



# B2B Outbound Marketing Guide for European Markets

# Introduction

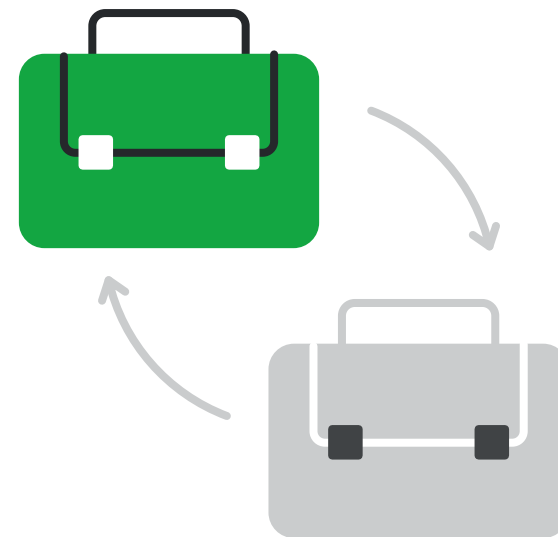
Outbound marketing is one of the most important activities any business can engage in.

It involves marketers reaching out to customers and making them aware of a product, service or brand. It requires companies to take the initiative and look for customers, rather than waiting for customers to come to them. For most sales and marketing professionals, the two main functions of outbound marketing are direct emails and cold calls.

In recent times, outbound marketing has been presented with a number of challenges, the most pressing of which has been the introduction of the General Data Protection Regulation (GDPR). This new and far-reaching legislation has implications for the ongoing success of outbound marketing, especially for UK marketers and salespeople who want to reach out to European customers - but is it as bad as some people suggest?

**This guide will explain the following:**

- What the GDPR is, its aims and the penalties it imposes.
- What rules the GDPR dictates on outbound marketing in a B2B context.
- How UK salespeople and marketers can launch B2B outbound campaigns to Europe in a safe and compliant manner.



# Contents

Introduction	2
What is the GDPR?	4
How does the GDPR impact B2B outbound marketing?	6
How should B2B organisations maintain compliance under the GDPR?	8
Glossary of Terms	23

# What is the GDPR?

The General Data Protection Regulation (GDPR) is a regulation in European Union (EU) law. It was put in place to address a number of data protection and privacy concerns for all individuals living inside the EU and the European Economic Area (EEA). It came into effect on 25th May 2018.



## What are the aims of the GDPR?

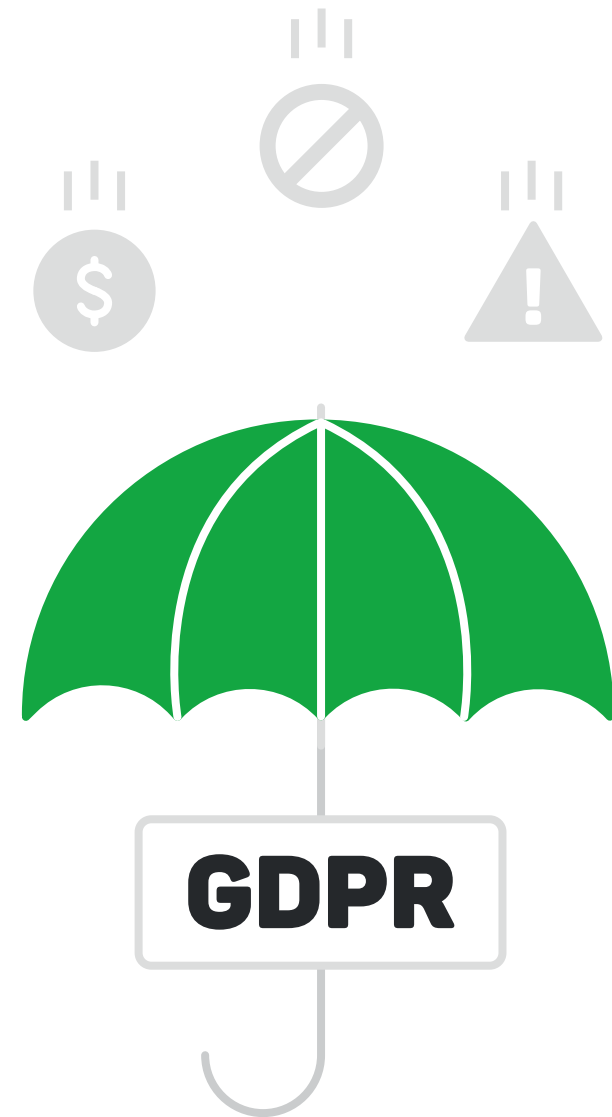
- The primary aim of the GDPR is to give European citizens greater control over their personal information. The regulation contains provisions and requirements applicable to the processing of the personal data of individuals (referred to as “data subjects” in the legislation wording).
- The GDPR alters how private sector businesses and public sector organisations (referred to as “data controllers” in the legislation wording) are allowed to collect, store and process personal data. There are a number of legal bases by which businesses are allowed to process this data, one being that unambiguous and individual consent is granted by the data subject before any personal data can be processed by the data controller. This, and the others, are discussed in this ebook.
- Although the GDPR is an EU regulation, it applies directly to any company that does business with European citizens. The GDPR was drafted to provide clarity to international businesses on how they should handle the personal data of those living inside the EU or EEA.
- Lastly, the GDPR was devised to harmonise the data privacy laws across Europe, and bring the legislation for all 28 member states under the same regulatory umbrella.

## What are the penalties for non-compliance?

Any company that fails to comply with the GDPR can expect severe penalties. In the UK, the independent regulator ICO is mandated to enforce the GDPR with the following sanctions:

- Issuing warnings and reprimands to companies that have demonstrated noncompliance.
- Imposing a temporary or permanent ban on data processing.
- Ordering the rectification, restriction or erasure of data.
- Suspending data transfers to third countries.

The maximum penalty allowed under the GDPR is a fine of up to 4% of a company's annual global turnover or €20 million - whichever is greater. To avoid such hefty punishments, it's essential for companies to stick to the rules.



# How does the GDPR impact B2B outbound marketing?

GDPR wasn't designed to prevent B2B outbound marketing outright. It doesn't signal the end of building email lists and using these to promote your product. Notably, authorities have affirmed differences in business-to-consumer (B2C) and [business-to-business \(B2B\) marketing](#).

**While GDPR still applies for B2B if you're reaching out to a specific person, you may rely on a [legitimate interest under GDPR](#). Article 6(1) (f) of GDPR states that:**

1. Processing shall be lawful [...] if and to the extent that [...]  
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Therefore, if B2B companies are able to demonstrate that their legitimate interest in marketing their [product is favorably balanced against the recipients' expectations](#), then gaining consent from data subjects is not required. That said, any organization working in B2B should have in mind a clear and specific benefit when processing data and carefully consider

whether the recipient would object to receiving such marketing (and comply with any such objection, of course). It is important to keep in mind that regardless of the legal basis for processing a person's data, [one must always provide information to the data subject on how their data is processed](#).

The ICO is the independent UK regulator. It recommends the following three tests, as a means of defining legitimate interest:

## 1. Purpose

Is there a legitimate purpose behind the data processing? This can be defined in numerous ways. For many B2B businesses, it could be as simple as: "our legitimate interest is in marketing our goods to existing customers to increase sales." However, that's not the same as saying that all potential purposes are legitimate. Any activity which is illegitimate, unethical or illegal is not a legitimate interest. A good example is that while marketing to consumers may be a legitimate interest, sending out spam emails to consumers is not.

## 2. Necessity

Is the processing necessary to fulfil the purpose? It must be demonstrated that the data processing is proportionate and targeted to meet its

objectives. It's worth considering if the processing is strictly necessary, or if the same outcome can be achieved by less intrusive methods.

### 3. Balancing

Is the legitimate interest overridden by the individual's interests, rights or freedoms? This test is designed to show whether the data processing impacts in any way on the fundamental rights and freedoms of the data subject.

**Recital 75 of the GDPR elaborates further, defining the potential risks for data subjects as:**

- Any data processing which could lead to physical, material or non-material damage.
- Any data processing which gives rise to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage.
- Any data processing which deprives data subjects of their rights and freedoms or prevents them from exercising control over their personal data.
- Any data processing which reveals racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, or anything related to health, sex life, criminal convictions and other offences.
- Any data processing for the purpose of personal evaluation, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles.
- Any data processing of the data of vulnerable persons, and children in particular.
- Any processing activity which involves a large amount of personal data and affects a large number of data subjects.

# How should B2B organisations maintain compliance under the GDPR?

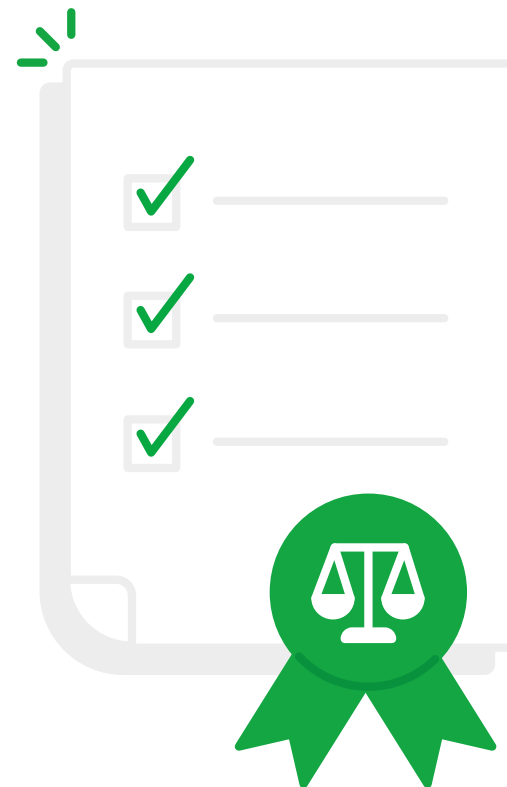
If the three tests are met, then legitimate interest has been proved, and data subject consent is not needed.

It's important to stress that while consent is not required in legitimate interest cases, opt-outs must still be provided. According to Article 139 of the ICO's Direct Marketing Guidance, "individuals have a right to opt out of receiving marketing at any time." So while B2B companies may be able to conduct direct marketing to corporate email addresses without consent (claiming a legitimate interest), they must nevertheless ensure that the data subject has the ability to opt-out of further communication.







To work out if you can use legitimate interests for employee or client data you should measure the data processing against the three tests: legitimate interest, the necessity of the processing, and whether it impacts on fundamental rights or freedoms.





Recital 47 of the GDPR says: "...Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller."





This does not say that the legitimate interest's basis always applies, but it does mean that a legitimate interest could exist where there is a 'relevant and appropriate relationship' between you and the individual, such as if the individual is your client or your employee.






















Country		1st Party Email Marketing	3rd Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
	Austria	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required	Prior opt-in required	Prior opt-in required.
	Belgium	To an individual B2B email address: Opt-in. Opt-out permitted†  To B2B generic email address (i.e. info@; sales@ etc): Opt-out.	Prior opt-in required	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.
	Bulgaria	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required	Prior opt-in required.	Prior opt-in required.
	Canada	Prior opt-in required.	Prior opt-in required	Opt-out Option required.	Opt-out Option required.
	Croatia	Prior opt-in required. Some opt-out contact permitted†.	Prior opt-in required	Opt-out Option required.	Prior opt-in required
	Cyprus	Prior opt-in required.	Prior opt-in required	Prior opt-in required.	Prior opt-in required

Country	1st Party Email Marketing	3rd Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
 Czech Republic	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required	Prior opt-in required.  Exception: If the phone number is in the public telephone directory.	Prior opt-in required
 Denmark	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.
 Estonia	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.
 Finland	Opt-out option required.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.

Country	1st Party Email Marketing	3rd Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
 France	Opt-out option required.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.
 Germany	Double opt-in required.  Some opt-out contact permitted†.	Double opt-in required.  Double Opt-in.	Prior opt-in required.	Prior opt-in required.
 Greece	Opt-out option required.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.
 Hungary	Opt-out option required.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.

Country		1st Party Email Marketing	3rd Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
	Ireland	Some opt-out contact permitted†.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list. Mobile phone: Prior opt-in required.	Prior opt-in required.
	Italy	Prior opt-in required.	Prior opt-in required	Prior opt-in required.	Prior opt-in required
	Latvia	Opt-out option required.	Opt-out option required.	Prior opt-in required.	Prior opt-in required.
	Lithuania	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required	Prior opt-in required.	Prior opt-in required
	Luxembourg	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.

Country	1st Party Email Marketing	1st Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
 Malta	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required.	Opt-out option required.	Prior opt-in required.
 Netherlands	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required.	Opt-out option required.	Prior opt-in required.
 Norway	To individual B2B email address: Prior Opt-in required. Some Opt-out contact permitted† to B2B generic email address which does not belong to an individual person (i.e. info@; sales@ etc.): Opt-out	To individual B2B email address: Prior Opt-in required. Some Opt-out contact permitted† to B2B generic email address which does not belong to an individual person (i.e. info@; sales@ etc.): Opt-out.		
 Poland	Prior opt-in required.	Prior opt-in required.	Prior opt-in required.	Prior opt-in required.
 Portugal	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.

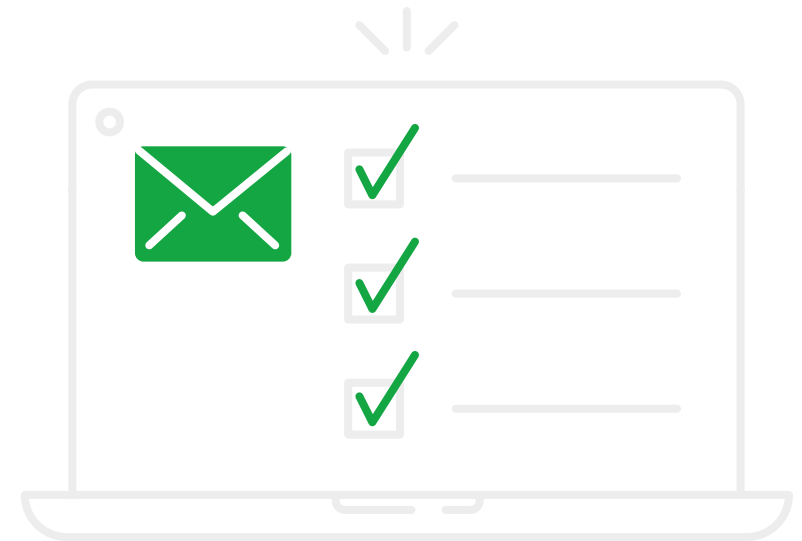
Country		1st Party Email Marketing	1st Party Email Marketing	B2B Non-Automated Calling	B2B Automated Calling
	Romania	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required.	Prior opt-in required.	Prior opt-in required.
	Slovakia	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.
	Slovenia	Prior opt-in required.	Prior opt-in required.	Prior opt-in required.	Prior opt-in required.
	Spain	Prior opt-in required.  Some opt-out contact permitted†.	Prior opt-in required.	Opt-out option required.	Prior opt-in required.
	Sweden	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.
	United Kingdom	Opt-out option required.	Opt-out option required.	Opt-out option required.  Required check of national 'do-not-call' list.	Prior opt-in required.
	United States	Opt-out option required.	Opt-out option required.	Opt-out option required.	Prior opt-in required.





## KEY

\* A national legislation implementing the General Data Protection Regulation 2016/679 (GDPR)






† Contact with the recipient is permitted on an opt-out basis if:





- The cold call is to general business numbers (i.e., contacting a business in general and not a specific employee) and not existing customers.
- Before the implementation of the upcoming EU ePrivacy Regulation into the national laws of the EU Member States, cold calling is mostly regulated by the applicable national telecommunications laws.
- If a marketer attempts to contact a specific employee of a company by using his/her personal details, the personal data protection requirements set out in the General Data Protection Directive (GDPR) and its national implementations will be triggered. A marketer who would like to contact a specific employee rather than a company has to have a legal basis for contacting him/her.













Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Austria	Telecommunications Act	Art. 107 of the Federal Act enacting the Telecommunications Act Federal Act amending the Data Protection Act 2000 (Data Protection Adaptation Act) 2018*
 Belgium	Article XII.13 of the Code of Economic Law Royal Decree of 4 April 2003 regulating advertising by electronic mail	Art. VI.111-114 and XIV.78-81 of the Code of Economic Law Law of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data*
 Bulgaria	Electronic Communications Act (Promulgated, SG No. 41/22.05.2007, last amended: SG No. 58/18.07.2017	Art. 261 of Electronic Communications Act Law for Protection of Personal Data*
 Canada	Canada's Anti-Spam Legislation (CASL)	Canadian Radio-television and Telecommunications Commission Unsolicited Telecommunications Rules
 Croatia	Electronic Communications Act (Official Gazette No. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017)	Art. 107 of Electronic Communications Act The Law on Implementation of the General Data Protection Agreement*










Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Cyprus	<p>The Processing of Data of a Personal Character (Protection of the Individual) Law (138(1)/2001)</p> <p>The Regulation of Electronic Communications and Postal Services Law (Law 112(I)/ 2004), as amended</p>	<p>Art. 106 of the Regulation of Electronic Communications and Postal Services Law</p> <p>The Order on the Legal Persons (Safeguarding of Legitimate Interests concerning Unsolicited Communications) of 2005</p> <p>Law Providing protection of natural persons against the processing of personal data and the free movement of this data*</p>
 Czech Republic	<p>Act on Certain Information Society Services (480/2004 Coll.)</p>	<p>Section 7 of the Act No. 480/2004 Coll., on certain Information Society Services and on Amendments to some Acts</p> <p>Draft Data Protection Act*</p>
 Denmark	<p>Danish Marketing Practices Act no. 426 of 3 May 2017, article 10.</p>	<p>Art. 10 of the Marketing Practices Act</p> <p>Law No. 502 of 23 May 2018 on Supplementary Provisions to the Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Exchange of Such Information*</p>
 Estonia	<p>Electronic Communications Act</p>	<p>§ 103 of the Electronic Communications Act</p> <p>Personal Data Protection Act 616 SE*</p>
 Finland	<p>Information Society Code (917/2014), Chapter 24, Sections 200 &amp; 202</p>	<p>Section 202 of the Act on Electronic Communications Services Data Protection Act*</p>

Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 France	Information Society Code (917/2014), Chapter 24, Sections 200 & 202	L34-5 of the Postal and Electronic Communications Code Law concerning the protection of personal data*  Section 7 of the Act Against Unfair Competition
 Germany	German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb - UWG) as last amended 17 February 2016	The German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680*
 Greece	Information Society Code (917/2014), Chapter 24, Sections 200 & 202	Art. 11 of the Law 3471/2006 Protection of personal data and privacy in the electronic communications sector  Art. 172 of the Law 4070/2012 Draft Law on the Protection of Data*
 Hungary	Act CXII of 2011 on the Right of Informational Self - Determination and on Freedom of Information (Info Act). 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. For certain sectors, such as medicine, other legislation may apply	Art. 162 of the Communications Act Data Protection Act*

Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Ireland	The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011	Art. 13 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 Data Protection Act 2018*
 Italy	Consolidation Act regarding the Protection of Personal Data (Data Protection Code – Legislative Decree No. 196 of 30 June 2003)	Sections 23, 24, and 130 of Italian Data Protection Code*
 Latvia	Law on Information Society Services, dated 4 November 2004	Section 9 of the Law On Information Society Services  Personal Data Processing Law*
 Lithuania	Law on Legal Protection of Personal Data 1996 Law of Electronic Communications 2004 Law on Advertising 2000	Art. 68 of the Law on Electronic Communications Law on the Protection of Personal Data *
 Luxembourg	Law of 14 August 2000 on e-commerce Law of 30 May 2005 on electronic communications networks and services	Art. 11 of the Law of 30 May 2005 Relating to Specific Provisions Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector Law of 1 August 2018 on the organization of the National Commission for Data Protection and the General Scheme on Data Protection*

Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Malta	Processing of Personal Data (Electronic Communications Sector) Regulations – Legal Notice 16 of 2003 as amended – implementing Directive 2002 / 58 / EC (as amended) – the “Regulations	Art. 9 of the Subsidiary Legislation 586.01 Processing of Personal Data (Electronic Communications Sector) Regulations Data Protection Act*
 Netherlands	Telecommunications Act dated 5 June 2012	Art. 11.7 of the Telecommunications Act Law Implementing The General Data Protection Regulation*
 Norway	The Marketing Control Act dated 9 January 2009	
 Poland	The Act on Personal Data Protection (‘PDP’) The Act on e-Services (‘e-Services’) Telecommunications Law (‘Telco’)	Art. 172 of the Telecommunications Act of 16 July 2004 Art. 10 of the Act of 18 July, 2002 on Providing Services by Electronic Means Law on the Protection of Personal Data*
 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) that implemented Directive 2002/58 subsequently	Art. 13-A and 13-B of the Law no. 46/2012, of 29 August Proposed Law No. 120/Xiii (3)*

Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Romania	Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector	Art. 12 of the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector Law 190/2018 on measures to implement regulations of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the EU Directive 95/46*
 Slovakia	Act on e-Commerce (22/2004 Coll.) Act on Electronic Communications (351/2011 Coll.)	Section 62 of the Act No. 351/2011 Coll. on Electronic Communications of 14 September 2011 Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. *
 Slovenia	Electronic Communications Act (Zakon o elektronskih komunikacijah; ZEKom-1) Personal Data Protection Act (Zakon o varstvu osebnih podatkov; ZVOP-1)	Art. 6 of the Electronic Commerce Market Act Article 158 of the Slovenian Electronic Communications Act Proposal of the Law on Personal Data Protection*
 Spain	Law 34/2002 on information society services and electronic commerce	Art. 48 of the Law 9/2014 on Telecoms 5/2018 on urgent measures for the adaptation of Spanish Law to European Union regulations on data protection*

Country	Applicable Legislation for Email Marketing	Applicable Legislation for Cold Calling
 Sweden	<p>Marketing Practices Act (Sw. arknadsforingslagen (2008:486)) amended 4 May 2017</p> <p>The Electronic Communications Act (Sw. lagenom elektronisk kommunikation (2003:389)) amended 17 May 2017</p>	<p>Sections 19 and 21 of the Marketing Act (2008:486)</p> <p>Regulation (2018: 219) with additional provisions to the EU Data Protection Ordinance*</p>
 United Kingdom	<p>Privacy and Electronic Communications (EC Directive) Regulations 2003 last amended on 30 December 2016</p>	<p>Art. 21 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Data Protection Act*</p>
 United States	<p>CAN-SPAM Act</p>	<p>Title 47, Part 64, subpart L of the Electronic Code of Federal Regulations</p>

# Glossary of Terms

## Generic Email Address

This refers to non-personal business email addresses, e.g., enquiry@company.com or info@company.com. They are not considered personal data under the GDPR.

## Individual Corporate Address

This refers to personal business email addresses, e.g., james.isilay@company.com. As the email address states the recipient's name and place of work, it is considered to be personal data under the GDPR. Further information can be found on the European Commission website - "What is personal data?"

## Opt-In

This means that the prospect must give permission for a company to send emails to them. Opt-in emails must be targeted and only sent to the individuals who specifically request them. Opt-in enables B2B marketers to run safe outbound email campaigns, as the emails are sent only to contacts who opted to receive the information.

An opt-in generally takes the form of a tick box which, if filled in by the recipient, indicates that they would like to be contacted via a specific mode of communication. If the recipient doesn't tick the box, then the organisation cannot use their details for the form of marketing listed.

## Opt-Out

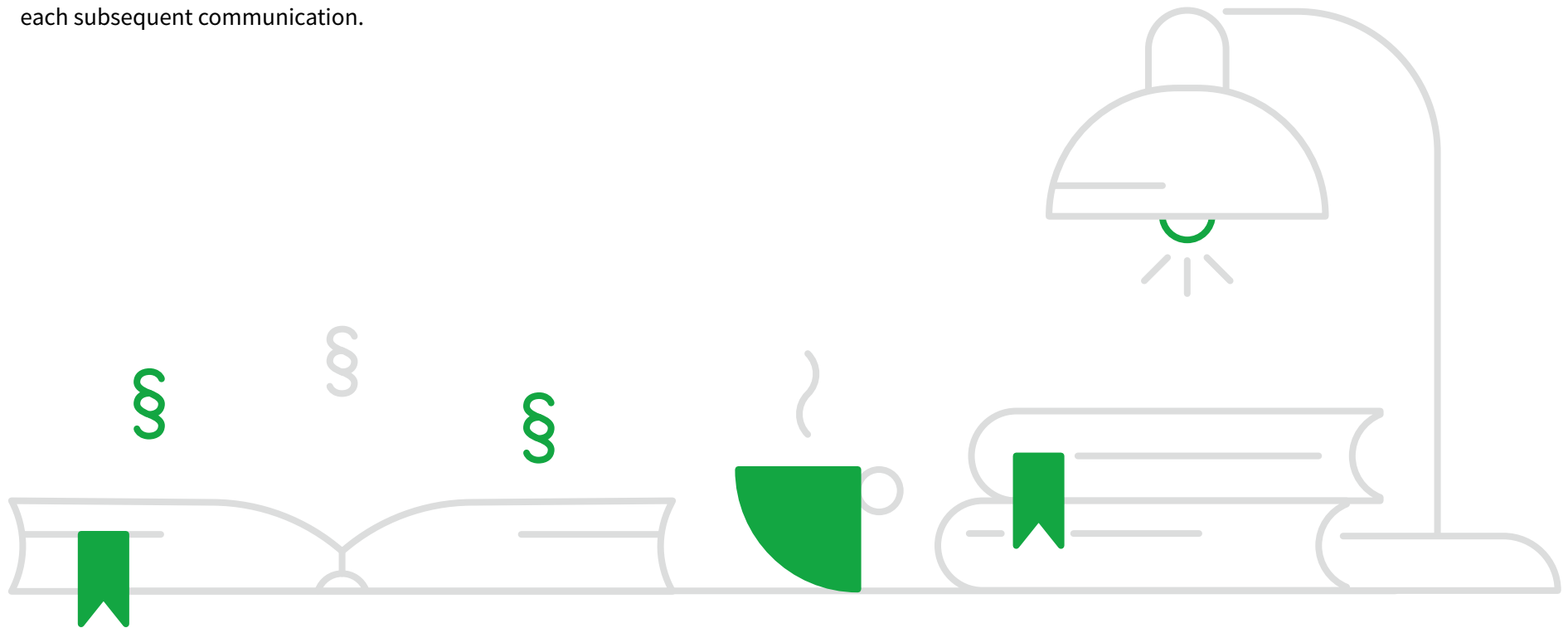
In contrast, opt-out means that the company is allowed to contact the prospect via email, unless the prospect specifically forbids it. Again, this usually takes the form of a tick box, which if ticked indicates that the prospect doesn't want to be contacted. To stay compliant, B2B companies must always act on this request. The information should be recorded and the prospect must be removed from your mailing list.

## Soft Opt-In

This means that the sending of marketing emails to the recipient is permitted on an opt-out basis if:

- The recipient's details were originally collected in the context of a sale or negotiation.

- The entity sending the emails is the same legal entity that collected the recipient's details initially.
- The email marketing relates to similar products and/or services for which the recipient's details were originally obtained.
- The recipient is given the opportunity, free of charge, to object to the marketing emails, both at the time their details were collected and in each subsequent communication.





## Pipedrive is a CRM built for sales reps by sales reps.

Our easy-to-use platform helps your reps keep everything they need to make a sale in one place: contact information, emails, information about where in the pipeline a client is and yes, even stats for your sales deck and slides for your presentation.

Never used Pipedrive before?

**Sign up for a 14-day free trial with just a couple of clicks and get started today.**

