EXPLAINER

Europe's ePrivacy regulation paused

What are the implications for Third Level Institutions?

WHEN we think of data protection in Ireland, the General Data Protection Regulation or GDPR is what first comes to mind.

However, there is another EU privacy law that must be considered by Irish colleges and universities – the Privacy and Electronic Communications Directive 2002/58/EC or ePrivacy Directive for short. This is an EU law that protects the privacy of online communications, including electronic direct marketing activity.

The Directive was long viewed to be outdated, due to the rapid pace of technological change since its introduction back in 2002. The EU planned to replace it with the ePrivacy Regulation, first proposing this in 2017. It was significant, therefore, that in February of this year the EU Commission announced its decision to pause work on the development of the Regulation.

Key reasons cited were the lack of any foreseeable agreement between EU member states and a view that the proposal was now outdated due to legislative and technological changes. In this short article, we will consider the implications for Ireland's third level institutions.

ePrivacy in Ireland

In Ireland, the ePrivacy Directive is most commonly known as the 'cookie law', due to a further update in 2009 that led to the introduction of cookie consent banners on companies' websites.

The Directive was introduced into Irish law in 2011 via statutory instrument SI 336 and is known as the ePrivacy Regulations. As with GDPR, the Data Protection Commission (DPC) is Ireland's designated supervisory authority.

ePrivacy is a lex specialis with regard to the GDPR. This means that where personal data processing takes place in the context of electronic communications, the ePrivacy Directive has primacy.

Compliance challenges

The EU's ePrivacy Regulation was intended to create a standardised approach across the EU's 27 member states. With the Regulation paused, it means substantial differences of interpretation remain across EU countries.

One example is the threshold for website cookie consent. In Spain, continuing to scroll on a page or click on links is considered sufficient consent, whilst in France, Germany and the UK this is not deemed to be compliant.

Similarly, in the area of business-to-business communications, The Netherlands adopts a strict interpretation and treats communications to business emails similarly to personal email addresses. In contrast, Ireland and the UK have tended to operate on an opt-out basis.

The DPC provides useful guidance for Irish organisations, stating 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'.

Penalties and fines

Non-compliance with website cookie requirements has resulted in significant fines across the EU. For example, in 2022, France's supervisory authority fined Google and Facebook a total of €210 million for alleged breaches under the Directive.

In Ireland, the DPC has issued fines to a range of companies for breaches of ePrivacy laws, albeit at a much lower level. Many of these breaches related to non-compliance regarding e-direct marketing and a failure to adhere to the 'general rule' that such communications should always have the prior affirmative consent of the recipient.

How should Irish institutions respond?

Many institutions' marketing and compliance teams will have been keeping a watchful eye on developments around the ePrivacy Regulation. Now that it has been paused, there are a number of actions institutions can take to ensure they remain compliant with the existing Directive and SI336.

1. Review the DPC's guidelines on electronic direct marketing and on the use of cookies and online tracking technologies.
2. Where operating in other EU jurisdictions, take account of variations in local laws.
3. Ensure that all relevant personnel receive training, with regular refresher sessions.
4. Ensure all e-direct marketing communications include an unsubscribe option.
5. Regularly audit email databases to enable compliance.
6. Use a cookie consent platform to facilitate accurate, GDPR-compliant records of consent obtained and that this adheres to agreed retention timelines.
7. If undertaking business-to-business direct marketing on an opt-out basis, make sure the activity adheres to the DPC's guidance on business communications.
8. Be clear on retention timelines for all email databases.
9. Remember the data minimisation principle. Having a smaller but accurate and up-to-date database of marketing leads that are genuinely interested in receiving information about your institution is preferable to a larger database containing cold, inaccurate or redundant contacts.
10. Undertake a Data Protection Impact Assessment when considering a new online communication platform or customer relationship management system. This ensures risks are identified at the outset and appropriate mitigating actions put in place.
11. Have clear records of processing activities, ensuring the organisation can demonstrate it meets the GDPR's accountability principle.
12. If in doubt, ask your legal or data protection colleagues for advice and guidance.

Organisations that put in place clear processes, demonstrate accountability and undertake regular training for their teams regarding e-privacy requirements are best placed to ensure compliance.

By

Steven Roberts

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.