

PULSE

Quarterly Newsletter of Deloitte's Charities and Not for Profit Group



Welcome to our Autumn edition of Pulse.

As you will be aware, the new SORPs have arrived and charities have already begun to consider the potential areas of change. It will take a couple of years or so for implementation to kick in and therefore for any problem areas to emerge. The Charity Commission is seeking new members for its SORP Committee, possibly in anticipation of future technical issues of implementation.

The area of data protection is of huge importance, particularly to charities as they tend to hold personal information about donors. We have a couple of very interesting articles on this subject in this edition. Another area that has attracted a lot of attention in the press is that of cyber security. In this edition, we interview one of our specialists to find out how cyber security affects charities. We also have a very interesting article on raising finance in the sector as well as an update on the publication of the new SORPs.

Please note that the views expressed in this publication are those of the authors and not of Deloitte. In the complicated environment we all operate, always seek professional advice specifically and don't rely on contents of articles that have been written for general guidance only.

Reza Motazed

Partner

Head of Charities and Not for Profit
Deloitte LLP



Reza Motazed
Partner
rmotazed@deloitte.co.uk



Paul Simpkins
Director of Act Now Training
www.actnow.org.uk

Data protection for Charities

If you're running a charity you're probably wondering what all the fuss is about Data Protection? It's something you've heard of and it's something you'll sort out one of these days but it's not yet a priority for many.

Two recent cases may change your view...

A social care charity has been fined £70,000 after confidential reports about four children went missing when left outside a house in London. A social worker trying to deliver the files to the children's prospective adoptive parents left them at the side of the property in December. An Information Commissioner's Office inquiry found Norwood Ravenswood Ltd had not fully trained its employee.

The Information Commissioner's Office has imposed a penalty of £200,000 on the British Pregnancy Advice Service for exposing thousands of personal details to a malicious hacker.

So it is a priority and there are repercussions. And when something happens it invariably ends up in the public domain. Your reputation is in tatters and your customers lose confidence in you.

So how do charities address Data Protection?

First of all your organisation needs to accept that it's the law of the land. Data Protection has been enshrined in legislation for 30 years and every organisation in the UK, public or private, that handles data about people has to do something. The Act contains criminal offences which can be tried in court as well as other sanctions such as fines. Ignorance of the law is no excuse.

So find out what it means for you. There are a variety of ways to do this. Books exist, training courses exist online and face-to-face; Consultants, Accountancy firms and legal firms will advise you on what to do and some will charge you for the privilege. In this article we'll highlight a few of the big issues.

The starting point should be to give the job to someone – preferably in the management team of your organisation

It's not necessarily a full time job but someone needs to keep up-to-date and put a few measures in place! This person needs to learn the language of Data Protection and be prepared to talk to the media if there is a breach of the Act. The last thing you want to say when a News at Ten microphone is shoved into your face is "er...what Act?"

This person needs to acquire enough expertise to ensure the organisation complies with the Act and demonstrates its compliance to its staff and customers (and the world in general).

Compliance starts with telling the regulator (The Information Commissioner) that you process personal data. It's an easy process – most of it can be done online – and after filling in an online form designed for you and paying a fee you will have notified the regulator of the fact that you are a data controller and in return the regulator will allocate you a unique number. All charities pay the same fee of £35 a year. Doing this tells people you know about the Act. You can use this number in your literature and on your website. It's also a criminal offence to process personal data without notifying the regulator. There are some exemptions from this process for some small organisations. The regulator will advise you on this or you can read a guidance note on the website. (<http://www.ico.org.uk>)

The next job is to tell your staff and your customers/clients about your data protection practice

First staff: all you need to do is train them so they know what the act says and what it means for them. If you don't feel adequately resourced to do this yourself there are specialist training companies who can help. Most staff only need a short session, preferably at induction, so they understand the basics and know when to check with the corporate expert (that's the person who got the DP job a few paragraphs ago). It's also worth giving your staff some literature about the Act and a list of "dos and don'ts" particularly about security and disclosure of personal data. The great challenge is not losing personal data and there have been over 50 fines issued over the last few years for organisations behaving badly and managing to lose data, usually on unencrypted laptops or USB sticks (and often on trains and in public houses). Stress to your staff that the organisation's data is one of your most important assets and it has to be looked after properly. It may be also worthwhile developing policies for working from home, secure transfer of data, mobile computing and also use of social media.

Telling your customers isn't too difficult either. You develop a Privacy Policy (or a DP policy) which tells them what data you collect from them, why you process it, who you share it with and maybe a few other items such as how long you will keep it. Examples can be found on the web or a specialist can help draft one for you. This policy needs to go on your website and copies need to be held in your organisation so if anyone asks about your data handling procedures you have something ready to give them. If ever you work in partnership with another organisation they may ask if you "Do Data Protection". If you can supply them with all these things they should realise you know what you're doing in this area.

Now you're doing well. You told everyone you know about the Act, you're compliant, your staff are trained and you have a policy on how you manage personal data.

What can go wrong?

There are a few potholes along the data protection highway that may cause you a few problems. The first is the unexpected request for personal data from someone who appears to be entitled to it such as a tax inspector, a policeman, a man in a suit who looks important or a private investigator looking into a messy divorce. Take care! Just because they look impressive doesn't mean that they can access data about your staff or clients. If you receive such a request make sure you ask for the request in writing. Never supply information over the phone or at the reception desk, ask for the request in writing. This simple tactic may put off someone who knew he wasn't entitled to the data but was trying it on. If they persist and produce something in writing share it with your line manager or your DP expert and make a decision as to whether they are entitled to it. There are some exemptions for Police, Tax etc. but staff need to take advice before applying exemptions.

The other area that may cause problems is when someone exercises their rights under the Act. This is the Act that allows people to object to marketing such as junk mail, junk phone calls etc. They also have the right to see any files you hold about them. This is called Subject Access. So, if someone mentions Data Protection and their rights, make a note of their request and make sure you understand what you have to do. Your DP expert should be your initial port of call again. Most of these rights have deadlines and procedures to follow and not doing so may lead to complaints about your organisation.

If you understand the Act, it's not too difficult to comply with the law and do Data Protection properly. A top level person looking after the issue; staff training and literature; policies on handling data; fair processing information for clients, and on websites; and you should avoid ever making a mistake and ending up in the media.

And, if you do meet that News at Ten microphone it would sound so much better if your boss stood tall and said "We are aware of the Act; We have notified the regulator of our processing; Staff have been trained; Policies, procedures and fair processing statements have been in place for years and can be viewed on our website. We are confident that we comply with the Act. We will look into this incident and if there has been a breach of the Act we will take appropriate action".

Data controllers and data processors: what is the difference?

The Information Commissioner's Office (ICO) has published updated guidance on the difference between data controllers and data processors under the Data Protection Act 1998 (the "Act"). ICO has produced this guidance because of the increasing difficulty organisations face in determining whether they or the organisations they are working with have data protection responsibility. It is important for organisations to understand their role, especially where there is a data breach.

Under the Act, it is the data controller that must exercise control over the processing and carry data protection responsibility for it. They determine the purpose for which data are processed. The data processor processes data on behalf of the data controller. The guidance acknowledges that the definitions under the Act can be difficult to translate into the complexity of modern business relationships, hence the need for updated guidance.

ICO suggests that organisations establish their roles before processing commences to ensure there are no gaps in organisations' responsibilities.

To determine whether you are a data controller you need to ascertain which organisation decides:

- to collect the personal data in the first place and the legal basis for doing so;
- which items of personal data to collect, i.e. the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply i.e. the exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

These decisions can only be taken by a data controller.

A data processor may decide:

- what IT systems or other methods to use to collect personal data;
- how to store the personal data;
- the detail of the security surrounding the personal data;
- the means used to transfer the personal data from one organisation to another;
- the means used to retrieve personal data about certain individuals;
- the method for ensuring a retention schedule is adhered to; and
- the means used to delete or dispose of the data.



Donald Taylor
Charities and not-for-profit team
Charles Russell Speechlys
LLP Solicitors
Donald.Taylor@crsblaw.com

Although these lists are not exhaustive, they illustrate that a data processor has the freedom to use their technical knowledge to decide how to carry out certain activities on the data controller's behalf. The key distinction is to determine the degree of independence that each party has in determining how and in what manner the data is processed, as well as the degree of control over the content of personal data.

The new guidance provides useful 'real life' examples of how data are processed in different scenarios, such as at a market research company, in an online retailer/third party payment provider scenario, in a client/solicitor or accountant relationship, using cloud providers or how statutory bodies deal with data. The guidance is helpful in outlining where common difficulties and misunderstandings arise and how the data controller/data processor roles can and should be determined from the outset.

See left to access the latest ICO guidance.

http://ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf



Dean Atkinson
Cyber Risk Services
Deloitte
deatkinson@deloitte.co.uk

Cyber security for Charities

Esha Malkani, a Deloitte audit assistance manager, talks to Dean Atkinson of Deloitte's Cyber Risk Services.

Could you briefly explain what Cyber security is and why it is so important for charities?

Cyber security relates to the protection of organisation's assets and differs from information security, which is mainly involved with the security of more tangible assets. More recently cyber security has broadened to include security of non-tangible assets such as a company's or charity's reputation.

Companies and charities have become and continue to become more and more dependent on the internet to improve business efficiencies, for example by making more online payments and receiving online donations. However, this also means they are exposed to a greater amount of risk, driven by attackers who consider barriers to entry are low. For example it is relatively easy to buy specialised services or buy passwords which would allow attackers to access the information they are looking for. Last year was the first year that there was a decrease in physical bank robberies but an increase in cyber-attacks: This is down to the lower risks cyber attackers face.

Charities may store considerable amounts of data related to the online donations they receive. Therefore, a charity's systems could hold a lot of personal data such as a person's name, date of birth, address and bank details. If the charity's cyber security was breached then this could damage its reputation, damaging the donors 'feel good' factor of donating which may lead them to either donate elsewhere or possibly not to donate at all.

We have worked with a large international charity looking at their cyber security control maturity. This involved looking at what their risks and threats were and what controls they have in place around these. We then calculated their residual risk and were able to close this gap by implementing a stronger controls environment. We have also been able to advise clients on the importance of training their staff to make them aware of the risks and take the relevant precautions. These principals can be applied to all charities.

What are the challenges when considering cyber and information security?

Most importantly charities must *recognise* that there are risks as they own valuable assets and their systems hold information that may be of interest to potential attackers. They need to understand that if they do not have the appropriate controls in place there could be a serious reputational damage to the charity.

The biggest challenge is securing cyber security investment. Just because you don't know you have lost something, it doesn't mean you haven't. The difficulty lies in understanding the assets, how protected you are, whether that level of controls is sufficient to stop attackers from getting in and if not then what needs to be improved. It is therefore important to work in such a way that you are able to directly link cyber security investment to business assets. Many businesses refuse to accept cyber risks as a business risk and don't end up making the right investments.

Over the years, there has been greater dependence on the internet resulting in lower barriers to entry as potential attackers have the ability to make more money with a lower risk of being caught. As people continue to increase their dependence on the internet the risks will continue to rise.

Are there any simple precautions charities should look to implement in their day-to-day running?

Yes, there are. They could refer to the Government's '10 steps to Cyber Security', which is underpinned by the SANS 20 Critical Security Controls. Although some of them are quite difficult to achieve, applying the first four could mitigate risks by up to 80%.

The two key questions a charity, or for that matter, any organisation should ask themselves are:

1. What assets and information do we have that could hurt us should we lose them?
2. What is it that we have that could make someone else rich?

Once you have got your answers, it is crucial to ensure that the controls around these assets and information are tight.

<https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets>

Raising finance: Is the bond market the right solution for your charity?

Charities often have limited resources to develop and invest in new projects and are nervous about taking on debt to help fund growth as their trustees are risk adverse. This, coupled with limited sources of growth capital to date, has restricted the amount of inward investment seen across the charitable sector. However this is set to change as new social investment products come to market which can be used to underpin growth in social activities within a charitable framework. However, you need to bear in mind that this is not without risks and needs to be properly managed.

With many charities looking to raise finance in the near future, the bond market appears an attractive option following the recent success of a number of new issues and the launch of the Retail Charity Bond platform. David McHattie, Head of Charities, Corporate Banking Barclays, you need to bear in mind that shares his experience of working on a number of bond issues for Housing Associations, where bond finance is now a major part of the funding stream.

From David McHattie, Head of Charities Corporate Banking Barclays

One area your charity might want to consider more closely, especially during this prolonged period of low interest rates, is that of the bond market. I know from previous experience of working with bond issues for Housing Associations, that they can be a viable financing option if the conditions and circumstances allow, and it would appear that an increasing number of charities are now turning to bonds to diversify their access to finance.

As with all investment options, bonds won't be suitable for everyone, but if you think you might be interested in finding out more, then the following information should help to address some of the early questions that you might have:

- **Who can issue a bond?** – Any charity that needs long term finance and that has the power to borrow. You need to be able to explain to investors what the money will be used for, and how the money will be repaid.
- **What is the term?** – Typically a maximum of 5 years. The money will arrive in one lump sum on the day of issue and be repayable again in one lump sum on the maturity date. You will need to be clear about how quickly your charity can make use of the bond proceeds as interest is payable to the bond holders whether it is used or not, hence there is a cost to raising money too far in advance.
- **Certainty of funding?** – An Investment Memorandum is prepared to sell your charity to a wide range of investors. These will typically be Foundations and private individuals. They will be attracted by the purpose of the charity and the rate of return offered. With many competing investment

ideas you must ensure you offer a competitive return to attract investors.

It may take a while to corral all the investors together, so you need to allow plenty of time, especially if the terms of your offer are a bit tight from the investor perspective. Most bonds succeed in raising the full sum required, but it is not guaranteed and can take several months from start to finish.

- **How can we make our bond more attractive?** – Charity bonds are not rated, so investors prefer secured rather than unsecured issues. A strong brand name helps with investor recognition but isn't essential if the purpose of the bond monies is very clear and has a strong social purpose. For key investors, the charity management will usually undertake a series of roadshows or investor meetings, either one on one or in small groups. This is quite time consuming, but gives an opportunity to sell the charity and deal with any investor questions directly
- **What will it cost?** – An Investment Memorandum has to be prepared to sell your charity to investors, there are arrangement fees, listing fees and legal fees to pay. This is not a low cost option, although it can be set up as a bond programme to allow future issues under the same documentation which is more cost effective.
- **Will issuing a bond impact our donations?** – With both individuals and Foundations there is a risk that they will divert donations to invest in a bond, thus reducing revenue, however they may be prepared to leave the money in the charity at maturity rather than requiring repayment. Bond and loan monies have the advantage of being unrestricted monies which is helpful to some charities whose main incomes are heavily restricted.
- **With interest rates forecast to rise in 2015, will our bond interest costs also rise?** – Bonds are typically issued with a fixed interest rate until maturity, so changes in interest rates in the meantime won't affect you. Typical interest rates range from 2% to 5% pa dependent upon term.
- **What interaction should we typically have with the investors after issuance?** – A Bond issue will usually include financial covenants, so investors will want an annual report on your financial accounts, and potentially a social impact report annually. Regular communication is helpful, in the same way as you do for your donors so that they understand what the charity is doing with the bond monies. Whilst most investors will hold the Bond until maturity, and most understand that a market for selling the Bond may be limited, it is helpful for investors to have the bond listed on an exchange, so that they have a means of liquidity if they need it.



David McHattie
Head of Charities
Corporate Banking Barclays
david.mchattie@barclays.com

- **What else do I need to know?** – If you want to raise long term funding, the bond market is a valid alternative to the bank debt market. However, if all this sounds like it is not for you, then traditional bank debt remains a very flexible option. It is cheap and quick to arrange, using standard documentation so fees are low and can be arranged with staged drawdowns and regular repayments, so that you do not face having to pay the entire sum all at once in the future. The other key difference is that bond debt is a public debt market, so a retail bond issue will be publicised, giving an increased profile in the media. If this is your rationale for looking at the bond market then bank debt wouldn't be for you in this case.

Conclusion

There are a number of third parties who can assist with arranging bond issues. Speak to one of them or speak to your bank manager to see what terms your bank can provide. With low interest rates set to continue for now, this could be a good time to borrow to further your charity's cause.



Nikki Loan
Senior Manager, Charities
and Not for Profit, Deloitte
Nloan@deloitte.co.uk

Two SORPs and two briefings

The new charities SORPs (the FRS 102 SORP and the FRSSSE SORP) were published in July 2014 and will be applicable for periods beginning on or after 1 January 2015. These replace the existing SORP 2005. Deloitte has prepared two briefings; one for those preparing accounts under FRS 102 and one specifically for small charities.

They key changes for those preparing accounts under FRS 102 include:

- SOFA formats simplified using 'plain' English.
- Comparatives required for all funds disclosed in the statement of financial activities.
- Income should be recognised when receipt is probable rather than the current criteria of virtually certain – which may be particularly significant for charities with sizeable legacy income. Specific guidance on legacy income recognition is provided.
- Donated goods for sale or distribution are to be recognised on receipt at fair value where practical unless not justified on cost/benefit grounds.
- No cash flow statement exemption for small charities.
- Deficit funding agreements must be recognised as liabilities for multi-employer defined benefit pension scheme arrangements.
- Total remuneration for key management personnel is required in the notes to the accounts and larger charities must disclose their arrangements for setting the pay and remuneration of the charity's key management personnel in the trustees' report.

- Disclosure of the number of employees paid over £60,000 is required in bands of £10,000 from £60,000 upwards.
- The trustees' report will need to be more balanced, with increased emphasis on public benefit, successes, failures and lessons learned.
- The requirements that previously only applied to charitable companies requiring specific disclosure of the principal risks and uncertainties have been extended to all larger charities and mitigating actions must also be included.
- The reserves policy must be fully explained or an explanation given of why there is no policy.

For charities who are small in accordance with Companies Act definitions there is a choice:

From 2015, small charities will have a choice as to whether to adopt FRS 102 – the replacement for UK GAAP – or the FRSSSE. The Charity Commission and OSCR have prepared two separate SORPs depending on which underlying standard is adopted– the FRSSSE SORP and the FRS 102 SORP.

The FRSSSE SORP has been designed to deliver minimal changes to charities currently adopting the FRSSSE. The FRSSSE is only subject to minor changes for 2015, with the FRC having announced their intention to withdraw the FRSSSE in 2016 and ask small entities to apply FRS 102 with reduced disclosures.

Why pick the FRSSSE and FRSSSE SORP?

- Fewer changes in 2015 from current practice – allowing more time to consider the changes that may be necessary for 2016.
- No cash flow statement.
- No change for accounting for financial instruments.
- No change to the presentation of gains and losses on investment assets.
- No requirement to provide for additional contributions under multi-employer pension schemes.

Why pick FRS 102 and the FRS 102 SORP?

If your charity is growing in size, change may be inevitable and best dealt with in one go.

If your affairs are simpler (no complex financial instruments, no multi-employer pension schemes), there may be little difference in practice other than producing a cash flow statement.

Next steps

The new SORPs will be applicable for periods beginning on or after 1 January 2015. Early adoption is not permitted until the law is amended. The SORPs are available on the Charity Commission micro-site (<http://www.charitycorp.org/>).

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2014 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 39788A