Baker McKenzie.

Regulatory Changes & Enforcement 2019/2020

Embrace the Direct Marketing Challenge

Timelines of the legal framework changes

EU General Data Protection Directive 95/46/EC	General Data Protection Regulation (GDPR)	In force (May 25, 2018)
EU Directive 2002/58/EC (ePrivacy Directive)	ePrivacy Regulation	Expected to be in force (end 2019/2020)

The requirement to obtain consent to send electronic direct marketing messages is set out in the ePrivacy Directive (implemented through local legislation, e.g. PECR in the UK), not in the GDPR. The ePrivacy Directive is due to be replaced by the ePrivacy Regulation, which is in draft and expected to come into force by the end of 2019/2020.

Although the GDPR is now in force, failure to comply with direct marketing rules for 'unsolicited communications' will remain a breach of the ePrivacy Directive, not the GDPR. As a result, fines that could be imposed for breaches are not at GDPR-level.

Financial risks for sending unsolicited communications for direct marketing purposes remains the same after 25 May 2018, as it was before. However, this will change once the new ePrivacy Regulation comes into force (expected end of 2019 / 2020).

Operational risks for direct marketing might have increased with the introduction of the GDPR.

- Non-compliance with consent requirements might be a higher regulatory priority and assessed against the 'GDPR standard' (e.g. we may see stricter interpretations of the requirements for consent to be freely given, informed, specific and unambiguous)
- Regulators might also expect the 'GDPR standard' with regard to the controller's accountability, i.e. the obligations to document and record the consent giving and withdrawal process, including audit trails.

Advised actions

Review consent language against the GDPR standard.

Ensure GDPR compliance of the direct marketing 'back-office', incl., data brokerage, profiling, segmentation, data analysis, re-targeting. Determine the appropriate legal grounds for processing (e.g. consent vs. legitimate interest); consider compatibility with the original purpose of processing; assess whether a DPIA is required.

Develop and deploy a successful consent renewal strategy

- Develop GDPR-proof consent mechanisms and methods of recording consent;
- Qualify customer leads in your CRM database, improve data quality, consider cleansing details where you don't have valid demonstrable consent to send marketing and where you cannot rely on the soft opt-in;
- Only email individuals where you are sure to have valid GDPR-proof consent or where you are confident that you can rely on the soft opt-in;
- Develop other (non-direct, 'non-electronic') communication channels for consent renewal;
- Understand the conversion rate of the electronic communication (e.g. which emails are read or acted upon);
- Learn from 'unsuccessful' renewal strategies, e.g. BT (2018), Honda (2017) and Flybe (2017), which were fined in the past (ICO, UK).