A Lawyer's Guide To Marketing Compliance In Europe

By **Alja Poler De Zwart and Mercedes Samavi** (March 27, 2023)

Alja Poler De Zwart

Mercedes Samavi

Content marketing, promotional campaigns, MarTech — software used to optimize marketing efforts — these are a compliance minefield, requiring organizations to juggle various legal requirements while trying to create a successful campaign.

There are certain roles for in-house lawyers when it comes to understanding the marketing rule book, from ensuring good housekeeping around marketing, to complying with various privacy requirements.

This checklist should help in-house counsel determine whether their organizations have considered the key steps for meeting the marketing requirements in Europe.

1. What Is and Is Not Direct Marketing

As a rule of thumb, direct marketing means any communication that contains some form of advertising or promotion of an organization.

The definition of direct marketing may vary in each country but will generally include communications such as contacting prospects, for whatever reason; sending newsletters, event invitations and articles; presenting discount offers; and publicizing new product or service launches.

In some countries, an email might be considered marketing even if it only contains a company logo with a link to the company website or a discount offer at the bottom of the message.

Direct marketing does not include communications that are purely transactional, such as messages about a change in a website's terms or privacy policy, or specific security or account messages, such as a password reset email.

For in-house lawyers, it is worthwhile providing their marketing teams with appropriate training and ongoing support, so that they:

- Understand the implications of their intended actions; and
- Can correctly identify which communications would trigger marketing requirements.

Consider preparing business-friendly marketing guidelines that the marketing teams can use to ensure adequate compliance.

2. Identify the Requirements for Various Marketing Channels

The type of marketing that the organization wants to send will determine which rules to follow. In the U.K., for example, there are stricter requirements for electronic marketing, e.g., for email and SMS, compared to telephone and postal marketing.

An organization may be required to obtain prior opt-in consent in certain circumstances, while in others providing only an opt-out option would be sufficient. The important thing to note is that certain marketing rules will apply depending on the location of the marketing recipients, regardless of where an organization is established.

So, if an organization is marketing to individuals in the U.K., the U.K. Privacy and Electronic Communications Regulations will apply.[1] If marketing is directed at individuals in the Netherlands, the Dutch Telecommunication Sector Act will apply, and so on.[2]

In-house lawyers should work with their marketing teams to compile a list of all relevant marketing channels and track them according to the laws of the jurisdictions of the intended recipients. The penalties in the EU Privacy and Electronic Communications Directive 2002 are determined locally and do not fall under the one-stop shop principle of the EU General Data Protection Regulation.

Each European country has its own arsenal of enforcement powers that could increase an organization's legal exposure, particularly when launching a pan-European campaign.

3. Do not Assume a Lower Threshold for B2B Marketing

It is not always the case that business-to-business marketing is less regulated than business-to-consumer marketing. Countries such as Germany, Hungary and Poland impose the same rules on B2B email marketing as B2C email marketing: Organizations in these countries will need to have valid consent before sending out email marketing to business contacts in the same way as they would for consumers. We have seen regulators recently raise inquiries with respect to B2B marketing in the Czech Republic and Ireland on the basis of just one complaint.

4. The GDPR

Marketing to individuals will always involve some form of processing of personal information, including their names, contact details and marketing preferences. If marketing communications are tailored to a recipient's interests, such as their use of the website, purchase history, etc., this will be deemed to be profiling and the privacy rules for profiling will apply.

The marketing laws in Europe run parallel to the EU General Data Protection Regulation. Consequently, any organization's marketing campaign will need to comply with the GDPR, including having a valid legal basis for the processing, e.g., consent or legitimate interest, maintaining a transparent privacy notice that explains the relevant processing activities in sufficient detail, completing GDPR, Article 30 records and data protection impact assessments, and implementing appropriate contracts with third-party marketing campaign vendors.

In-house lawyers should always involve their privacy colleagues before starting a marketing campaign to determine the relevant privacy requirements. In practice, if a regulator is alerted to noncompliance with direct marketing rules, e.g., following an individual's complaint or a tip-off, it may expand the scope of its investigation to look into an organization's wider privacy actions.

Legal, privacy, compliance and other relevant departments should be aligned to preempt any regulatory inquiries into the organization's data protection compliance efforts.

5. The Right Type of Consent

Valid consent for marketing needs to be GDPR-compliant, i.e., freely given, clear, specific, informed and an unambiguous indication that the individual wants to receive marketing. The consent wording should name the organization and the marketing channels through which the individual consents to receive marketing.

Similarly, if an organization wants to send marketing on behalf of another entity, the consent should refer to that entity. In-house lawyers should consider developing baseline consent language for their organization's various marketing campaigns. This will generate a consistent approach to obtaining consent that remains true to each organization's voice and style.

In very narrow circumstances, organizations are permitted to rely on "soft opt-in consents." This option is only available where organizations directly obtain an individual's email address during a sale or negotiations for a sale of a product or service, and subsequently use that email to market similar products or services to the individual.

However, the key to this option is making sure that the individual was given an easy choice to opt out of marketing at the time when they provided their contact details and at each point of communication thereafter.

Not all organizations remember to do this and therefore are unable to rely on the soft opt-in approach. In-house lawyers should check that their marketing teams are using the soft opt-in approach correctly.

6. Legitimate Interest Is Not Always a Friend

Recital 47 of the EU GDPR states that the processing of personal information for direct marketing purposes may be regarded as carried out for a legitimate interest. However, it would not be right to assume that Recital 47 gives organizations carte blanche to carry out marketing without consent.

The EU Privacy Directive and its implementing laws require opt-in consent for the mere act of sending electronic marketing to an individual, e.g., using email, SMS or technologies such as cookies. This requirement is entirely separate and unrelated to the GDPR and cannot be disregarded by relying on legitimate interest.

In fact, a recent case in the U.K. noted that there is significant difficulty in relying on legitimate interest, particularly where the personal information had originally been acquired from third parties on a consent basis.[3]

In addition to obtaining consent under the EU Privacy Directive, in-house lawyers should work with their privacy colleagues to ensure the use of the correct legal basis under GDPR Article 6 for processing personal information as part of their marketing efforts.

This legal basis could be legitimate interest if appropriate, e.g., when using simple segmentation, individuals in Germany will receive different offers than individuals in Belgium, but in-house lawyers should not forget to carry out a legitimate interest assessment.

The legal basis could also be a separate consent, e.g., if marketing is based on extensive,

privacy-intrusive profiling. The Italian regulator fined an Italian utility company €4.9 million ($5.3 million) in December last year for, among other factors, failing to obtain a separate consent for marketing and for profiling.[4]

7. Easy to Opt Out

Individuals should not have to jump through hoops to opt out of marketing. The opt-out mechanism should be free, quick and easy to use, e.g., at the bottom of every email or SMS.

In-house lawyers should involve IT colleagues to find the best technical solutions in this respect. One or two steps to opt out should be appropriate, but anything more could be viewed as excessive, e.g., individuals should not have to justify opting out or have to log into their account to opt out.

The harder the opt-out process, the more likely that an individual will get annoyed and complain to a regulator. For example, in June last year, the French regulator fined a French electricity and gas producer and supplier €1 million ($1.07 million) for not giving customers the opportunity to opt out of marketing calls.[5]

In the Italian case, the utility company was also fined for not providing individuals with a direct, simplified procedure to opt out of promotional campaigns.

8. Opt-Out Lists

In-house lawyers should check with their marketing teams to make sure they have a reliable and accurate internal process for separating out individuals who ask to be removed from an organization's marketing activities.

If an individual's contact details are deleted but are not noted on the internal suppression list, i.e., the list containing individuals who do not want to receive marketing, there is a risk that the individual may be contacted again in the future as there will be no record of their original opt-out request. Only a minimum amount of personal information should be retained for this purpose.[6]

In-house lawyers should also train their marketing teams to regularly check national do-not-contact lists, sometimes referred to as "Robinson lists," to see which individuals have opted out of being contacted by all organizations sending a certain type of marketing, e.g., phone marketing.

If it acts against someone's wishes, an organization would be in violation of marketing laws and the GDPR. It is important to remember that a regulatory investigation can often be triggered by just one unwanted piece of marketing that arrives at the wrong time and annoys the recipient who then complains to their regulator.[7]

9. Purchasing Marketing Lists

Marketing lists can be seen as a shortcut to reaching a wide audience, and purchasing the lists is not an issue by itself. However, such lists come with their own set of challenges and risks. As part of any marketing guidelines, organizations should check the source and how accurate the information is on a marketing list prior to purchase.

If any red flags come up as part of such due diligence, the legal department should be

consulted before proceeding. An organization can only contact individuals on these lists if the individuals have given specific consent to receiving marketing from that organization.

Furthermore, marketing teams should know to include their in-house lawyers in contractual negotiations with the vendors that are supplying the lists. In-house lawyers should seek to include appropriate contractual warranties in their contracts, confirming that the vendor has obtained the correct type of consent that will allow the organization to reuse the contact details on that list.

Organizations may also want to include audit rights if they are receiving marketing lists on a regular basis from a vendor, so they can check if the vendor has complied with applicable laws.

10. Change Is Coming

The EU Privacy Regulation is on its way to becoming law in the EU, and many organizations are waiting with bated breath to see how it will impact their marketing efforts, particularly with regard to other electronic communications, such as cookies and voice over internet protocol platforms.

Negotiations are ongoing, making it unlikely that we will see anything finalized over the coming months, and there will likely be a transitional period in any event. Nevertheless, organizations should remain vigilant while the EU Privacy Regulation evolves, so they are ready to act once the new rules take effect.

Alja Poler De Zwart is a partner and Mercedes Samavi is an associate at Morrison Foerster LLP.

[1] The Privacy and Electronic Communications (Amendment) Regulations 2018 2018/1189.

[2] Telecommunication Sector (Undesirable Control) Act 2020.

[3] [2023] UKFTT 00132 (GRC). Experian" rel="noopener noreferrer" target="_blank">https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i3176/Experian Limited EA-2020-0317 FP (17.02.23).pdf.

[4] The Garante's decision is availablehere, in Italian. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9856345.

[5] The CNIL's press release on its decision is available here, in English. https://www.cnil.fr/en/commercial-prospecting-and-personal-rights-totalenergies-fined-1-million-euros.

[6] Interestingly, the Danish data protection regulator rebuked an online marketing solutions provider in September 2022 for its suppression list, on the grounds that it

amounted to unnecessary processing of personal information. This view, however, has not been shared by any other
regulator. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/smartresponses-behandling-af-personoplysninger-i-forbindelse-med-udbud-af-internetkonkurrencer.

[7] Note that the CNIL decision mentioned above was started by only 27 complaints.