Findings from ICO information risk reviews at eight charities

April 2018

Information Commissioner's Office

Introduction

The Information Commissioner's Office (the ICO) enforces and promotes compliance with the Data Protection Act 2018 (DPA), which applied from 25 May. This report was completed under the previous Data Protection Act 1998, which contained eight principles of good information handling, but we have included GDPR recommendations where long term actions were appropriate.
The Privacy and Electronic Communications Regulations (PECR) sit alongside the DPA. They give people specific privacy rights in relation to electronic communications including fundraising.

Approach

Eight charities participated in the information risk reviews, which the ICO Assurance Department conducted at the charities' head offices between December 2017 and February 2018.

This report is based on these reviews. It highlights our experience of how effective the controls in place were for the agreed scope areas, and to what extent they were embedded. It is intended to help them and others in the sector to recognise where they can make improvements in the same areas. No individual organisation is named in this report.

In addition, we also compared the findings with those from 25 advisory visits (AVs) carried out at smaller charities during 2017/18. Whilst these were generally smaller charities and not part of the project, we discovered correlations in our findings where the scope areas overlapped. This was largely to do with records management and training, and is noted where this is the case.

Typical processing of personal data by charities

Charities process both paper and electronic records relating to staff, service users, volunteers, supporters, members and major donors. The majority of personal data is processed for fundraising purposes.

The charities involved process a limited amount of sensitive personal data as defined by the DPA, including staff sickness records and sometimes donor or service user information relating to health and receipt of benefits. Some charities also process information relating to children and vulnerable people.

Personal information is either held electronically in computer databases or manually in filing cabinets.

Areas of good practice

During this project many examples of good practice were seen including:

- ✓ All charities had clear governance structures in place with delegated responsibility from the board down.

- ✓ In order to comply with GDPR all charities taking part had either already appointed Data Protection Officers (DPO), or work was underway to appoint one. In some cases the charity had delegated joint responsibility for information governance (IG) to two senior members of staff.

- ✓ Either GDPR or IG working groups were in place although not all of these had been formalised. There were programmes of work in place in preparation for GDPR although these were not always documented. We advised that these groups be formalised in order to ensure corporate oversight of IG going forward and programmes of work should be documented and progress reported on to make them more effective.

- ✓ Data audits to establish what data is held and how it flows into and out of the organisation were already underway, with a small number already completed. It is a requirement of GDPR for larger organisations to keep a record of processing activity.

- ✓ Half the charities ensured all policies were signed off by either senior management and/or the board.

- ✓ One charity had mapped their compliance against GDPR and any non-compliance risks were documented and reported the IG group.

- ✓ We saw two good examples of measures to assess Data Protection (DP) compliance: one had linked IG compliance to business assurance processes, and another had their DP champions report on DP compliance for each business area as well as including IG in their internal audit programme.

- ✓ The majority of charities were reviewing their training content and delivery for GDPR or had already done so. Whilst all provide some level of DP training at induction, they were using GDPR as an opportunity to introduce more robust mandatory training programmes. One charity demonstrated outstanding practise by incorporating DP issues raised by staff, and lessons learnt from

potential/actual incidents into their training content. They also had the highest completion rate for training of both staff and volunteers.

- ✓ Most charities had moved to an opt-in approach to consent for marketing. Of these, most were also using opt-in for postal marketing with the rest relying on legitimate interests for postal marketing. Consent was granular, providing separate check-boxes for each type of communication, ie phone, email, sms.

- ✓ Two charities had specific consent requirements for children. One required parental consent for use of data where under 16s or under 18s were volunteering. Another asked if someone was under 18 on their online donation form, and subsequently did not use their information for marketing purposes.

- ✓ All consent was recorded on supporter databases/customer relationship marketing (CRM) systems along with an audit trail demonstrating how and when consent was given. This often included a reference to the relevant marketing campaign and fair processing information provided, as well as a copy of the relevant consent form.

- ✓ Supporter contact preferences were managed effectively. Any requested changes or section 11 notices were actioned without delay and reflected quickly on the CRM systems. Prior to carrying out any marketing activity, all the charities screened against their own suppression lists, as well as appropriate Telephone Preference Service, Fundraising Preference Service and Royal Mail 'gone-away' lists. If necessary they subsequently updated their supporter databases to prevent future unwanted marketing activity.

- ✓ All the charities had a privacy policy/statement on their website explaining how personal information will be collected and used by them. Some had already been updated to comply with GDPR.

- ✓ None of the charities share personal data with other organisations for marketing purposes.

- ✓ Most charities have appropriate systems in place for destruction of confidential waste, using a combination of locally provided cross-cut shredders and/or third-party shredding companies for disposal of bulk confidential waste paper. Destruction certificates are obtained from these providers.

- ✓ Three charities had already drafted procedures to deal with requests under the new 'right to erasure' required by the GDPR. Others intended to draft procedures and include the right in their privacy policy.

Areas for improvement

Governance

- ➔ Not all the charities we visited had documented IG arrangements included in their overall governance framework.

- ➔ At the charities we visited, KPIs for IG were either not in place at all, or were limited as to what they covered.

Policies & procedures

- ➔ Not all charities we visited had key IG policies in place. Policies were inconsistent in format and version control and not all contained a document control table. Only a few charities had a policy management framework that detailed how policies should look and what approval process should be followed. Not all policies were reviewed regularly and only a few had a documented review schedule in place.

- ➔ Communication of policies to staff and volunteers was inconsistent. At least half the charities had no requirement for staff to read IG policies as part of their induction and sign to say they have read and understood them; and there was generally no strategy or formalised approach to disseminating or raising awareness of new/revised policies and procedures.

Monitoring & reporting

- ➔ The majority of charities we visited did not undertake any routine data protection or direct marketing policy compliance checks or include it in their internal audit programme.

- ➔ Compliance checks on data processors were also inconsistent with only three carrying out routine checks.

Training

- Most charities did not provided annual refresher training and staff and volunteers often don't receive any data protection training before being allowed to access or process personal data. In some cases it can be up to six months. Few provided specialist training or carried out a training needs analysis to assess training requirements of roles/individuals. Training was not always monitored effectively, especially volunteer training. This was mirrored in the findings of the advisory visits to charities where 19/25 charities had no induction or refresher training which included staff *and* volunteers.

Consent, fair processing and data sharing

- Only two charities we visited had a consistent and co-ordinated approach to fair processing notices (FPNs) provided on consent forms. Most did not have a log of FPNs or any kind of sign-off process and as a result they varied in content and quality.

- Some consent forms did not contain any fair processing statement at all which means consent is not valid as the individual has not been fully informed. Not all were linked to the charity's main privacy policy and none required an individual to confirm they had read the policy prior to giving consent.

- Most charities visited were in the early stages of developing their privacy impact assessment (PIA) process and still developing policy and procedures. Only two were carrying out PIAs routinely and only one of those had a register of PIAs. They were not necessarily carried out for new contracts with data processors.

- Most charities used data processors to carry out certain tasks, however, there were not always contracts in place or contracts were not adequate and did not include relevant DP clauses.

Business continuity

- Not all charities we visited had overarching business continuity plans in place. Those plans that were in place did not necessarily identify critical systems and were not always routinely tested.

Case study – business continuity

One charity had an emergency response plan in place which identified critical records for continued functioning in the event of a disaster. A number of 'emergency boxes' are kept – one on each floor of the main building and another in an off-site location. These contain a copy of the plan and other useful emergency equipment such as multi-chargers. The plan is tested annually against a possible scenario.

Incident reporting

- Whilst there was mostly good awareness among staff of how to report an incident and who to report it to; most charities visited did not have documented reporting procedures in place.
- Half the charities visited did not have an incident log, and those that were in place were not always comprehensive or used consistently.
- The majority do not rate risk associated with a breach as part of the investigation. This means there is no considered way of knowing when to escalate risks to the relevant risk register to ensure corporate oversight, or report them to the ICO.

The AV findings show 15/25 charities did not have a formally documented incident reporting procedure or mechanism.

Case study – incident reporting

One charity analysed reported incidents and near misses and incorporated lessons learned into their data protection training.

Retention and disposal

- The majority of charities we visited were retaining personal data for far longer than was necessary, in some cases indefinitely. Some of this was due to poor records management, and some due to retaining data in case it may be useful in the future (for example, to trace a legacy gift to a previous supporter.)

- Not all charities visited had retention and disposal documented in either a retention, confidential waste, or records management policy.

- In most cases the retention and disposal of records was not being actively managed, and in nobody had been allocated specific responsibility for weeding and disposing of records.

- In some cases IT systems did not allow for permanent deletion of records. As well as resulting in them keeping records for longer than is necessary, this also means these charities will not be able to comply with an individual's 'right to erasure' under GDPR.

- Where third party confidential waste companies were used, contracts were not always in place. Where contracts did exist, they did not always include the right for the charity to carry out compliance checks, and there was no record of any such checks being carried out on third party providers. This was mirrored by the findings of the charity AVs.

- Most did not keep any kind of information disposal log to record what information had been deleted in line with the retention schedule.

The AVs show that 16/25 charities visited do not have retention schedules in place, or were not adhering to them.