GDPR and Direct Marketing

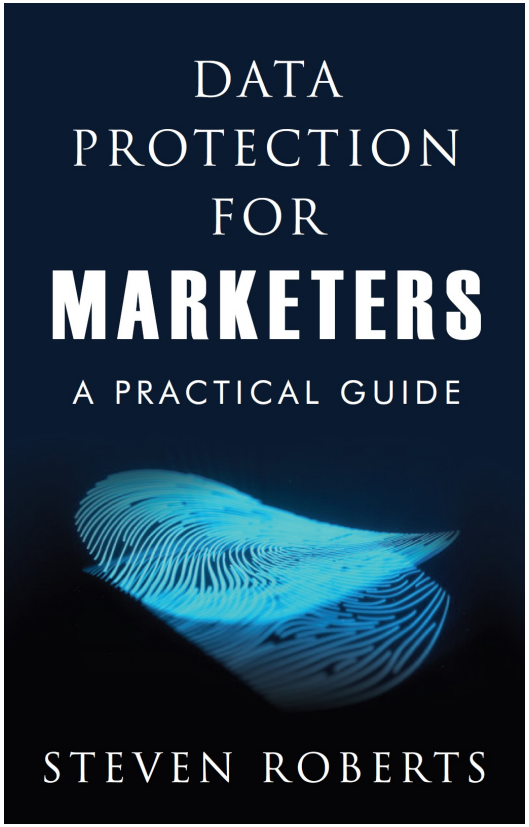
Steven Roberts FCIM CDPO
Head of Marketing & Data Protection Lead
Griffith College

Note: this presentation is for information purposes and should not be considered legal advice.

GRIFFITH COLLEGE

Bio

- Head of Marketing & Data Protection Lead, Griffith College
- Certified Data Protection Officer & Fellow of Chartered Institute of Marketing
- Vice-chair Data Protection & Information Security Working Group, ACOI
- Columnist, Marketing Magazine
- Author *Data Protection for Marketers: A Practical Guide* (Orpen Press)



GDPR – A Quick Refresher

- EU regulation which seeks to provide a common data protection framework across the European Union.
- It came into force on 25th May 2018
- Brought into Irish law via the Data Protection Act 2018.
- Provides individuals with more rights and control over their personal data.
- It significantly increases the obligations and responsibilities in how businesses collect, use and protect this data.

GDPR only applies to personal data

Personal data is "*any information relating to an identified or identifiable natural person "* (Art. 4 GDPR)

Examples:

- Email address
- Name and contact details
- Date of birth
- Internet Protocol (IP) address
- Exam scripts
- Identification card number

It can be considered personal data "**once it is clear to whom that information relates, or it is reasonably possible to find out.**" (DPC)

The 7 Principles of Data Protection

- Lawful, fair and transparent processing of data
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

The 6 Lawful Bases for Processing

- The individual has provided their **consent** – freely given, specific, unambiguous and informed
- To enter into or perform a **contract**
- A **legal obligation** (for example, relating to HR or financial records)
- In the subject's **vital interests**
- In the **public interest**
- In the **legitimate interests** of the controller or processor.
  - Requires a Legitimate Interest Assessment (LIA)
  - Assess purpose, necessity and balance of rights

Data Breaches

- Defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".*
  Article 4(12)

- The integrity, confidentiality or availability of the data has been affected in some way.

- 6,628 valid data security breaches were notified in 2020 (+10% YOY)
  (Source: DPC Annual Report 2020)

- Third highest number of data breaches in EU per 100,000 population during the period from 25th May 2018 to 27th January 2021
  (Source: DLA Piper)

- Recent fines for Tusla (x3), HSE, UCD, and Twitter

Direct Marketing Activity

- GDPR recognizes marketing as a legitimate business activity (Recital 47)
- Direct marketing must have an appropriate legal basis
- Channels can have different requirements (postal, digital, etc)
- General rule: affirmative consent required for e-direct marketing
- Must always have an opt-out / unsubscribe option

Direct Marketing Activity (cont'd)

- Customers: contact if within the past 12 months
- Digital communications to non-customers: individuals have to give their consent in advance
- https://www.dataprotection.ie/en/organisations/rules-electronic-direct-marketing
- https://www.dataprotection.ie/sites/default/files/uploads/2020-05/FAQ%20on%20Consent%20for%20Electronic%20Direct%20Marketing%20-%20April2020.pdf

Electronic Direct Marketing

- The ePrivacy Regulations implement Directive 2002/58/EC ('the ePrivacy Directive') in Irish law
- S.I. 336/2011 — European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations')
- Marketing conducted by **phone, fax, text message, and email**
- Data Protection Commission is the supervisory authority
- Fines of up to EUR5,000 per instance of a breach
- New ePrivacy Regulation delayed (website cookies)

Some Considerations

- Proximity - different channels are deemed to be more or less invasive of an individual's privacy
- Consent for e-direct marketing must meet GDPR standards
- The GDPR and Data Protection Act 2018 forbid direct marketing and micro-targeting to children
- Business to Business communications – differing interpretations (Ireland vs Germany and Netherlands)
- In all cases, e-direct marketing must include a *valid address at which the sender may be contacted.* 13(10)(c), ePrivacy Regulations

DPC Annual Report 2020 – Complaints Investigated

- 147 new complaints were investigated under S.I. No. 336 of 2011 in respect of various forms of electronic direct marketing:
  - 66 related to email marketing
  - 73 related to SMS (text message) marketing
  - 5 related to telephone marketing
  - Prosecutions were concluded against six companies

DPC Annual Report 2020 – Complaints Investigated (cont'd)

The DPC prosecuted six companies during 2020 for sending ***unsolicited text messages*** *or* ***electronic mail to customers or former customers or prospective customers*** *without their* ***consent*** *and in one case* ***without a valid address*** *to which the recipient might send a request for such communications to cease.*

(Source: DPC Annual Report 2020)

Channels

- Post:
  - Direct marketing to non-customers on edited electoral register
  - To customers as long as informed in advance and had opportunity to opt out at that time
  - Unsubscribe option must be included each time

- Mobile Phone Calls / Text / SMS:
  - Require prior consent
  - Unsubscribe option must be included each time

- Telemarketing (Landline):
  - Can contact customers, but must inform them in advance and provide opt-out at that time
  - Non-customers: check National Directory Database

Channels (Cont'd)

- Email:
  - Customers informed at point of sale, with opt-out option
  - Contact within 12 months of sale, with similar product/ service
  - Provide opt-out on each occasion
  - Continue correspondence as long as within 12 months of previous communication
  - 28 days to action an unsubscribe request
  - Non-customers: prior consent is always required

Case Study 1

- Mobile phone company
- Customer had requested to opt-out of electronic direct marketing
- Due to a technical error his preference had not been updated on the company's systems.
- Second customer's request to opt-out had been delayed due to an IT fault.
- DPC viewed these as unsolicited marketing text messages

(Source: DPC Annual Report 2020)

Case Study 2

- Insurance Firm
- Customer one: opted-out of electronic direct marketing in 2017.
- Received further emails a couple of years later, due to a ‘system issue’ which opted the person in.
- Separate complaint: Text message reminders to customers noting insurance renewal date was approaching.
- DPC deemed unsolicited marketing.

(Source: DPC Annual Report 2020)

Responsibility for GDPR?

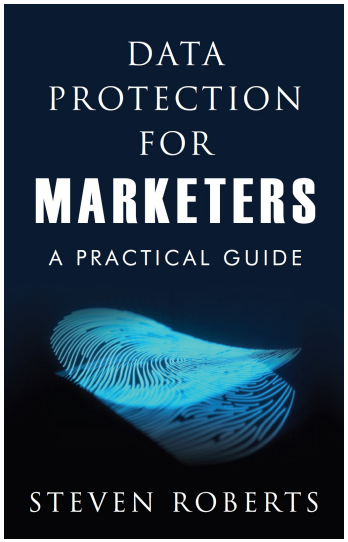
- It is the responsibility of every staff member in the company.
- Not just the Data Protection Officer (DPO), head of compliance or the board.
- Data protection sub-committee (multi-disciplinary)
- Identify ‘data champions’

The importance of training

- Most data breaches are due to human error (up to 90% according to some reports)
- You're only as compliant as your least trained team member
- Incorporate into induction programmes for new staff
- Refresher training
- Requirements for Data Protection Impact Assessment (DPIA)

Looking Ahead

- New ePrivacy Regulation – ongoing delays
- Revised Standard Contractual Clauses (SCCs)
- Supplementary measures for international data transfers
- More clarity on the level of fines
- An Adequacy Decision for the UK
- Still ‘ambiguities’ of interpretation – DPC Draft Regulatory Strategy


DATA
PROTECTION
FOR
MARKETERS
A PRACTICAL GUIDE
STEVEN ROBERTS

Thank you!