ePrivacy Regulation Paused - What does this mean for businesses?

Author: Steven Roberts, Chartered Director, Certified Data Protection Officer and a Fellow of the chartered Institute of Marketing. He is Vice Chair of The Compliance Institute's Data Protection & Information Security Working Group and Group Head of Marketing at Griffith College.

The EU published its schedule of work for the year on the 11th February 2025[1]. A notable entry was the decision to pause work on the development of the proposed ePrivacy Regulation. Key to this was the lack of any foreseeable agreement, alongside the view that the proposal was outdated due to recent technological and legislative changes. In this article, we will look at the background and rationale behind the original proposal, and what its pausing means for Irish businesses in 2025.

The Original Directive

The original ePrivacy Directive (2002/58/EC) was introduced back in 2002 as the EU sought to respond to privacy concerns in the early days of email and the internet. The Directive intended to ensure the privacy rights of EU citizens were secure in the context of online communications and applied to both personal and non-personal data. It is often referred to as the 'Cookie Law', due to a subsequent update in 2009[2] which led to the introduction of cookie banners on websites[3].

In Ireland, the Directive was introduced into law in 2011 via statutory instrument SI 336[4], 'to provide for data protection and privacy connected with electronic communications networks and services and to enhance the security and reliability of such networks and services'. Known, somewhat confusingly, as the ePrivacy Regulations, the DPC is the designated supervisory authority in Ireland.

Proposal for a New Regulation

The EU's ePrivacy Regulation was first proposed by the European Commission in January 2017. Commentators and legislators viewed the Directive as being significantly outdated; it failed to reflect the privacy challenges presented by modern digital communications technologies.

The introduction of the GDPR in May 2018 created further impetus. The ePrivacy Directive is a lex specialis in the context of the GDPR. This means that where personal data processing takes place in the context of electronic communications, the ePrivacy Directive has primacy[5]. Recital 173[6] of the GDPR notes the Regulation should 'apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC'.

Compliance Challenges

One of the key issues for businesses, providing momentum to the proposed ePrivacy Regulation, was the lack of consistent application of the Directive across EU countries. Whilst a Regulation is binding and must be transposed in its entirety directly into national law, a Directive leaves local lawmakers to devise their own laws based on the goals intended to be achieved.

Significant variations of interpretation had emerged across the EU. For Irish businesses trading across the Union, this resulted in a myriad of local laws and nuances that had to be taken into account.

An example is the lack of consistency in what constitutes consent on the part of a website user. Under the Directive, a user must give their consent before any non-essential cookies or tracking technologies can be activated[7]. In Spain, data protection authorities considered this threshold could be met by scrolling a page or clicking on a link had taken place. French, UK and German authorities took a different view, deeming such actions to be insufficient. Similarly, these four jurisdictions demonstrated variances regarding consent for analytics cookies, and on the overall lifespan and retention periods for cookie consent.

Authorities appeared unclear as to whether cookies needed to achieve the same bar as for consent under GDPR; namely that it must be a clear, affirmative act, freely given, specific, informed, and unambiguous. A range of guidelines and guidance were issued, including by Ireland's Data Protection Commission [8]. While often helpful at a national level, these did not deliver a consistent EU-wide approach.

There were differing interpretations around business-to-business (B2B) electronic communications. Countries such as The Netherlands[9] treated business and personal emails in a similar manner, with the former (save for some exemptions) also needing opt-in consent before marketing communications could be sent. In Ireland[10] and the UK, by comparison, a slightly less stringent approach was taken, with B2B e-direct marketing activity tending to operate on an opt-out basis.

Fines

Non-compliance with ePrivacy cookie requirements has resulted in substantial penalties. The French supervisory authority, CNIL, imposed a €150 million fine on Google in January 2022, finding the company to have used misleading cookie consent and dark patterns[11]. Rejecting non-essential cookies was found to be more difficult than accepting them.

Whilst not at the same eye-watering levels, the Data Protection Commission regularly issues fines to Irish-based companies for non-compliant e-direct marketing practices that fall under the e-privacy laws. Many of these breaches result from a failure to comply with the 'general rule' around electronic marketing. Namely, that such activity requires the affirmative consent of the recipient. Even where the firm has the individual's consent, this may be withdrawn at any time; consumers also have the right to object to such marketing under Article 21 of the GDPR.

Commissioner Des Hogan was clear in the requirements placed on Irish companies to comply with these laws, stating:

> **"Those engaged in electronic marketing activities should take note of the consequences, which may arise if they breach the regulations. It is critical that before they embark on electronic marketing campaigns, companies carry out robust testing and checks with their service providers to ensure that they have valid and up-to-date consent of the individuals on their marketing lists and that their opt-out mechanisms are fully functional[12]."**

Guidance for Irish Businesses

For Irish companies faced with a plethora of new legislation in areas such as AI, data governance and digital services, it is key they continue to devote sufficient time to ensuring their business remains compliant with ePrivacy laws.

Effective website cookie consent tools, the provision of an unsubscribe option on all e-marketing communications, the use of customer relationship management platforms with built-in privacy features, and regular auditing of consumer databases are just some of the actions that businesses can take. Data Protection Impact Assessments (DPIAs) should also be used, even where not mandatory under GDPR, as a best practice mechanism for identifying potential risks and mitigants when considering new online communications platforms or tools that involve processing of personal data.

Firms undertaking electronic direct marketing activities in Ireland should have clear policies in place and are recommended to review the DPC's Rules for Direct Electronic Marketing, which provides guidance as well as a useful FAQ section[13]. Another useful resource is the Compliance Institute's Data Protection Guide, which can be found on the Institute's website[14].

For those operating in multiple EU jurisdictions, they must continue to adhere to both the requirements of the GDPR for processing of personal data, as well as local nuances of interpretation around the current ePrivacy Directive.

It remains to be seen whether the EU Commission revisits the ePrivacy Regulation in the future. The range of legislation recently introduced and upcoming suggests the focus will remain elsewhere. For companies and their compliance teams, this may not be unwelcome news as they continue to meet the challenge of complying with these new and existing laws.

About the Author

Steven Roberts is a Chartered Director, Certified Data Protection Officer and Fellow of the Chartered Institute of Marketing. He is Vice Chair of the Compliance Institute's Data Protection & Information Security Working Group and Group Head of Marketing at Griffith College. His forthcoming book on Data Protection for Business is due for publication by Clarus Press in 2026.

REFERENCES

1. https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en
2. www.edps.europa.eu/data-protection/our-work/publications/legislation/directive-2009136ec_en
3. The DPC defines a website cookie as 'a small text file that may be stored on your computer or mobile device that contains data related to a website you visit'. The Commission provides useful guidance on cookies and tracking technologies at www.dataprotection.ie/en/dpc-guidance/guidance-cookies-and-other-tracking-technologies
4. www.irishstatutebook.ie/eli/2011/si/336/
5. The European Data Protection Board, in an opinion issued in 2019, noted that in 'situations where the ePrivacy Directive "particularises" (i.e. renders more specific) the rules of the GDPR, the (specific) provisions of the ePrivacy Directive shall, as "lex specialis", take precedence over the (more general) provisions of the GDPR'. https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf
6. https://gdpr-info.eu/recitals/no-173/
7. A detailed comparison on the different interpretations between France, Germany, the UK and Spain can be found at https://iapp.org/media/pdf/resource_center/CNIL_ICO_chart.pdf.
8. https://www.dataprotection.ie/en/dpc-guidance/guidance-cookies-and-other-tracking-technologies
9. https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-devices/advertising/digital-direct-marketing
10. The DPC provides useful guidance on B2B communications. The Commission notes that 'marketing material that is directly relevant to the role of the recipient in the context of their commercial or official activity (i.e. within their workplace) may be sent by an organisation without the prior consent of the recipient'. www.dataprotection.ie/en/pre-gdpr/case-studies#201801
11. Dark patterns are deceptive design patterns that impact a consumer's ability to exercise their privacy rights. For more information, see the EDPB's guidelines at: https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
12. https://www.dataprotection.ie/en/news-media/data-protection-commission-welcomes-outcomes-prosecutions-marketing-offences
13. https://www.dataprotection.ie/en/organisations/rules-electronic-and-direct-marketing
14. https://www.compliance.ie/Public/public/News/Data-Protection-Guide-2024.aspx