Data Protection for Charities

CFG

15 May 2014

Bates Wells Braithwaite

Overview

- Overview and key definitions
- The data protection principles
- Fair and lawful processing
- Data security and outsourcing
- Rights of data subjects
- Recent cases
- Direct marketing
- Unlocking supporter databases
- European developments

Bates Wells Braithwaite

Key areas of law

- Data Protection Act 1998
  - ICO duty to promote good practice
- Privacy and Electronic Communications Regulations 2003
  - Electronic Marketing

Bates Wells Braithwaite

… and in addition to the law …

- Relationship with clients/supporters/the public
  - Respecting them and their data
  - Preventing harm to those whose data you hold
  - Reputational issues

Bates Wells Braithwaite

Overview of data protection – Quick test

Which of the following are personal data?

- a photo of a supporter attending an event
- list of mobile numbers of people who have given text donations to your charity
- an online gift aid form completed by a donor
- an email address
- “suppressed” details of a contact
- Return envelope marked “now deceased”
- Handwritten notes about a major donor prospect

Bates Wells Braithwaite

Definition:

Personal Data

- Information about a living individual from which they are identifiable (either from that piece of information or in conjunction with other personal data held)
- Held either on a computer or in a relevant filing system
- Most physical files are exempt
- Examples: records of donors, newsletter mailing lists, staff files, details of attendees at a talk

Data controllers and data processors

Data Controller

- The organisation which determines how personal data is used must comply with the DPA
  - for instance the charity

Data Processor

- Not subject to the DPA
  - for instance fulfilment house

Bates Wells Braithwaite

Processing

- obtaining
- recording
- holding
- organising
- adapting
- amending
- destroying
- retrieving
- consulting
- using
- disclosing
- blocking
- erasing!

  – Very widely defined: anything you do with personal data

Bates Wells Braithwaite

The eight data protection principles:

1. fair and lawful processing of personal data
2. obtained only for specified and lawful purposes
3. adequate, relevant, not excessive
4. accurate and up to date
5. not to be kept longer than necessary
6. process in accordance with subject's rights
7. appropriate security measures (technical and organisational)
8. no transfer outside EEA without adequate protection

Bates Wells Braithwaite

FAIR AND LAWFUL PROCESSING

Bates Wells Braithwaite

Fair & Lawful Processing (First Principle)

Fair information requirements

- identity of the Data Controller
- purposes (e.g. organisation's general activities, specific appeals)
- including who else you will pass their details to (not including people acting on your behalf)
- any other necessary information

Applies to Personal Data held by:

- the data controller
- a trading company
- an associated local/regional branch or group
- consultants

Bates Wells Braithwaite

Fair & Lawful Processing (First Principle)

Also must fulfil a schedule 2 condition – most likely to be either:

- consent; or
- legitimate interests (balancing act);

Other rarer alternatives include:

- necessary for compliance with a legal obligation or to perform a contract; or
- Vital interests; or
- Others listed in the 1998 Act

Bates Wells Braithwaite

Sensitive Personal Data

- Includes:
  - religious or similar beliefs
  - political opinions
  - racial/ethnic origin
  - union membership
  - physical/mental condition
  - sexual life
  - alleged or actual criminal offences

  * NB : Financial information and age are personal data but NOT sensitive personal data

- Must satisfy one ordinary (sch 2) condition PLUS additional (sch 3)

  condition (see next slide – e.g. explicit consent)

Bates Wells Braithwaite

Sensitive Personal Data – Schedule 3

- obtain explicit consent unless:
- already in public domain or
- under a legal obligation in connection with employment or
- a not for profit organisation – political, philosophical, religion, trade union purposes

  PROVIDED THAT

  – safeguards for rights of data subjects are in place
  – members/regular supporters only
  – no third party disclosure without consent
- other rarely applicable alternatives

Bates Wells Braithwaite

DATA SECURITY

Bates Wells Braithwaite

Data Security – Overview

- Data security breaches
  - 1370 electronic devices stolen or lost in 3 year period to March 2014 from MPs and civil servants
  - 502 complaints made against charities a 5 year period
  - About 15% relate to security
  - 52 fines issued by the ICO. Most relate to security breaches. Highest was £325,000

- Seventh Data Protection Principle
  - Must take appropriate technical and organisational measures
  - to protect against unauthorised processing of data and against accidental loss or destruction of, or damage to, data

Bates Wells Braithwaite

Data Security – Appropriate Security Measures

- ICO's view – what is appropriate depends on circumstances
  - Risk-based approach
  - Level of security appropriate to risks presented by processing

- Security policy

- Control access to information (physical security and access)
  - Who has access to premises?
  - How is waste (including redundant computers) containing personal information disposed of?
  - Encrypt personal information which leaves the office electronically – not just password access for laptops, remote access, blackberries
    - Especially if information will cause damage or distress if lost or stolen

Bates Wells Braithwaite

Data Security – Employees

- Ensure reliability of staff having access to personal data
- Training
  - Education on importance of data security
  - Comprehensive policy and ensure staff have read and are familiar with procedures relevant to their role
  - Part of induction process?

Bates Wells Braithwaite

Data Security – Outsourcing

- When processing is carried out by data processor on behalf of data controller (e.g. fulfilment houses, PFOs, payroll processing, disposing of data), the data controller is responsible
- Data controller should ensure:
  - Sufficient guarantees in respect of their technical and organisational measures
  - Ensure compliance with those measures
  - Carried out under written contract
    - Act only on data controller's instructions
    - Complies with security obligations

Bates Wells Braithwaite

Negotiating Contracts with Partners and Suppliers

- Agreement will normally set out commercial terms
- Data controller
  - Service level specifications & security measures
  - Ensure it owns all rights created in connection with personal data and obtain assignment
  - Restrictions on overseas transfers of information by processor without data controller's written consent
  - Restrict appointment of sub-processors or enter into direct agreements with each sub-processor

Bates Wells Braithwaite

RETENTION OF PERSONAL DATA

Bates Wells Braithwaite

Retention of personal data

- Fifth principle: personal data should not be retained for any longer than necessary
- Should only be kept for as long as there is an identifiable purpose for which it need to be retained – and should then be destroyed
- ICO guidance:
  - Should review the length of time for which personal data is held, and consider the purposes for which it is held
  - Securely delete information which no longer needs to be held
- Consider having a retention policy setting out guidelines for how long different types of data should be retained
- Be aware of requirements in certain areas – e.g. HMRC requires VAT records to be kept for six years

Bates Wells Braithwaite

Case Study: British Pregnancy Advisory Service

- BPAS fined £200,000 Feb 2014
- Website attacked by hacker with anti-abortion views
- Call back details for 9,900 people
- Names, addresses, DoB, phone numbers of 9,900 people who requested call-back
- Website gave reasons why call-back could be requested, e.g. contraceptive advice, abortion, STI screening
- Ethnicity and social background could have led to serious harm and even death
- Kept call-back details for 5 years longer than was necessary
- Privacy policy gave false assurances about security and confidentiality

Bates Wells Braithwaite

How did security breach arise?

- BPAS did not realise call-back details retained on the site
- No written agreement with IT companies
- ICO found serious breach of 7th Data Protection Principle:
  - ICO - should have ensured website did not store details or that appropriate measures were in place, eg storing passwords securely
  - should have carried out appropriate security testing to show up vulnerabilities
  - should have ensured website software up-to-date
  - Unacceptable in view of very sensitive and personal services provided by BPAS
  - No agreement with IT companies

Bates Wells Braithwaite

SUBJECT'S RIGHTS

Bates Wells Braithwaite

Subjects' Rights (Sixth Principle)

- Right to request stop processing – if substantial damage
- Right to request stop processing – if direct marketing
- Automated decision-taking
- Damages/compensation
- Rectification/blocking/erasure
- Subject access requests

Bates Wells Braithwaite

Accessing Personal Data

- Access to personal data you hold about data subjects
- On request, must tell subject the information you hold about them:
  - the data
  - the purposes it is used for
  - people to whom it has or may have been disclosed
  - any automated decision making to which it is subject

Bates Wells Braithwaite

Accessing Personal Data - Subject Access Requests

- Written request
- Enough information to:
  - Identify subject
  - Enable compliance
- £10 fee
- 40 days
- Unless:
  - Not possible
  - Disproportionate effort – but IT systems search is unlikely to be disproportionate
  - Subject agrees
  - Recent compliance
  - Disclosure of third party data
  - Other exemptions

Bates Wells Braithwaite

Subject Access Requests - Disclosure of Third Party Data

- Obtain consent of the third party
- Unless otherwise reasonable to disclose having regard to:
  - Confidentiality
  - Steps to obtain consent
  - Capability of consenting
  - Express refusal

Bates Wells Braithwaite

DIRECT MARKETING

Bates Wells Braithwaite

Direct Marketing

Definition of marketing in DPA (s.11)

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals"

ICO says:

- Includes messages with some marketing elements even if not their main purpose
- Includes 'promoting an organisation's aims and ideals' i.e. promotional and campaigning activities such as encouraging supporters to attend a rally – not just selling goods or services

Bates Wells Braithwaite

Direct Marketing - Restrictions

- s11 DPA gives individuals the right to stop direct marketing
- Mailing preference service
- Telephone preference service
- Privacy and Electronic Communication Regulations 2003

NB: only limited rights to prevent other types of processing

Bates Wells Braithwaite

Summary – The Privacy & Electronic Communications Regulations 2003

- email, fax, text messaging
- no unsolicited e-marketing to “individual subscribers” unless consent
- exception: prior consent not necessary if pre-existing relationship in connection with *sale* of similar goods/services (“Soft opt-in”)

  NB: Does not apply to donations
- consent must be given to the sender/caller (ie no bought in lists unless marketing is solicited)

Bates Wells Braithwaite

Consent for e-marketing

- Positive indication of consent
- Can use opt-in or opt-out tick boxes
- Don’t have to use a tick box
- Need communication where consent indicated e.g. subscribing to service, completing “sign up” form
- If you don’t use tick box, make sure they understand giving consent
- Recent ICO guidance: need separate consents for separate types of communication (but not the law – yet!)

Bates Wells Braithwaite

Consent opt-out
Offline version

XYZ Organisation

Data Protection Act 1998

We [*and our subsidiary companies*] would like to use your information:

☐ (a) For use in connection with our activities including fundraising

☐ (b) To pass to other organisations [*with similar objects*]

Please tick the appropriate box(es) if you do not wish us to do this

Bates Wells Braithwaite

Online version – for discussion

XYZ Organisation

Data Protection Act 1998

"I want to hear from other organisations so that they can send me offers. Please pass my details onto them so that they can contact me"

Please *untick* the relevant box(es) if you do not wish us to do this

[Note: ICO good practice differs]

BWB
Bates Wells Braithwaite

Currys online collection statement

☐ Please do not send me details of products and offers from currys.co.uk

☐ Please send me details of products and offers from third party organisations recommended by currys.co.uk

Bates Wells Braithwaite

What does this mean for sharing lists?

- Technically, 3rd parties should use first person when collecting consent
- If not you wouldn't have consent to send email marketing and it would be unsolicited
- NB – does not include fulfilment houses, professional fundraisers
- Consider likelihood of complains/enforcement?
- ICO guidance
- Recent news stories regarding UCAS

Bates Wells Braithwaite

Soft opt-in – Consent not needed

- Exception: “soft opt-in” where
  - you have the person’s details from a sale/negotiations of a sale of product/service to them; AND
  - you are marketing YOUR similar products/services; AND
  - if they do not refuse then (=opt-out), you give them a simple way to do so in every future message (free of charge except cost of transmitting referral)
- The opt-out options should allow the person to reply directly to the message
- **NB does not apply to charity donations!**

Bates Wells Braithwaite

E-marketing - summary

- Need prior consent
- Given to sender
- Exception for soft-opt-in

Bates Wells Braithwaite

Electronic marketing to corporate and public bodies

- Must say who marketing is from
- Include contact details
- Consent not mandatory
- ICO recommends, as best practice, treat in same way as individual subscribers
- If emailing named person at business, they have a right under DPA to ask to stop marketing

Bates Wells Braithwaite

Postal Marketing/Direct Mail

- Use of data marketing should be consistent with their expectations
- Respond to stop requests (28 days to suppress)
- Very narrow data collection statement, e.g. “we will only use your details to process your donation” not sufficient
- Mailing Preference Service (“MPS”)
- Voluntary but good practice for fundraisers to check the list

Bates Wells Braithwaite

Summary of rules in data protection statements (1)

1. What will you use information for?
   - make wide enough to include marketing

     "*We may use your information to send you updates on campaigns and activities that we think you might be interested in*".
2. State if you will be sharing with other organisations

   e.g. corporate partners, trading subsidiary?
3. Provide a means of stopping marketing (contact details are sufficient)
4. Keep clear record of preferences e.g. "post only"

Bates Wells Braithwaite

“UNLOCKING” SUPPORTER DATABASES

Bates Wells Braithwaite

“Unlock” supporter databases

- Historical data without clear record of preferences
- May be acting unlawfully in contacting people

Contacting people by email

- PECR prohibit unsolicited marketing without consent
- “Marketing” interpreted widely
- How do you “unlock”?

Bates Wells Braithwaite

Possible solution

- Write to individuals and ask whether they'd like to receive marketing, going forward
- Silence not consent
- Should not contain marketing
- "Fact-finding exercise"
- Consider likelihood of consent
- Technical breach so there is a risk of complaints

Longer Term Solution

- Get data collection statements right from the beginning
- Model statements for organisation

Bates Wells Braithwaite

EU DEVELOPMENTS

Bates Wells Braithwaite

Draft EU Data Protection Regulation

- Still being debated within the EU institutions
- Not expected to come into effect until 2016/2017 at earliest
- Likely to be some transitional period after it comes into effect

Bates Wells Braithwaite

Draft EU Regulation – key changes

Obligations:

- Data processors will have to comply
- No longer any requirement to register with the ICO
- Mandatory requirement for data protection officer (where 250+ employees or regularly and systematically monitoring data subjects)

Direct marketing:

- Prohibition on using pre-ticked boxes and possible stronger emphasis on consent (e.g. consent for each type of medium)
- The right to be forgotten (if data subject objects to processing)

Sanctions/breaches:

- Mandatory breach notification within a certain period of becoming aware (if severely affects rights/freedoms of individuals)
- Increased fine – up to €100m or 5% annual turnover whichever is the higher

Bates Wells Braithwaite

Lawrence Simanowitz

Partner

Charity & Social Enterprise Department

Bates Wells Braithwaite

2-6 Cannon Street

London EC4M 6YH

l.simanowitz@bwbllp.com

Tel: 020 7551 7796

Bates Wells Braithwaite