parties
- ☐ We assess and record whether we are using consent or legitimate interests under GDPR, aligned with national ePrivacy laws
- ☐ All the consent mechanisms we use for marketing purposes comply with the standard in GDPR and national ePrivacy law requirements such as double opt in
- ☐ We keep records of consent, in accordance with data protection authority guidance
- ☐ We have a process in place to handle requests related to data subject rights
- ☐ We regularly check that that the unsubscribe or opt out mechanisms operate correctly
- ☐ We undertake a due diligence check on third party vendors we purchase data from or use for the provision of other data services, such as data verification, augmentation, or analytics services
- ☐ We ensure that any uses of AI in B2B marketing, where personal data is processed, comply with the GDPR and we conduct a Data Protection Impact Assessment if it is deemed high risk

12. USEFUL RESOURCES

General guidance on data protection

Guidance on EU GDPR from the European Data Protection Board

Guidance on EU GDPR from the European Commission

Guidance on UK GDPR from the Information Commissioner's Office (UK)

Specific guidance on B2B marketing compliance from regulators

B2B guidance from the Information Commissioner's Office (UK)

Direct Marketing guidance from Belgian DPA

Guidance on commercial prospecting from the CNIL In French.

Direct Marketing guidance from the German Data Protection Conference (group of German Data Protection Authorities) In German.

BIC / BUSINESS INFORMATION COALITION

ANNEX A

ANNEX A

DATA PROTECTION AND EPRIVACY LAWS IN EUROPE

NATIONAL EPRIVACY LEVEL LAWS - SUMMARY TABLE

Re-used and adapted with permission from ZoomInfo:

https://www.zoominfo.com//wp-content/uploads/2022/08/EU-Member-State-Marketing-Laws.pdf

This table covers all 27 EU member states, plus the countries of the European Economic Area (EEA). Switzerland is not in the EU or EEA, but is part of the EU single market. The UK is also included given its previous EU membership.

We have also provided a map in Annex B, indicating the countries that are opt-out, opt-in and double opt-in for email and text marketing.

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Tier 1 – Laws with the highest compliance burden (double opt in)					
Austria	§ 107 of the new TelecomLaw 2003 (TKG 2003) TelecomLaw 2003 (TKG 2003)	Prior consent required unless: (1) the message is not sent for direct marketing purposes; (2) the message is addressed to fewer than 50 recipients; or (3) the prior relationship exception applies.	Yes	Prior consent required	None
Germany	§ 7. of the "Gesetz gegen den unlauteren Wettbewerb" (Law Against Unfair Competition)	Prior consent required unless prior relationship exception applies. Per German DPA guidance and court cases, should obtain double opt-in consent. Double opt-in is a two stage process where two separate actions are required. The user must take an action to opt-in, and then the user must confirm their opt-in by taking a second action. For example, signing up to a mailing list on a website and then confirming consent to receive mailing list emails by clicking on a link in a confirmation email.	Yes	Prior consent required	**Phone Exception:** Only implied consent required. Implied consent met if the individual could reasonably be expected to be interested in the product or service.

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Greece	Article 11 of Law 3471/ 2006	Prior consent required unless prior relationship exception applies	Yes	Consent required if the individual or business has indicated to their provider of publicly available electronic communications service (i.e., phone service providers) that they do not wish to receive Such communications. Otherwise, consent not required, but opportunity to opt-out must be provided.	None
Switzerland	Article 3(1)(o) of the Federal Act on Unfair Competition Article 88 of the Ordinance on Telecommunications Services	Prior consent required unless prior relationship exception applies.	Yes	Consent not required unless individual is listed on national do not call registry. Must provide opportunityto opt-out.	None
Tier 2 - Laws with the middle compliance burden (opt in - single consent)					
Austria	§ 107 of the new TelecomLaw 2003 (TKG 2003) TelecomLaw 2003 (TKG 2003)	Prior consent required unless: (1) the message is not sent for direct marketing purposes; (2) the message is addressed to fewer than 50 recipients; or (3) the prior relationship exception applies.	Yes	Prior consent required	None
Belgium	Article XII.13 of the Code of Economic Law Royal Decree of 4 April 2003 regulating adv	Prior consent required unless prior relationship exception applies	Yes	Consent not required unless individual is listed in the national do not call registry.	None
Bulgaria	Electronic Communications Act, Chapter 15, Section III, Article 261	Prior consent required unless prior relationship exception applies	Yes	Prior consent required unless prior relationship exception applies	None
Cyprus	The Regulation of Electronic Communications and Postal Services Law (Law 112(I)/ 2004)	Prior consent required unless (1) prior relationship exception applies or (2) the person/entity has stated in the Cyprus Phonebook Database that they wish to receive such messages.	Yes	Prior consent required.	None
Czech Republic	Act on Certain Information Society Services (480/2004 Coll.)Act on Electronic Communications (127/2005 Coll.), section 96	Prior consent required unless prior relationship exception applies	Yes	Consent not required unless individual is listed in the national do not call registry.	None
Denmark	Danish Marketing Practices Act no. 426 of 3 May 2017, Article 10	Prior consent required unless prior relationship exception applies	Yes	Consent not required unless individual is listed in the national do not call registry.	None
EEA - Iceland	Electronic Communications Act No 81/2003	Prior consent required unless prior relationship exception applies.	Yes	Consent not required unless individual is listed in the national do not call registry.	None

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Italy	The Italian Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) as amended by Legislative Decree No. 101 of 10 August 2018, Chapter X, Section 130	Prior consent required unless prior relationship exception applies.	Yes	Prior consent required unless the individual's phone number is listed in the public telephone directory and is not enrolled in the public opt out register.	None
EEA - Liechtenstein	Law of 17 March 2006 on Electronic Communications DPA guidance on direct marketing	Prior consent required unless prior relationship exception applies.	Yes	Consent not required if the individual is listed in a public telephone directory or a business directory and has not added an exclusion regarding use for advertising purposes.	None
Lithuania	Law on Legal Protection ofPersonal Data 1996. Law of Electronic Communications 2004. Law on Advertising 2000	Prior consent required unless prior relationship exception applies.	Yes	Prior consent required.	None
Luxembourg	Law of 30 May 2005 on Electronic communications networks and services.	Prior consent required unless prior relationship exception applies.	Yes	Prior consent required.	**Exception:** Consent requirements only applicable to natural persons; consent not required for marketing sent to legal entities. Must provide opportunity to opt-out.
Malta	Processing of Personal Data (Electronic Communications Sector) Regulations Subsidiary Legislation 586.01 the "Regulations".	Prior consent required unless prior relationship exception applies.	Yes, but only applicable to email (not SMS)	Consent not required. Must provide opportunity to opt-out.	None
Netherlands	Article 11.7 of the Dutch Telecommunication Act dated 5 June 2012 2021 amendment to Telecommunication Act	Prior consent required unless prior relationship exception applies.	Yes	Opt-in consent required unless prior relationship exception applies.	**Email & SMS Exception:** Consent not required to communicate to a person acting in the exercise of their profession or business if: (1) the sender is using contact information "intended and provided by the user" for such purposes; or (2) the person is based outside of the EEA and the applicable country's laws are complied with.

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
EEA - Norway	Article 11.7 of the Dutch Telecommunication Act The Marketing Control Act dated 9 January 2009	Prior consent required unless prior relationship exception applies.	Yes	Consent not required unless an individual is listed in the national do not call register. Must provide an opportunity to opt-out.	None
Poland	The Act on e-Services ('e-Services'). Telecommunications Law ('Telco').	Prior consent required unless the individual made their email address available for marketing purposes.	None	Prior consent required.	None
Romania	Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector	Prior consent required unless prior relationship exception applies.	Yes	No legal provisions specifically regulating live marketing by phone. Under GDPR, must provide opportunity to opt-out.	None
Slovakia	Act on Electronic Communications (351/2011 Coll.).	Prior consent required unless prior relationship exception applies.	Yes, but only applicable to email	Prior consent required	**Exception:** Act requirements only apply to natural persons. No language specifically governing communications for B2B purposes.
Spain	Law 34/2002 on information society services and electronic commerce (LSSI). Law 9/2014 on General Telecommunications.	Prior consent required unless the individual made their email address available for marketing purposes.	None	Consent not required unless individual is listed on national do not call registry ("Robinson lists"). Must provide opportunity to opt-out.	None

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Tier 3 – Law with the lowest compliance burden (opt out regimes – no consent required)					
Croatia	Electronic Communications Act, Article 107	Prior consent required unless prior relationship exception applies	Yes	Prior consent required unless prior relationship exception applies	**Phone Exception:** Consent not required for non-automated phone calls to a business for marketing and sales purposes.
Estonia	Electronic Communications Act Law of Obligations Act, Section 60	Prior consent required unless prior relationship exception applies	Yes	Prior consent required.	**Email & SMS Exception:** Consent not required for B2B email or SMS. Must provide an opportunity to opt-out. Phone Exception: Law of Obligations Act only applies to ""consumers,"" defined as natural persons entering transactions not related to professional activities. Consent requirements inapplicable to B2B transactions.
Finland	Information Society Code (917/2014), Chapter 24, Sections 200-202 Data Protection Ombudsman FAQs on Direct Marketing	Prior consent required unless prior relationship exception applies	Yes	Prior consent required unless prior relationship exception applies	**Exception:** Consent not required if marketed product/ service issubstantially related to the person's work duties. Must provide opportunity to opt-out.
France	Article L34-5 of the Postal and Electronic Communications Code CNIL's 28 December 2018 guidance on commercial prospecting by email Article L121-34 of the Law on Consumer Protection	Prior consent required unless prior relationship exception applies	Yes	Consent not required unless individual is listed in the national do not call registry.	**Email & SMS Exception:** Consent not required if (1) the marketed product/ service is related to the individual's profession and (2) at the time the email address/phone number was collected, the individual was informed their information would be used for marketing purposes,and given an opportunity to opt-out. **Phone Exception:** Consumer protection law only applies to "consumers," defined as a person acting for purposes that don't fall within the scope of its commercial activities. Consent requirements inapplicable for B2B.

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Hungary	Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Advertising Act). Act CVIII of 2001 on Electronic Commerce and on Information Society Services (E-commerce Act). Act C of 2003 on Electronic Communications	Prior consent required	Consent not required unless individual has indicated in subscriber directories that their information can't be used for direct marketing. Must provide opportunity to opt-out.	None	**Exception:** Consent requirements only applicable to natural persons acting for purposes outside their occupation or economic activity; consent not required for marketing sent to legal entities. Must provide an opportunity to opt-out.
Ireland	The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, Section 13	Prior consent required unless prior relationship exception applies.	Yes, but only applicable to email (not SMS)	"Landlines: Consent not required unless individual has indicated in the National Directory Database that their information can't be used for direct marketing.Mobile: Prior consent required."	**Email Exception:** Consent not required if (1) marketing is sent to an email address used in context of a commercial or official activity and (2) the message relates solely to that commercial or official activity. Must provide opportunity to opt-out.
Latvia	Law on Information Society Services, dated 4 November 2004	Prior consent required unless prior relationship exception applies.	Yes	Prior consent required.	**Exception:** Consent requirements only applicable to natural persons; consent not required for marketing sent to legal entities. Must provide opportunity to opt-out.
Portugal	Law 41/2004 of August 18 on processing of personal data and the protection of privacy in the electronic communications sector (amended by Law 46/2012 of August 29).	Prior consent required unless prior relationship exception applies.	Yes	Consent not required unless individual is listed in the national do not contact registry. Must provide opportunity to opt-out.	**Email & SMS Exception:** Consent not required for "legal person" (business) unless it is entered into the national do not contact registry. Must provide opportunity to opt-out.
Slovenia	Electronic Communications Act (Zakon o elektronskih komunikacijah; ZEKom-1). Personal Data Protection Act (Zakon o varstvu osebnih podatkov; ZVOP-1)	Prior consent required unless prior relationship exception applies.	Yes	Prior consent required	**Exception:** Act requirements only apply to natural persons. No language specifically governing communications for B2B purposes.
Sweden	Marketing Practices Act (Sw. marknadsforingslagen (2008:486)) amended 21 July 2019. The Electronic Communications Act (Sw. lagen om elektronisk kommunikation (2003:389)) amended 1 October2019.	Prior consent required unless prior relationship exception applies.	Yes	Consent not required. Must provide opportunity to opt-out.	**Exception:** Act requirements only apply to natural persons. No language specifically governing communications for B2B purposes.

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
United Kingdom	Privacy and Electronic Communications Regulations (PECR) 2003	Sole traders and some partnerships treated as individuals, and express consent required unless prior relationship exception applies. For corporate bodies (company, Scottish partnership, limited liability partnership, government body), only need to provide ability for individual employees to opt-out.	Yes	Express consent required for live calls to individuals and businesses who are listed in the UK's do not call lists (Telephone Preference Service (TPS), and Corporate TPS (CTPS)).Opt-out consent required for individuals not listed in the do not call lists.	**Exceptions:** Consent not required for phone calls to companies not listed in the TPS or CTPS. Consent not required for emails/ texts to certain companies.

Table of countries outside of Europe

At the request of BIC members, information for Australia and Canada has now been added

Country	Law of reference	Consent for Email & Text	Prior Relationship Exception (Applies to Email & Text)*	Consent for Phone Calls	B2B Exceptions
Australia	Spam Act 2003 Do Not Call Register (DNCR) Act 2006	A commercial electronic message (including emails and SMS sent for marketing purposes) must not be sent without the prior opt-in consent of the recipient.	Consent can be inferred where there is an existing commercial relationship between the sender and the customer which relates to the subject matter of the marketing communication.	Telemarketing calls made or sent to a number registered on the Do Not Call Register ('DNCR'), by a person (including a partnership), are only permitted if a relevant account holder or their nominee has consented to the making of the call.	No
Canada	Canada's Anti-Spam Legislation CASL) 2010 Telecommunications Act and the Competition Act Canadian Radio-television and Telecommunications Commission Unsolicited Telecommunications Rules	Under CASL, individuals and businesses are required to obtain consent from customers before sending them commercial electronic messages, such as emails or texts	Consent can be implied: • When the sender has an existing business relationship with the person to whom the message is sent. • The person to whom the message is sent has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's business, role, functions or duties in a business or official capacity • The person to whom the message is sent has disclosed, to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity	Express consent required for live calls to individuals and businesses who are listed in the UK's do not call lists (Telephone Preference Service (TPS), and Corporate TPS (CTPS)).Opt-out consent required for individuals not listed in the do not call lists.	**Exceptions:** Consent not required for phone calls to companies not listed in the TPS or CTPS. Consent not required for emails/texts to certain companies.

BIC / BUSINESS INFORMATION COALITION

ANNEX B

ANNEX B

EUROPE MAP

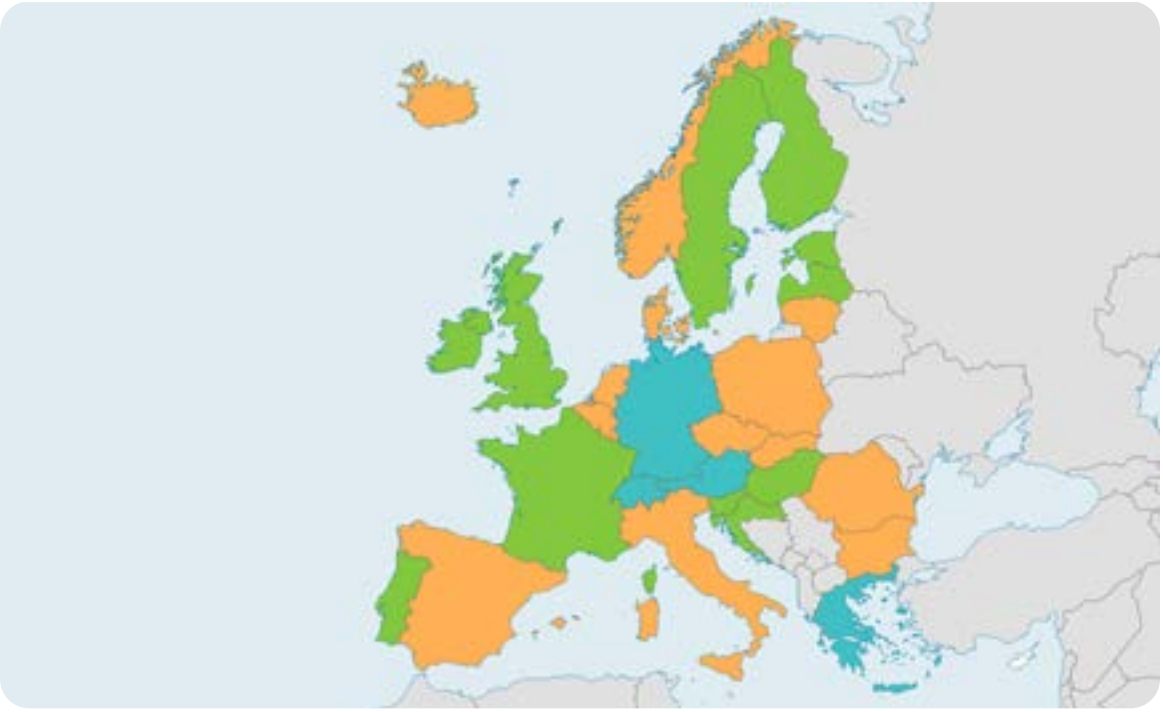
COLOR CODE FOR EMAIL/TEXT CATEGORY OF B2B MARKETING LAW

Opt-out: Croatia, Estonia, Finland, France, Hungary, Ireland, Latvia, Portugal, Slovenia, Sweden, United Kingdom (consent not needed, just a mechanism to opt-out)

Single opt-in: Belgium, Bulgaria, Czech Republic, Denmark, Iceland, Italy, Lithuania, Luxembourg, Netherlands, Norway, Poland, Romania, Slovakia, Spain (single consent needed).

Double opt-in: Austria, Germany, Greece, Switzerland

(double opt-in means consent must be gained and then confirmed again, usually in an email).



BIC / BUSINESS INFORMATION COALITION

ANNEX C

ANNEX C

LIST OF EUROPEAN DO NOT CONTACT REGISTRIES

As noted above some European countries operate a 'do not contact' registry, if allowed under their ePrivacy law. Most of these are focused on telephone calls but some also cover email or post. We have listed the key services below. In some countries, they are often called 'Robinson Lists'.

Austria	*Email - https://www.rtr.at/TKP/service/ecg-liste/ECG-Liste.de.html*
Belgium	*Calls - https://www.dncm.be/en/home*
Croatia	*Calls - https://www.hakom.hr/en/e-registry-do-not-call/224*
Finland	*Calls - https://www.asml.fi/kieltopalvelut/*
France	*Calls - https://www.bloctel.gouv.fr/*
Ireland	*Calls - https://www.comreg.ie/advice-information/unsolicited-contacts-national-directory-database/*
Italy	*Calls - https://registrodelleopposizioni.it/*
Netherland	*The Do-not-call-me register was discontinued in 2021*
Poland	*Calls - https://listarobinsonow.pl/*
Portugal	*Calls - http://www.amd.pt/*
Spain	*Calls, postal, email, SMS https://www.listarobinson.es/*
Sweden	*Calls - https://nixtelefon.org/english/*
EEA- Iceland	*Calls - https://www.skra.is/umsoknir/rafraen-skil/bannmerking/*
EEA - Norway	*Calls - https://www.brreg.no/en/products-and-services-2/opting-out-of-telephone-sales-and-addressed-advertising/*
United Kingdom	*Calls - https://www.tpsonline.org.uk/ and https://www.tpsonline.org.uk/register/corporate_tps*
Switzerland	*Calls - https://www.seco.admin.ch/seco/de/home/Werbe_Geschaeftsmethoden/Unlauterer_Wettbewerb/Unerbetene_Werbeanrufe.html#2138079370*

BIC / BUSINESS INFORMATION COALITION

ANNEX D

ANNEX D

MEMBERS OF THE BUSINESS INFORMATION COALITION

The Business Information Coalition ("BIC") is a collective of like-minded companies in the data and business intelligence community. These organizations come together to coordinate their work and share insights about developments in the legislative and regulatory world. The following companies have provided material and financial contributions towards this project: