Welcome to our Webinar

General Data Protection Regulation ("GDPR")
John Mitchison
Director of Policy and Compliance
john.mitchison@dma.org.uk
EU GDPR and the future of marketing

John Mitchison
Who is the DMA?

• Largest marketing community in the UK

• Professional body to shape the future of the industry

• Over 1,000 corporate members
  – Agencies
  – Brands
  – Suppliers

• Over 16,000 marketing and communications professionals

• Self-regulating body for 1-to-1 communications
  DMA Code of Practice
DMA services

What you have access to

Research  Code  Guides  Councils  Events  Directory
DMA Awards  Pitch protection  DataSeal  Legal helpdesk  Social media helpdesk  Compliance support
Mail Preference Service  Telephone Preference Service  TPS Assured  Training
What is the EU GDPR?
Highlights

- Accountability
- Expanded definition of Personal Data
- Consent
- Legitimate Interest
- Privacy notices
- Data breach notification
- Profiling
- Data Subject Rights
- Processors responsibilities
- Larger Fines
How can I demonstrate that I comply?

• Implement technical and organisational measures that ensure and demonstrate that you comply.
  – Policies, training, audits, and reviews.

• Maintain documentation on processing activities.

• Where appropriate, appoint a data protection officer.

• Implement measures that meet the principles of data protection by design and data protection by default.
  – Data minimisation
  – Pseudonymisation
  – Transparency

• Use data protection impact assessments.
Consent

*Defined in the Regulation as*

- Freely Given
- Specific
- Informed
- Unambiguous

*Additionally*

- Unbundled
- Granular
- Named
- Documented
- Easy to withdraw
Consent

Written, including electronic or oral statement

• Includes
  – Ticking a box when visiting an internet website
  – Choosing technical settings
  – By any other statement or conduct which clearly indicates acceptance

• Does Not include
  – Silence
  – Pre- ticked boxes
  – Inactivity
Your gift will be doubled, meaning twice as far to help children like Prince.

Text FOOD to 70555 to give £3, and your gift will be doubled by The Power of Nutrition, a charitable foundation. Unicef would like to contact you by phone and SMS to tell you more about our work and how you can be part of it. By texting you consent to future phone & SMS marketing contact from Unicef. Text FOODNO 70555 to give £3 and stop future calls and texts. To discuss payment call 020 3282 7863.

Your gift will be used to support nutrition programmes in Liberia. Food provided may not be as pictured. Texts cost £3 plus 1 standard rate SMS. Unicef receives 100% of your donation. To discuss payment call 020 3282 7863. Registered Charity no. 1072812 (England & Wales) SC043677 (Scotland). Photo: ©Unicef/Maulé-ffinch. Plumpy nut photo: ©Nutriset.

FOR EVERY CHILD IN DANGER 🙁
Refreshing existing Consent

We’ll create badges, bags and t-shirts, so people can show their support.

We’ll even use the device on forms.

Make up your mind to let us stay in touch.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec et ex vel sapien tempor
rhoncus.

- By Post
- By Email
- By Phone

Your Address

Your Email

Your Number
ICO warns UK firms to respect customers’ data wishes as it fines Flybe and Honda

Date 27 March 2017
Type News

Two companies have been fined a total of £83,000 for breaking the rules about how people’s personal information should be treated when sending marketing emails.

An investigation by the Information Commissioner’s Office (ICO) found Exeter-based airline Flybe deliberately sent more than 3.3 million emails to people who had told them they didn’t want to receive marketing emails from the firm.

The emails, sent in August 2016 by Flybe, with the title ‘Are your details correct?’ advised recipients to amend any out of date information and update any marketing preferences. The email also said that by updating their preferences, people may be entered into a prize draw.
Legitimate interests

Recital 47
The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

- Do you have a relationship
- Weigh up the legitimate interest of the organisation with the rights of the consumer
- Reasonable
- Provision of unsubscribe or opt-out normally satisfies test

There are 6 legal grounds for processing data
There is no hierarchy of legal grounds – all are equally valid
Privacy Notices

• What individuals need to know?
  – Name/contact details of the data controller
  – Is the data for direct marketing purposes?
  – Third parties
  – How long will you keep the data for?
  – Data subject rights (erasure, portability, rectification etc)
  – Information about profiling

• concise, transparent, intelligible and easily accessible;
• written in clear and plain language, particularly if addressed to a child; and free of charge.

• ‘Privacy Notices Transparency and Control’ ICO Code of Practice
Facebook hit with €1.2m fine in Spain for breaking privacy laws

- The regulator found Facebook had failed to inform users how their data would be used to drive advertising.
- It accused Facebook of using "generic" and "unclear" terms in its difficult to navigate privacy policy.
Rules for B2B marketers

• The only difference between B2C and B2B marketers now is in connection with email and text marketing.

• When dealing with sole traders or partnerships, the rules governing B2C marketing will apply.

• The rules for telephone marketing and direct mail are the same for both B2B and B2C, opt-out.
Rules for B2B marketers

- For email or text marketing you do not need prior consent/opt-in from the individual. You must provide an opt-out.

- For any B2B marketing, the content must be relevant to the recipients’ job role.

- This situation will not change under GDPR. These rules come under the Privacy & Electronic Communications Regulations (PECR).
Data breach notification

• Notify the ICO without undue delay/within 72 hours
  – Do you have a robust detection framework?

• You must alert your customers too, if the breach poses a high risk to their rights and freedoms.
  – Was sensitive personal data breached?
  – What about financial information?
130 days, 1,500 notifications: Does Dutch breach rule foreshadow GDPR?
Profiling

• The more extensive or intrusive the profiling for direct marketing, the more likely it is to infringe the individual’s rights and thus not fulfil the LI processing condition

• A person can object to profiling for marketing or fundraising at any time.

• People need to be told:
  – Meaningful information about the logic involved
  – The significance and envisaged consequences of the processing
  – Sufficient information to make processing fair
Data Subject Rights

- The right to be informed
- The right of access (SAR)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.
Processor’s liability

"Processor - …a body which processes personal data on behalf of the controller."

"Controller – …a body which, alone or jointly, determines the purposes and means of processing of personal data…"

• Data protection obligations now shared between controllers and processors

• Processors subject to fines where they have not complied with obligations under Regulation or acted outside instructions of controller
ePrivacy

• Intended to be consistent with GDPR
• Correct the fragmented pattern of national laws

Issues in current draft
• Consent vs Legitimate Interests
• Definition of direct marketing
• TPS and telephone marketing
• B2B Marketing
The opportunity for business

“UK businesses should seize upon GDPR as the catalyst to transform their businesses into human-centric ones.

They should use the GDPR framework as the foundation for an authentic and transparent relationship with their customers.”
Customer engagement

75% of consumers “expect organisations to understand their individual needs”

40% stated they’d be less likely to buy from a company who sends them multiple communications that are irrelevant and don’t meet their needs

59% of said they would unsubscribe from that company’s content if the offers they receive are irrelevant to their needs and preferences

Relevancy beats personalisation:

40% are interested in a service that reminded them about upcoming birthdays and gave relevant suggestions on what to buy them. This rises to two thirds of 25-34s.
Drivers for data sharing: What entices consumers?

- Trust: 58%
- Lower prices: 30%
- Freebies: 30%
- Known brand: 25%
- Word of mouth: 20%

Source: nVision Research | Base: 912 online respondents aged 18+, GB, 2015 DMA
“I would like more control over the personal information I give companies and the way it is stored”

Source: nVision Research | Base: 912 online respondents aged 18+, GB, 2015 DMA
DMA Code: a Roadmap to Trust

Put your customer first
Value your customer, understand their needs and offer relevant products and services

Outcomes:
Customers receive a positive and transparent experience throughout their association with a company
Customers receive marketing information that is relevant to them and reflects their preferences
Customers receive prompt, efficient and courteous service
Respect privacy
Act in accordance with your customer’s expectations

Be honest and fair
Be honest, fair and transparent throughout your business

Be diligent with data
Treat your customer’s personal data with the utmost care and respect

Take responsibility
Act responsibly at all times and honour your accountability
DMA advice: GDPR checklist

4 Third party data

When buying third party data, make sure you do your due diligence. The GDPR makes you accountable and responsible for making sure the personal data you use for marketing is compliant. To be sure, give third party data suppliers rigorous checks. You should:

- Know how the list was compiled
- If an organisation withholds this information then do not use them
- Know whether the consent was recently obtained/updated
- Make sure that the third party can prove consent (see point 1)
- Ask whether data has been screened against the Telephone Preference Service and/or Mailing Preference Service. If not, you will need to screen the data.
- Make sure your organisation was specifically named when the data was collected
  - This may be a requirement in the ICO’s consent guidance so think about how you would manage it.
- See a sample of the data

Record this process so you have proof that you’ve carried out extensive due diligence of your third party data suppliers.

5 Profiling

Profiling means evaluating personal data so you can make predictions about an individual or groups. Marketing communications can then be targeted and personalised for individuals or groups.

- Tell people how and why we profile personal data but give people the chance to opt-out
- Explain how you profile an individual's personal data in your privacy notice/policy

If you process personal data via automated decision making then:

- Consent may need to be explicit - an informed opt-in like a tick box with clear copy explaining any consequences for individuals (see point 1)
- If the profiling has legal or other 'significant effect' on individuals
  - You need explicit consent
  - Undertake a privacy impact assessment to determine whether legitimate interest or consent, is the most appropriate legal basis for your profiling activities

6 Legacy data

To continue marketing to individuals on your database, you must make sure that data is GDPR compliant. You will have to satisfy the requirements mentioned in the consent, legitimate interests and information provision sections of this checklist above.

As long as the data you use is GDPR compliant then the ICO will have confirmed that the data can be used after May 2018.

To get your legacy data GDPR compliant:

- Demonstrate to individuals why you have collected their data
- Say this in clear and concise language appropriate for your target audience
- Give individuals the chance to object to the processing of their data
- Because you should be able to demonstrate compliance with GDPR, you should record your legal grounds for processing an individual’s personal data
What you can do now

- Raise awareness within your organisation
- Examine your data flows and technology
- Find out your legal basis for processing personal data
- Tell people why you are collecting their data
- Always use clear and concise language
- Give people control over their personal data
- Maintain a record of the decisions you take
- Train your teams and employees
John Mitchison
Director of Policy and Compliance
john.mitchison@dma.org.uk