Are You Ready for GPDR?

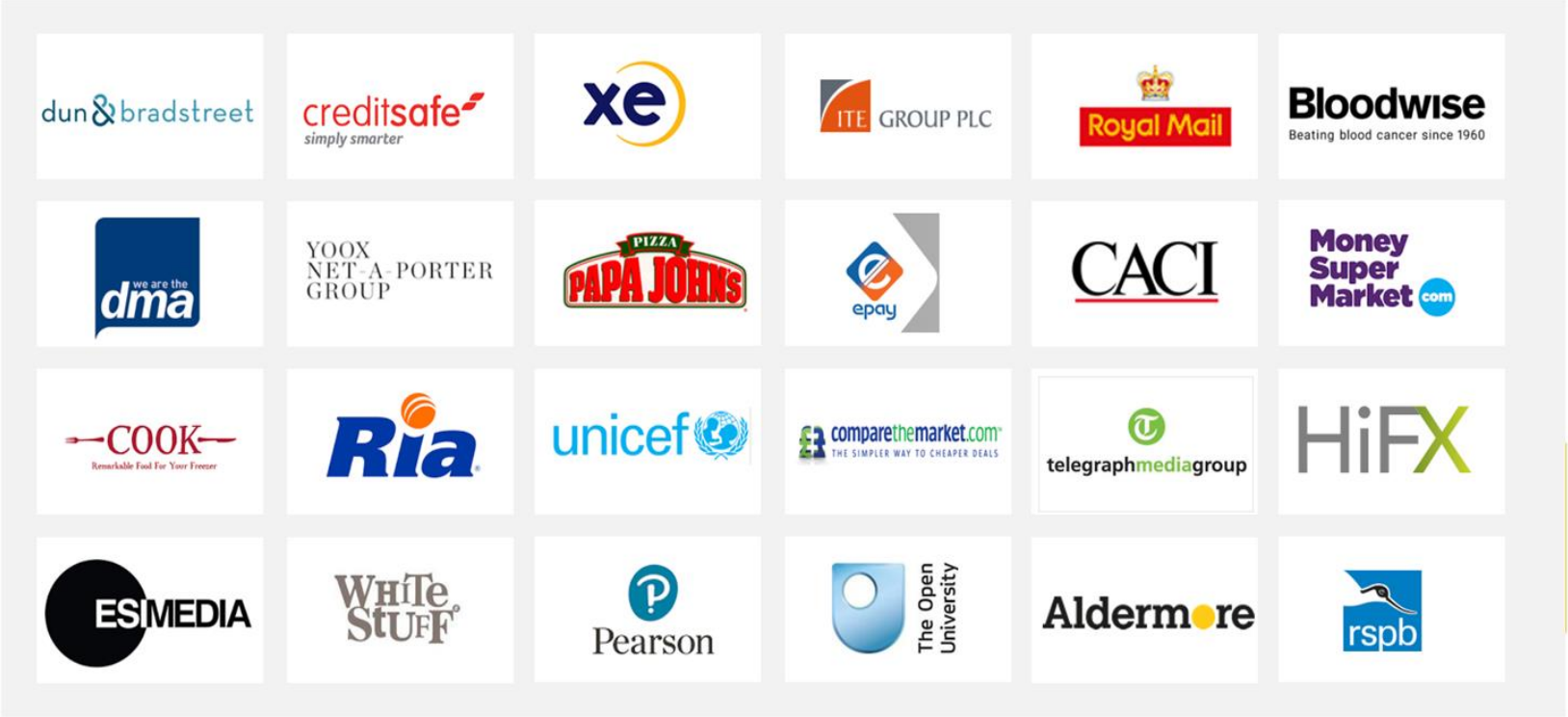
Christine Andrews

Managing Director DQM GRC

10th May 2018

DQM GRC™
CONFIDENCE IN DATA

Quick intro to DQM GRC



DQM GRC tm
CONFIDENCE IN DATA

GDPR in a nutshell

- It’s all about protecting and securing individual’s personal data (PII)
- Personal data is any data that can identify an individual – covers name, address, email, phone, IP address, mobile device etc.
- Its an EU Regulation and it applies to EU citizens **wherever their data is being processed**
- It’s aimed at replacing current EU Privacy Regulations into a One stop Shop

DQM GRC™ CONFIDENCE IN DATA

GDPR in a Nutshell – What is changing from current regulations? THE PRINCIPLES (Art 5)

- Data needs to be:
  - Processed lawfully, fairly and **in a *transparent* manner**
  - Collected for specified**, legitimate and explicit purposes (purpose limitation)**
  - Adequate, relevant and **limited to what is necessary in relation to purposes** for which it is processed (Data minimisation)
  - Accurate and where necessary kept up to date (taking steps to erase/rectify without delay)
  - Kept in a form which permits identification of data subjects for no longer than is necessary for purposes for which it is processed
  - Processed in a way which **ensures appropriate security of data**
- **The controller shall be responsible for and able to *demonstrate* compliance (*accountability*)**

DQM GRC™ CONFIDENCE IN DATA

GDPR in a nutshell – What's completely new?

- New citizens rights – wider rights of access and information
  - Whether the data is being processed
  - The source of the data
- Right to erasure of data, restrict processing, object to processing, data portability
- New controller and processor obligations
- Concept of Data Protection Impact Assessments (when there is new tech)
- Fines of 2% and 4% of global turnover

DQM GRC tm
CONFIDENCE IN DATA

Territorial Scope

- If you collect personal data or behavioural information from someone *in* an EU country, your company is subject to the requirements of the GDPR
- EU laws apply in the EU. For EU citizens outside the EU when the data is collected, the GDPR would not apply
- A financial transaction doesn't have to take place for the extended scope of the law to apply. If the organization just collects "personal data" for example as part of a marketing survey, then the data would have to be protected GDPR-style
- The organization would have to *target* a data subject in an EU country. Generic marketing doesn't count.
- Any U.S. company that has identified a market in an EU country and has localized Web content should review their Web operations.

GDPR: Main concepts for all organisations

DQM GRC™ CONFIDENCE IN DATA

Accountability

DQM GRC™
CONFIDENCE IN DATA

How do I show accountability?

Appoint a GDPR Owner

- Ensure there is someone in your organisation who understands this legislation and how it will affect the data that flows from the EEA to the USA and vice versa
- Some companies have appointed DPOs

Ensure your staff are aware

- Importance of Staff Training
- Consider specific role based training

DQM GRC™ CONFIDENCE IN DATA

Accountability: Clarity on Legal bases for Processing – Why are we processing EU residents personal data?

6 Legal Basis for Processing

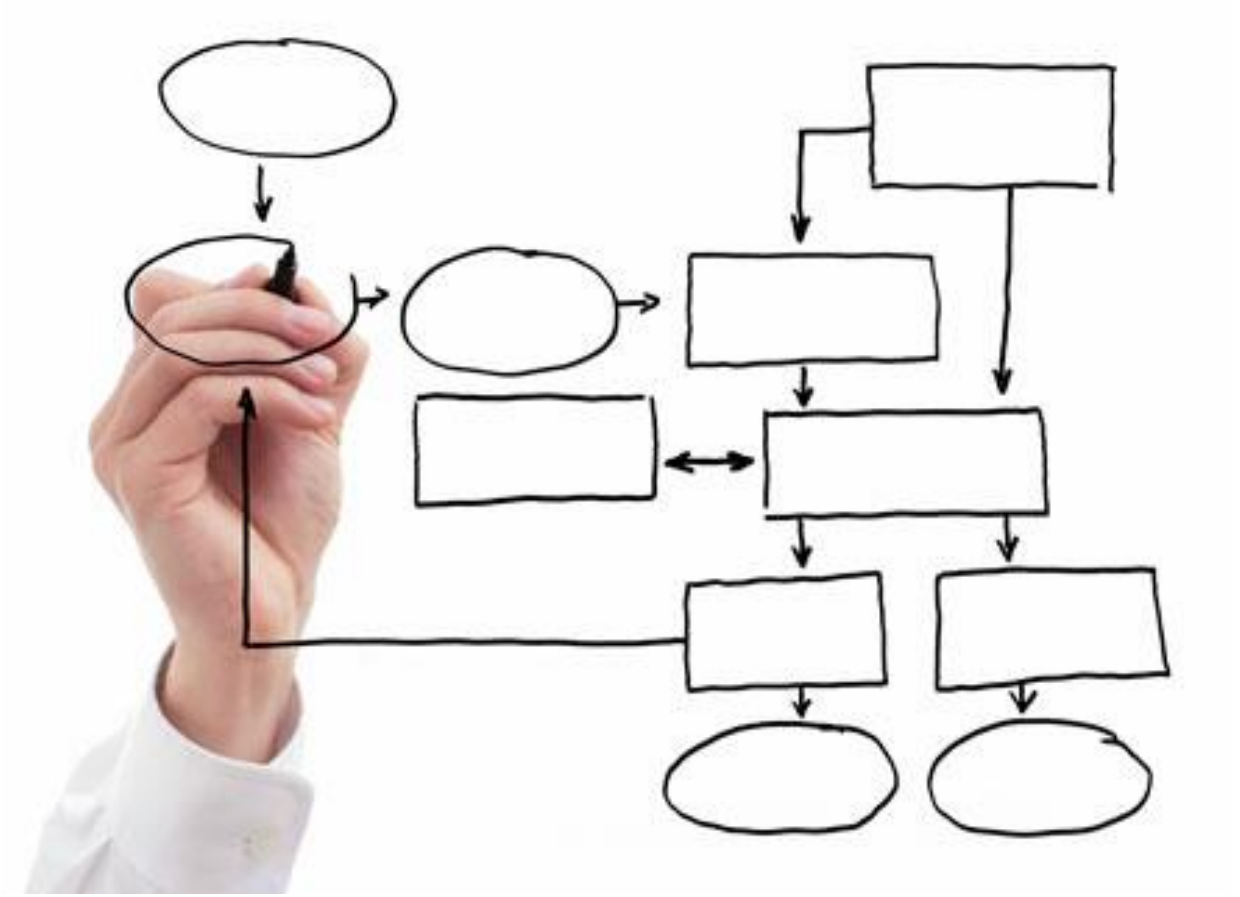
For Marketing

- As long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards, in most cases it is likely that **direct marketing is a legitimate interest**.
- ePrivacy laws do not require consent, for **communicating with existing customers** and thus legitimate interests may well be appropriate (**called soft opt in**)
- However, in the NFP sector you CAN'T use the soft opt in for fundraising emails – you must get **CONSENT.**

DQM GRC™ CONFIDENCE IN DATA

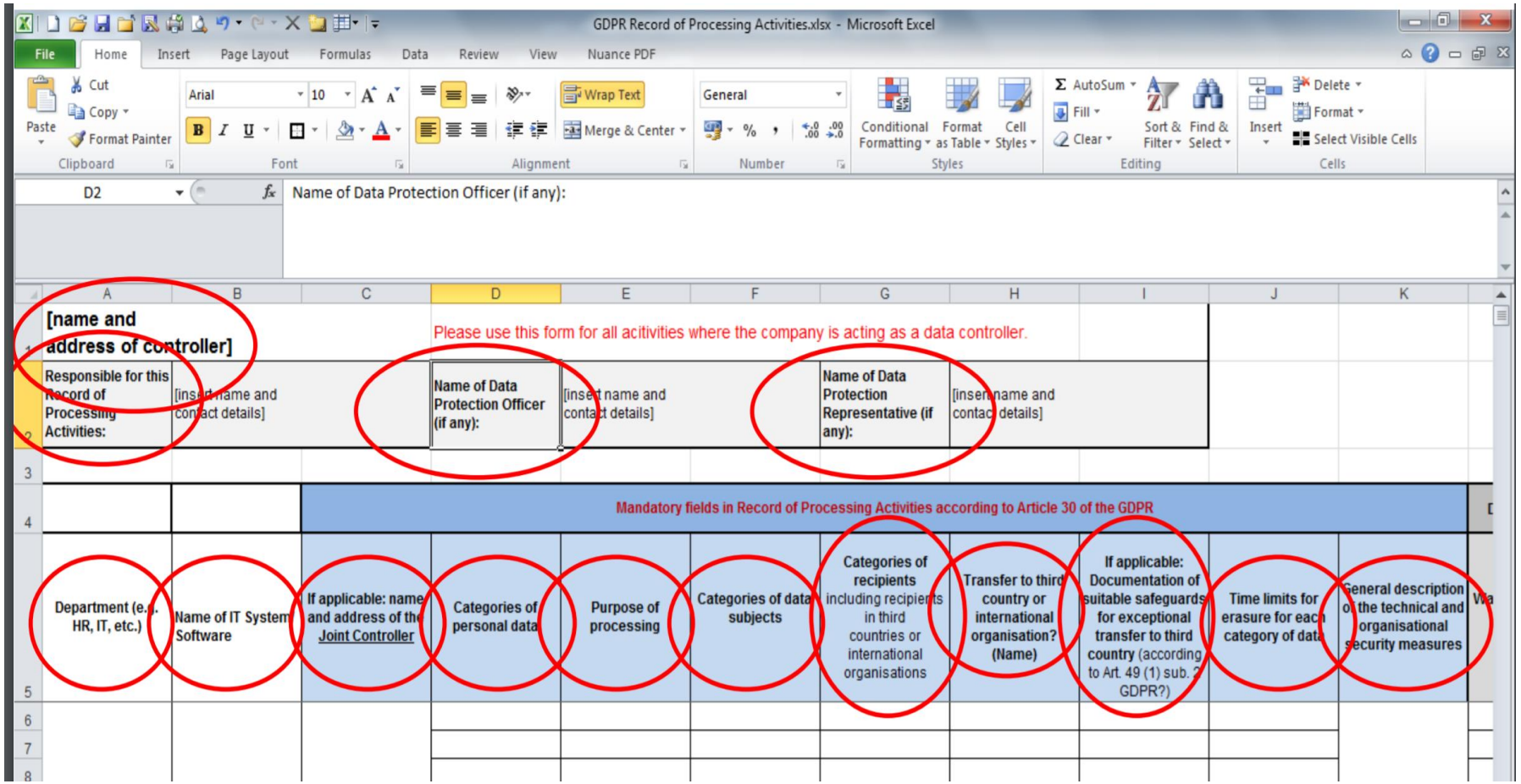
Demonstrability

Demonstrability: Understand your data flows – EEA to US



DQM GRC™ CONFIDENCE IN DATA

Demonstrability: Records of Processing (Article 30)

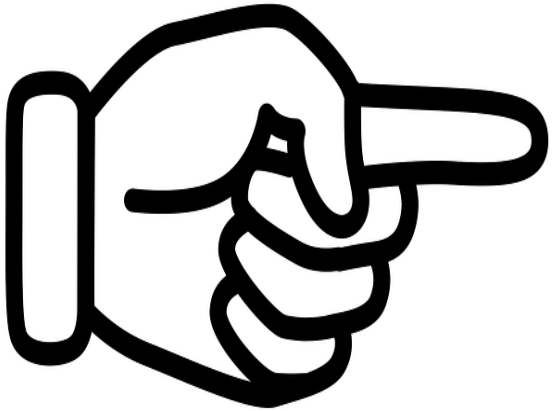


DQM GRC tm
CONFIDENCE IN DATA

Demonstrability: Documentation

DQM GRC™ CONFIDENCE IN DATA

Demonstrability: Documentation

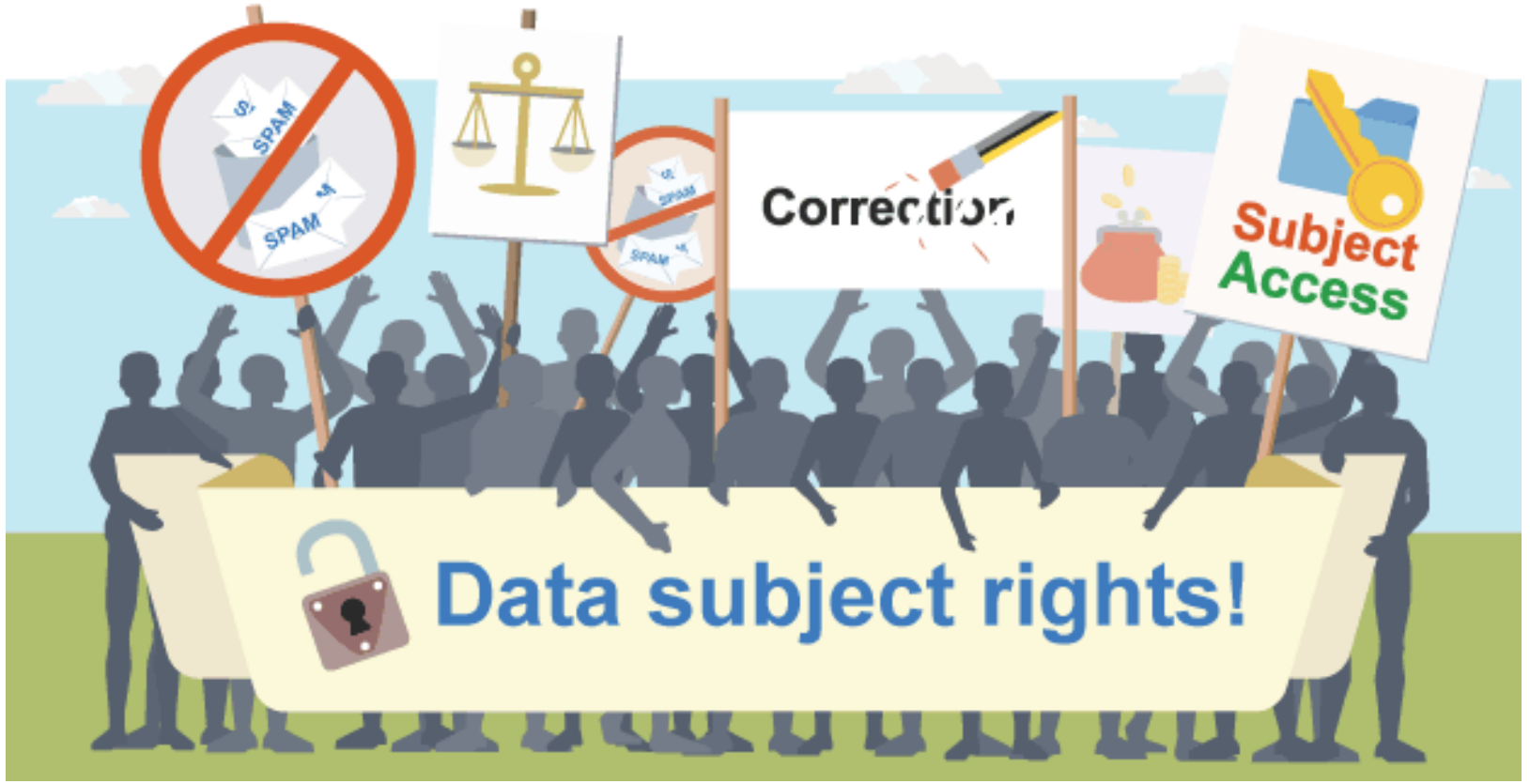


GDPR Documentation checklist
Data Protection Policy
Training Policy
Fair Processing Procedure
Subject Access Request procedure
Subject Access Request Form
Data retention policy
Data retention schedule
Privacy Impact Assessment Procedure
Breach notification Procedure
Breach notification form
Transfer of personal data outside the EEA
Marketing Consent Procedure
Removal of Consent Procedure
Managing of any sub contract Processes
Fair Process Notice
Data Protection Officer job description
Data Inventory (Information asset register)
Data Mapping Documentation
Information Classification policy and procedure
End User Access Process
Storage Removal procedure
3rd party contracts
Schedule of authorities and key suppliers
Information security policy
Managing security incidents procedure
Privacy Policy
Data erasure process
Data Portability Process

Demonstrability: Data Retention Policy. Do we keep EU citizens data in the US?

DQM GRC™
CONFIDENCE IN DATA

Demonstrability: Data Subject Rights. What do we have to provide if we have EU citizens data on our systems?



DQM GRC™
CONFIDENCE IN DATA

Demonstrability: Appropriate Data Security. Have we secured the EU citizens data we have?

Security mentioned 66 times

Safe Harbour

- U.S.-EU Safe Harbor Framework is not a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States.
- The EU-U.S. Privacy Shield Framework replaces the U.S.-EU Safe Harbor Framework.
- International transfer of data needs to be secure

DQM GRC™ CONFIDENCE IN DATA

Demonstrability: Have a Breach Notification Plan

72 hours to report if the data is unencrypted

DQM GRC™
CONFIDENCE IN DATA

Demonstrability: Know who your 3rd parties are (Processors)

DQM GRC™ CONFIDENCE IN DATA

Transparency

What are we doing with your data?

DQM GRC™
CONFIDENCE IN DATA

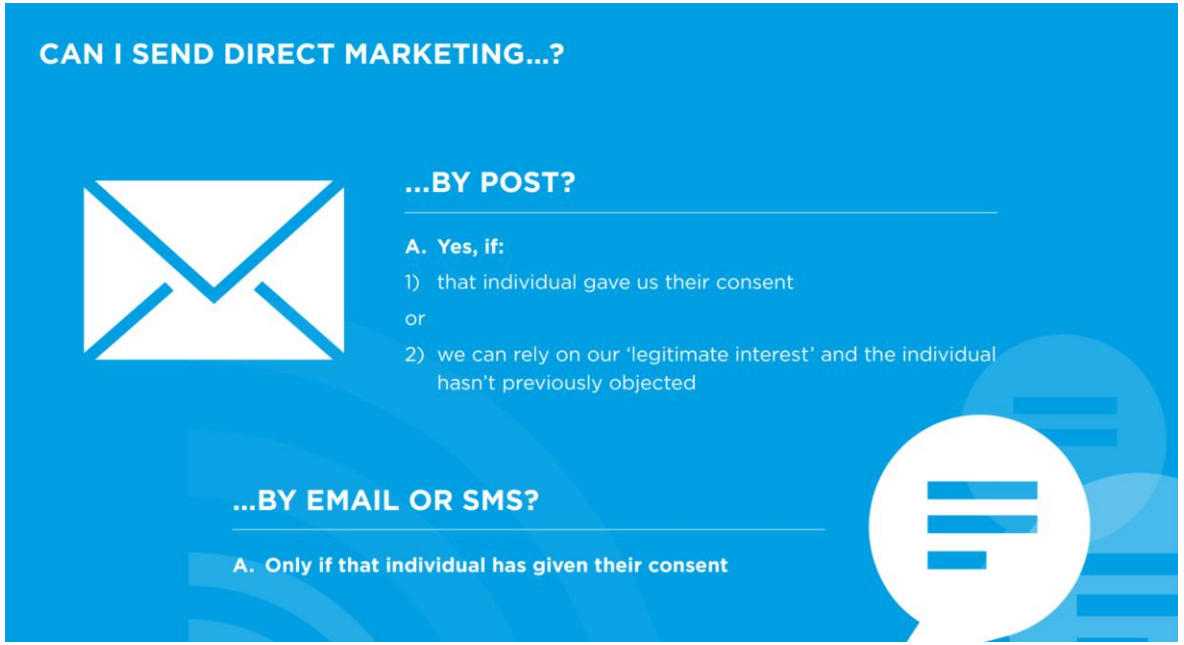
Transparency: Privacy Notice Update

Written clearly and **providing information** to the data subject at the point the data was gathered

DQM GRC™ CONFIDENCE IN DATA

GDPR: How does it affect fundraising?

https://www.institute-of-fundraising.org.uk/library/iof-gdpr-10-step-action-plan/



DQM GRC™ CONFIDENCE IN DATA

Summary of what to do now

Make sure key people are aware of the changes via workshops (1)	Document the Personal data you hold, where it came from and who you share it with (2)	Review current privacy notices and make any necessary changes (3)	Check your procedures covering individuals' rights, including deletion (4)
Update your SARs process and ensure you can respond within the new time frame (5)	Identify and document your legal bases (may be more than one) for processing. Include this in your privacy notice (6)	Review how you seek, record and manage consent. Refresh existing consents if they don't meet the GDPR standard (7)	Review security to ensure the appropriate technical and organisational measures are in place (8)
Make sure you have procedures in place to recognise and address a data breach. Do a practice run! (9)	Work out how and when you will implement Privacy by Design and PIAs in your organisation(10)	Designate a person or team to be responsible for GDPR compliance and decide whether you need a DPO (11)	If you operate in more than one EU Member State, determine your lead supervisory authority. (12)

Think how you'll handle subject access requests if EU citizens ask if you're processing their data

Check out your 3rd parties (what are they doing with the data?)

Review any cross border transfers (and be transparent in the Privacy Notice)

https://www.dqmgrc.com/gdpr-self-assessment

DQM GRC™ CONFIDENCE IN DATA