CFG INSPIRING FINANCIAL LEADERSHIP

GENERAL DATA PROTECTION REGULATION:

A GUIDE FOR CHARITIES

Buzzacott CHARTERED ACCOUNTANTS

Crowe Clark Whitehill

Kingston Smith Helping clients succeed

Charity Finance Group

The purpose of Charity Finance Group (CFG) is to develop a financially confident, dynamic and trustworthy charity sector.

Our 1,400 members are charity finance professionals, who between them manage £21bn of funds. We work with our members to: inspire and nurture leadership; drive up standards; create a better and fairer operating environment; identify best practice and share knowledge.

Ultimately, we strive to equip charities with the knowledge, skills and conditions they need to ensure that every pound works even harder, achieving a greater impact for even more beneficiaries.

Published by Charity Finance Group
First published 2018

Phone: 0845 345 3192
Website: www.cfg.org.uk
Email: info@cfg.org.uk

Edited by Heather McLoughlin, Policy and Public Affairs Officer, Charity Finance Group

Designed by Steers McGillan Eves

FOREWORD

Welcome to Charity Finance Group's *General Data Protection Regulation: A guide for charities*. I am sure this guide will be an invaluable resource in enabling charities to understand and improve on your data protection policies.

Data protection has always been historically important, from Caesar's cipher device to our modern data protection laws. Data protection is a core area of a charity's operations and the implementation of the GDPR by the European Union in May 2018 means that charities need to understand and implement regulation effectively and efficiently.

Effective and efficient data management is so much more than simply knowing what data is coming in and what your charity is doing with it. Having proper policies in place to protect your data can also help you to maintain your reputation, both with your donors and the wider public.

Charities are currently operating in an environment where the regulatory burden for data protection is increasing. So too is the expectation of all organisations to comply with existing legislation. Recent high-profile charity cases and figures from the Information Commissioner's Office (ICO) show an overall rise in the number of charities who have suffered a data protection breach. Compliance is important; by taking steps to ensure effective data management you can also help to manage your risks. Charities will see efficiencies in terms of staff time spent on locating, navigating and using data to help achieve objectives.

Charity Finance Group (CFG) is committed to supporting charities to be effective and responsible organisations. Working with our partners we have gathered all the latest information that charities need to fully understand data protection laws. This guide focuses on: governance, financial data, beneficiary data, and employee data and we hope this provides charities with the expertise you need to address the unique challenges that charities face when dealing with the GDPR.

It is our hope that as a trustee, staff or volunteer you can work your way through this guide, identifying areas for improvement, building your knowledge of the GDPR legislation, and moving towards actively managing your organisation's data protection policies. All charities have a duty to be proactive, to meet the challenges and changing needs of data protection, and to do our best to manage the consequences of data protection legislation, in the interests of our beneficiaries.

I hope this guide provides practical advice and concrete methods to support organisations to work towards achieving best practice in data protection. We are very grateful to Buzzacott, Crowe Clark Whitehill and Kingston Smith who helped to author this guide.

Nicki Deeson, Charity Finance Group, Chair

CONTENTS

1

DATA PROTECTION GUIDE 04

Introduction

What is this guide for?

Who is this guide for?

2

GOVERNANCE – BUZZACOTT 08

Understanding the General Data Protection Regulation Governance

Where do data protection laws come from?

Who are the regulators?

What are the regulators powers with regards to charities?

Differences between the Data Protection Act and the GDPR

What are the key principles of the GDPR?

How to build a good governance culture around the GDPR

What to do if you have a data breach?

Where do you report data breaches?

Creating a data protection policy

3

FUNDRAISING AND THE GDPR – KINGSTON SMITH 16

Meeting the challenges of fundraising and data protection

What to do with donor data?

Understanding how to store and dispose of donor data

How to ensure you've gained donor consent

A fair interpretation of the GDPR

Working with third party fundraisers

Consideration of risks to a charities business model

4

FINANCIAL DATA – CROWE CLARK WHITEHILL 22

What changes will charities have to make from the Data Protection Act?

Reporting financial data

Disposal of financial data

5

BENEFICIARY DATA – CROWE CLARK WHITEHILL 30

What changes will charities have to make from the Data Protection Act?

Consent and the GDPR

Legitimate Interest

Reporting beneficiary data

Disposal of beneficiary data

6

EMPLOYEE DATA – BUZZCOTT 42

What changes will charities have to make from the Data Protection Act?

Should a charity depend on explicit consent of their employees to process personal data?

How does GDPR change how charities hold and process employee data?

What must a charity do with employees' data?

What to do with volunteers?

OTHER USEFUL ORGANISATIONS AND RESOURCES 47

SPONSORS AND CONTRIBUTORS 49

CONTENTS

DATA PROTECTION REGULATION

INTRODUCTION

1.1 WHAT IS THIS GUIDE FOR?

The guide should be essential reading for those who are responsible for protecting their charity's data. It is not a technical document but provides a framework for a charity to increase its knowledge of data protection issues. The guide aims to help your charity understand the practical realities of what the law on General Data Protection Regulation (GDPR) means for your organisation and how it will impact on your work. It is important that charities, and by extension trustees, staff and volunteers, understand the seriousness of ensuring that your charity has excellent data protection policies. To do otherwise could result in a financial and reputational risk to your charity.

1.2 WHO IS THIS GUIDE FOR?

TRUSTEES

It is important that trustees know that they are responsible for ensuring that their organisation follows data protection law, whether that is the GDPR or other UK based legislation. The Charity Commission's CC20, ***Charity fundraising: a guide to trustee duties***, is clear that trustees are responsible for ensuring that there are proper systems and processes in place to ensure that any fundraising that collects data is compliant.

Under the Commission's **serious incident reporting** guidance, data breaches or loss should be reported to the Charity Commission. You also have a duty to ensure that you report serious incidents of data breaches to the Information Commissioners Office. Failure to do so is likely to be considered by the Commission as a breach of your duty as a trustee.

Your charity should therefore have effective processes to help avoid data breaches.

THE GUIDE SHOULD BE ESSENTIAL READING FOR THOSE WHO ARE RESPONSIBLE FOR PROTECTING THEIR CHARITY'S DATA. IT IS NOT A TECHNICAL DOCUMENT BUT PROVIDES A FRAMEWORK FOR A CHARITY TO INCREASE ITS KNOWLEDGE OF DATA PROTECTION ISSUES

STAFF AND VOLUNTEERS

Whether you are a finance officer, data protection officer or another member of staff, as employees of the charity it is essential that you understand your legal responsibility when working with data. It is important that you ensure that your data protection processes do not act against the interests of your charity. This will involve putting in controls, processes and structures to ensure that your organisation's data is managed to meet the legal requirements of the GDPR.

If you are responsible for the day to day processing of data it is essential that you advise your fellow trustees, staff and volunteers on how your organisation is implementing the GDPR. You need to ensure that everyone understands their responsibilities. This is also true for trustees and volunteers who may not be involved in the daily operations of the charity. By ensuring that all stakeholders understand the steps your organisation is taking to become GDPR compliant, you can ensure proper management of data.

GOVERNANCE AND THE GDPR – BUZZACOTT

Buzzacott
CHARTERED ACCOUNTANTS

UNDERSTANDING THE GENERAL DATA PROTECTION REGULATION

2.1 WHERE DO DATA PROTECTION LAWS COME FROM?

The European Union's data protection laws have long been regarded as a leading standard all over the world. Currently the UK is covered by the Data Protection Act 1998 (DPA) which came into force on the 1st March 2000. This Act came from the 1995 European Data Protection Directive; part of the EU's body of privacy and human rights law. The DPA and the European Data Protection Directive regulated the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Since the introduction of the DPA in 1998, technology, and how it is used to process data, has radically transformed the way organisations operate. To adapt to modern technology, in 2016, the EU adopted the General Data Protection Regulation (GDPR). It replaces the 1995 Data Protection Directive.

The GDPR is now recognised as law across the EU and Member States have two years to ensure that it is fully implemented in their countries by 25 May 2018. While the UK is still a part of the EU the GDPR will come into force for organisations in the UK. After the UK exits the EU, the GDPR will be enshrined in EU law through the UK's government Data Protection Bill.

DATA PROTECTION BILL

The UK has already made some provision for the GDPR after Brexit with the Data Protection Bill. This Bill will replace the Data Protection Act 1998 with a new law that will reflect more modern, digital practices for handling data. The Bill also allows the Information Commissioners Office (ICO) more power to bring criminal proceedings against offences of malpractice.

Alongside the GDPR, the UK Data Protection Bill will contain local derogations allowed by GDPR and any further steps the UK government will take after the UK leaves the EU. It may also introduce extra provisions where the UK government wishes to tighten areas or cover areas that are not contained in GDPR. It also introduces two new offences within the UK:

- The 're-identification of de-identified personal data': the matching of de-identified data with publicly available information in order to identify the individual to which the data belongs to;
- The 'alteration of personal data to prevent disclosure'. This offence criminalises the alteration of personal data after a subject access request has been filed with a data controller.

You can find out more about the Data Protection Bill at **www.gov.uk/guidance/data-protection-bill-overview**.

2.2 WHO ARE THE REGULATORS?

In the UK, the GDPR will be overseen by the Information Commissioner's Office (ICO). They are an independent public body set up to uphold information rights in the public interest. The ICO sit independently of government, though are sponsored by the Department for Digital, Culture, Media and Sport (DCMS).

The ICO will have powers to take action where organisations are failing to comply with the law; as indeed the ICO do currently with the existing Data Protection laws. The ICO also has powers under the Privacy and Electronic Communications Regulation (PECR) which governs the use of electronic means of marketing such as; emails, text messages, etc., which was updated in 2016.

2.3 WHAT ARE THE REGULATORS POWERS WITH REGARDS TO CHARITIES?

In terms of data protection, the rules are the same for charities as they are for any other organisation. Under the GDPR, the ICO will be given more powers to defend consumer interests and issue higher fines. In case of the most serious data breaches, this could be of up to €20 million or 4% of annual global turnover (whichever is higher), aligned to the financial sanctions set out within the GDPR. The ICO also provides a right for individuals to claim compensation in relation to data breaches if they cause damage or distress.

Furthermore, the ICO can take action, such as, performing a data protection audit, taking enforcement action, and levy a fine for serious incidents. Recently they have been particularly focussed on the use of data for purposes other than that for which it was collected: a number of prominent charities have had action taken over their fundraising activities under this focus.

THE INFORMATION COMMISSIONER'S OFFICE WILL HAVE POWERS TO TAKE ACTION WHERE ORGANISATIONS ARE FAILING TO COMPLY WITH THE LAW

The important thing to remember is that you should be only using data for the purposes that you told the data subject when you collected it, and for which they gave their consent. However, you might not need to ask the data subject for consent if there is another valid reason for processing the data – perhaps to fulfil a contractual arrangement, or in support of your legitimate interests (for more information on legitimate interests see Beneficiary section).

2.4 DIFFERENCES BETWEEN DPA AND GDPR

PERSONAL DATA

GDPR still covers Personal Data and Sensitive Personal Data (now to be known as Special Categories of Personal Data). These are almost the same as in the Data Protection Act.

For data to be classified under 'Personal Data; it must:

1. Be data (so not unrecorded conversations with service users, donors or customers); and
2. Be personal. Data is personal if it is concerned with identifiable, living individuals. It does not matter whether this data was processed automatically, electronically or manually.

Personal data has been expanded to include IP addresses, internet cookies and biometrics, such as, DNA and fingerprints.

It is common for IP addresses to be collected by websites or marketing campaign websites such as Mailchimp, so make sure that you have the right protections in place to look after this personal data.

SPECIAL CATEGORIES OF PERSONAL DATA

The GDPR maintains the same definition of sensitive personal data as the DPA. For data to be classified as sensitive personal data; it must fall into the following categories:

1. The racial or ethnic origin of the subject;
2. The subject's political opinions;
3. The subject's religious beliefs or beliefs of a similar nature;
4. Whether the subject is a member of a trade union;
5. Information on the subject's physical or mental health condition;
6. Information on the subject's sexual life;
7. The commission or alleged commission of an offence by the data subject; and
8. Information relating to the commission or alleged commission of an offence by the data subject.

The Special Categories now specifically includes Biometric Data and Genetic Data where processed to uniquely identify an individual. (e.g. fingerprint payment systems)

PRINCIPLES

The Principles are very much the same in GDPR as under the DPA, with some added details but there is the addition of a new accountability requirement. Specifically, GDPR requires you to show how you comply with the principles.

Here are some key differences:

DATA PROTECTION ACT	GDPR
EU member states created their law around data protection	A unified approach across all member states – the UK will continue to be part of the GDPR even after departing the EU.
Covers Personal Data and Sensitive Personal Data	Covers Personal Data and Special categories of Personal Data – now includes biometric and genetic data and online identifiers.
Data Protection Officer is not required in an organisation	Data Protection Officer is required for Public Authorities (e.g. local councils, regional government) and organisations where core activities consist of processing, on a large scale, special categories of personal data OR the processing activities require regular systematic monitoring of data subjects on a large scale (e.g. hospitals).
Consent – must have been freely given, be specific and informed	As before, but also consent must be clear, recorded, and be able to be withdrawn. Data Controllers must be able to demonstrate that consent has been given if consent is used as the basis for processing.
No legal obligation for data controllers to report breaches of security	Data breaches must be reported to supervisory authority (ICO in the UK) within 72 hours and in some cases to the data subjects as well.
Data Protection Impact Assessments are good practice for projects involving personal data	Data Protection Impact Assessments are now mandatory for projects/processing likely to result in a high risk to rights and freedoms of natural persons
Subject Access Requests – data to be provided to subject within 40 days and a fee of £10 could be charged	Subject Access Requests – data to be provided within one month and no fee chargeable. However, a 'reasonable fee' can be charged if the request is manifestly unfounded, excessive, or repetitive. A reasonable fee can also be charged to comply with requests for further copies of the same information. This does not mean that an organisation can charge for all subsequent access requests. Any reasonable fee must be based on the administrative cost of providing information.
Maximum penalty is £500,000	Maximum penalty could be up to €20 million or up to 4% of global turnover.
Accountability – limited and Data Processors have very little unless tied down in contract with a Data Controller	Data Controllers must be able to demonstrate that they comply with GDPR and there are requirements on Data Processors.

2.5 WHAT ARE THE KEY PRINCIPLES OF THE GDPR?

Article 5 of the GDPR contains the principles and requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability is referred to in Article 52 which requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." This means a policy with clear procedures in place, which are documented and stored, is important. Otherwise you may struggle to show how you are compliant with the GDPR.

It is important to remember that personal data can be held electronically, but may be held in other forms such as paper, photographs, etc. All are covered by the Regulation.

CFG realises, more and more charities are under pressure to demonstrate their impact and show the difference they have made. Provided that you anonymise the data of the people that you work with, you can still keep their information for measuring and charting your impact. You may also keep suitably anonymised records for historical purposes. Before you think about whether you can keep information, think about whether you need it in the first place. Has the reason for originally collecting and storing the data changed? Has the project or fundraising campaign ended? If so, it may be time to throw this data away. Not only is it against the rules to hold data longer than necessary, but the less data you hold, the easier it will be to keep on top of the rules. GDPR doesn't mean that you have to throw all your data away!

CFG realises that a lot of charities are focusing on getting consent for the data they have or processing it fairly. But is it up to date? This is just as important to avoid stress for the individuals concerned. Make sure that your charity's data is as up to date as possible and that you have a process to keep it up to date.

2.6 HOW TO BUILD A GOOD GOVERNANCE CULTURE AROUND GDPR

The GDPR states that the Data Controller 'must be able to demonstrate compliance'. A Data Controller means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

For the purposes of this guide, your charity is a Data Controller.

Under the GDPR, a Data Processor means 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. This could be, for example, a mailing house, a third-party fundraiser or a data destruction company. This means staff, volunteers, contractors and temporary staff are not classified as data processors. There must be a binding contract between the processor and the controller and must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the controller. A Data Processor must inform the controller if it believes that a processing of data breaches the GDPR or the Data Protection Bill.

To ensure that you are compliant with GDPR your organisation should have involvement at all levels from your board/trustees to general staff. It will be important to make sure staff, trustees, and volunteers, are all aware of their responsibilities in the area of the GDPR. This might be through a training/awareness programme. It is a requirement of the GDPR that everybody has the necessary skills and knowledge to be able to apply the law effectively. You should keep a log of who has been trained and when, and build this into the induction process for any new staff, volunteers and trustees.

It will be important to ensure that you have at least one of the necessary valid reasons for processing the data you are holding, which are:

- The individual whom the personal data is about has consented to the processing;
- The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract;
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract);
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident;
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions;
- The processing is in accordance with the "legitimate interests" condition.

For most charities, the processing of personal data will be because the individual has consented, entered into a contract or would like to, or because the processing is considered a "legitimate interest" by the charity. For more information on understanding the conditions of processing see the Beneficiaries section 5 of this guide. It is important to remember that processing activities include just about anything that you do to the data – for example: back-up, deletion, updating, sending correspondence etc.

DATA PROTECTION OFFICER

One change under the GDPR for the UK is the mandatory requirement to appoint a Data Protection Officer (DPO) in certain situations. An organisation will have to appoint a DPO if:

- You are a public authority or body;
- Where your data processing activities involve regular monitoring of data subjects on a large scale; and;
- Where the core activities of processing data involves a large amount of sensitive personal data.

2.7 WHAT TO DO IF YOU HAVE A DATA BREACH?

The ICO, describes a personal data breach as "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data."

If you suffer a personal data breach, then you should follow your Data Breach Policy. This should ideally contain the steps to follow, who to notify internally in your organisation and who to notify externally (if necessary). You should make sure that you have robust breach detection, investigation and internal reporting procedures in place. The ICO again has guidance on the requirement to notify both Regulator/Supervisory Authority and Data Subject.

2.8 WHERE DO YOU REPORT DATA BREACHES?

If a breach is likely to result in a risk to the rights and freedoms of individuals then the breach must be reported to the relevant supervisory authority within 72 hours. In the UK this is the Information Commissioner's Office.

If a breach is likely to result in a high risk (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then you must also notify those concerned without undue delay.

Failure to notify a breach when there is a requirement to do so can result in a fine.

You can report a breach at **www.ico.org.uk/for-organisations/report-a-breach/**

REPORTING TO THE CHARITY COMMISSION FOR ENGLAND AND WALES

Along with reporting a data breach to the ICO, a charity will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission. The Commission lists the below as a data breach that should be reported:

- Charity's data has been accessed by an unknown person; this data was accessed and deleted, including the charity's email account, donor names and addresses;
- A charity laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;
- Charity funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;
- A Data Protection Act breach has occurred and been reported to the ICO.

You can find out more about reporting a serious incident at **https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity**.

If you are a charity that is operating in Scotland and Northern Ireland, consult with The Officer of the Scottish Regulator and the Charity Commission for Northern Ireland for further guidance.

2.9 CREATING A DATA PROTECTION POLICY

A Data Protection Policy should ideally contain the following information:

- ☐ What data your organisation keeps and why it keeps this data.
- ☐ To what types of data the policy applies.
- ☐ Who in the organisation is responsible for processing the data?
- ☐ The main data risks faced by the organisation.
- ☐ Key precautions to keep data protected.
- ☐ How data should be stored and backed up.
- ☐ How the organisation ensures data is kept accurate and when data will be deleted.
- ☐ What to do if an individual asks to see their data and when you will turn down a Subject Access Request.
- ☐ Under what circumstances the organisation discloses data, and to whom.
- ☐ How the company keeps individuals informed about data it holds.
- ☐ Who is responsible for reporting any breaches to the ICO and Charity Commission.

Your policy may reference other policies such as a Data Security Policy, and a Data Breach Policy or Procedure.

Your practice and policy should match!

CFG and the British Academy Research Project *Digitising the Mixed Economy of Welfare in Britain*, based at UCL Institute of Education, have produced the *Record management in charities: A toolkit for improvement.*

This toolkit is an essential first step for any charity looking at their record management and archiving systems. It will help charities to make sense of what their current record management policy is and how they can improve this. The toolkit will help charities to identify issues and solutions to the size and scope of their organisation. Read and download the toolkit at **http://bit.ly/recordmanagement**

Finally, should you wish to take your reading further there is guidance as well as the full GDPR text available via the Information Commissioner's Website – **https:\\www.ico.org.uk**

3

FUNDRAISING AND THE GDPR – KINGSTON SMITH

MEETING THE CHALLENGES OF FUNDRAISING

Since 2015, the fundraising profession has faced a crisis of confidence. The use of donor data has featured with regularity in various criticisms of fundraising. The introduction of a new, rigorous General Data Protection Regulation (GDPR) will have significant impact on how charities fundraise. The GDPR presents a great opportunity for your charity to review policies and procedures to ensure absolute compliance with various fundraising practices.

Given that in most charities it is the fundraising department that has the broadest interaction with the external environment, it is critical that fundraising leaders fully engage with the rigours of GDPR. While trying to respond to GDPR in a perfectly compliant way, it could be quite easy to be at odds with best practice in fundraising. Communicating with donors and prospective donors is a specialist activity. It is important to start with best fundraising practice and then to overlay GDPR compliance, and not vice versa.

For example, one should generally interpret GDPR regulations about data retention, so that records are kept for as short a time as possible, and policies to discard data after two years, could easily be created.

However, it is helpful to keep some donor data for much longer if a charity receives legacy income. Gifts in wills often arrive after a multi-year period of silence from a donor, as these donors are less likely to make cash donations into old age, and it would be tempting to regard their records as 'lapsed'. But if a will is contentious, the charity will want to evidence that the legator was once a loyal supporter, and will need data to do this. In a more typical scenario, it is valuable to the legator's next of kin to receive a thank you letter that refers to the generosity of their relative. It may even help develop a new donor relationship with this next generation.

The GDPR is starting to create a cultural change in fundraising. Fundraisers are good at sharing ideas with each other, and are early adopters of new ways of working. However, often new ideas are simply transferred from one organisation to another without much thought about the reasons why such a tactic may work. **The GDPR encourages fundraisers to create an evidence base to justify why they are using data in certain ways.** For example, processing data for prospect research may be in the legitimate interest of many charities, but they will need to prove why this is so. It requires evidence that those being researched would reasonably expect it to happen and are unlikely to want to opt-out of such activity. This is all achievable, but individual fundraisers and the sector as a whole, will need to be better at relying on evidence when they justify their actions.

The GDPR is changing the fundraising profession, and charities that apply fundraising principles to the rules, and build up evidence to justify their actions, will be those that are more successful in the future.

GDPR is not just about fundraising, but given how important fundraising is to the financial sustainability of charities, it is unsurprising that a lot of focus has been there. Make sure that GDPR isn't just a conversation about fundraising in your charity, but covers all parts of your organisation and the issues brought up in this guide!

3.1 WHAT TO DO WITH DONOR DATA?

An area of concern covered by the GDPR is data collection and data storage, and how it applies to donor data. Charities must be able to demonstrate the necessity behind collecting and storing donor data. The practice of collecting as much data as possible, and then, in reality, only processing part of the data set (the remainder is generally not fit for purpose) will not be permitted under the GDPR. The ability of individuals to make a 'Subject Access Request' (SAR) and demand to see the data retained about them within 28 days should also influence a charity's decision to collect only certain data.

3.2 UNDERSTANDING HOW TO STORE AND DISPOSE OF DONOR DATA

Storage raises other issues beside accessibility, such as security. Data of any type should be stored securely. There must be adequate means in place to ensure data is only accessed by processors and not by anyone else. Most data breaches occur as a result of human error, and charities are responsible for training staff in data security matters. **Charities also need to ensure end-to-end security when they pass donor data on to any suppliers, such as mailing houses, telephone fundraising agencies, etc. Don't just rely on these agencies to comply with GDPR rules, make sure that you are getting the assurance that you need before signing any agreements.**

Another major change that GDPR brings in is around the disposal of data or data erasure. Most organisations with large data storage capacity hold data indefinitely. This is either done by storing data in their main database or as archives. Either way, there are liabilities attached to storing data. Generally when donor data is not being used, because a donor has not given for a significant period, it is better to erase it and reduce the risks it may pose to your organisation.

The GDPR requires a limited retention period for data storage and also the presentation of a clear policy on data deletion/erasure within the organisation's Privacy Policy. No one can store data indefinitely anymore, and charities need to be proactive in deciding what data they will keep for which duration.

According to HMRC, Gift Aid declarations need to be kept for six years, but if a donor gave once, and has since lapsed for three years, then their data can be minimized to only that which is essential for HMRC's purposes. It should also have a reminder to be discarded after six years.

In addition, the GDPR enforces accuracy of data. This is common sense, inaccurate data is of little value, but it can be hard to update records regularly with a trackable audit trail. While it may feel counter-intuitive, it is better that data which is out of date is deleted. The risk of a data protection breach through inaccurate records needs to be carefully balanced against the risk of discarding valuable data.

MOST DATA BREACHES OCCUR AS A RESULT OF HUMAN ERROR, AND CHARITIES ARE RESPONSIBLE FOR TRAINING STAFF IN DATA SECURITY MATTERS

3.3 HOW TO ENSURE YOU'VE GAINED DONOR CONSENT

Consent is only one of the six conditions that will often be used by charities when fundraising. Gaining consent to use personal data can however be challenging. Under the GDPR, the bar has been raised, and **each time that a donor's consent is requested, it must be unambiguous, freely given, demonstrable, specific and informed.**

It is helpful to think that consent should result in no surprises when donor data is subsequently processed. Taking each requirement in turn:

- There will be no confusion if the request is unambiguous;
- For consent to be freely given, the donor should feel the same as they do about the voluntary gift they make. They didn't have to give, but they chose to do so;
- To be demonstrable, the charity must be able to prove when and how consent was given. Obtaining consent over the phone can be hard to demonstrate, and requires excellence in following due process and recording what has been said.

The next two requirements will be more challenging for charities:

- Specific consent means that a carte blanche tick box to receive everything the charity sends out will no longer be good enough. Donors need to be given choices, and these need to be real and granular. Some people want to hear about a charity's activities, but don't want to be asked for money. Fundraisers will need to make use of their skills in asking for money and when asking people to provide their data so they can be asked in the future;
- Alongside this granularity, it will be important to inform people of what giving their consent means. Charities will need to be more open about their fundraising plans, and be prepared to be upfront about the consequences of ticking a box.

3.4 A FAIR INTERPRETATION OF THE GDPR LAW

The purpose of the GDPR is to empower data subjects and protect their rights. Fairness means that organisations have to be absolutely clear as to:

- Why they collect donor data;
- What they do with the data;
- Who they share donor data with;
- How they store donor data;
- How long they keep donor data; and
- When data subjects can access their data.

Data has previously been understood as an asset that an organisation, such as a charity, collects and uses. Phrases such as 'data mining' (meaning turning raw data into useable information; done by using software to look for patterns in large batches of data) reflect the attitude towards aggregated data. But each layer in a data mine could be one individual's personal data. **The GDPR puts control back in the hands of the data subject. They may give their data away to be processed, but it is only ever 'on loan' and the data processor has a responsibility to treat it very carefully.**

The GDPR requires organisations to make sure that they have the correct policies and procedures in place before making any attempts to collect or process data. The policies need to ensure that charities are more transparent in their processing and communicate more effectively with data subjects. In addition, the GDPR ensures organisations have the capacity and justifiable reasoning to collect and store data.

This means that data should only be collected if there is a legitimate use for it. Without having adequate means of collection, storage, updating and deletion, organisations will be in breach of the GDPR.

Lastly, the GDPR requires organisations to not only be compliant, but to monitor and test that compliance. If there is a data breach, then there are strict requirements for reporting that breach to the ICO within 72 hours if it is likely to harm the data subjects. A fundraising data breach should also be reported to the Charity Commission as a serious incident.

WORKING WITH THIRD PARTY FUNDRAISERS

CFG advises that charities that work with third party fundraisers, including consultants, freelance fundraisers, agencies and suppliers are expected to ensure that the third party supplier upholds the same standards as the charity. This means that organisations MUST require any third party or agency to comply with requirements under the GDPR and the Privacy and Electronic Communications Preference Service, regardless of the country or legal jurisdiction in which the agency is based or operating.

The Fundraising Regulator has produced further guidance for charities who work with third party fundraisers. You can view this guidance at **www.fundraisingregulator.org.uk/4-0-working-third-parties/**

Organisations must deliver effective and proportionate monitoring of any third party contracts. Charities should also ensure that donors know where and how they can report any concerns and suspected breaches resulting from third party fundraising practices.

3.5 CONSIDERATION OF RISKS TO A CHARITIES BUSINESS MODEL

The GDPR tries to promote a culture of risk awareness in organisations who handle any type of personal data. It also attaches importance and value to informing data subjects about their rights. The risk that the GDPR presents to charities' business models is serious. If charities do manage to comply with the GDPR and there are no widely reported data breaches, then trust and confidence in the sector will probably be elevated. If however, there is a perception that charities do not respect donor subjects rights, then this may have a negative impact on fundraising activities, and could reduce overall charitable income.

The emphasis on reaching GDPR compliance has highlighted that many charities had started to become non-compliant in their requirements under the Data Protection Act 1998. You should take time to deal with these issues and put in place polices in accordance with the new legislative requirements. This requires charities to spend time, human and financial resources, to identify areas of concerns and solve any issues immediately. Charity business models often develop over years of practice and it may be hard to change organisational behaviour within a limited timeframe to promote good practice.

The risk of a data breach for an individual charity may be small, but the consequence of a fine of €20 million or 4% of global turnover, whichever is larger, means that it should impact every charity's business model. Avoidance of this risk can be mitigated by appointing a Data Protection Officer (DPO), who will be able to stay up to date with future GDPR changes. Many charities are appointing external DPOs, especially where the fees include an indemnity against the risk of fines as a result of the DPO's advice.

Risk can also be avoided by a comprehensive and ongoing staff training programme on their use of data under GDPR. The majority of breaches arise from human error, so working with staff and volunteers is the most important place to start when it comes to reducing this likelihood.

The Institute of Fundraising have published *GDPR: The Essentials for Fundraising Organisations* to help fundraisers understand their legal obligations under the GDPR. You can download the guide at **http://bit.ly/IOFGDPR**

For more information on selecting and using online giving platforms, The Institute of Fundraising, along with CFG and Crowe Clark Whitehill, has published a guide *Making the most of digital donations: A practical guide to selecting and using online giving platforms*. You can download the guide at **http://www.cfg.org.uk/onlinegiving**

IF THERE IS A DATA BREACH, THEN THERE ARE STRICT REQUIREMENTS FOR REPORTING THAT BREACH TO THE ICO WITHIN 72 HOURS IF IT IS LIKELY TO HARM THE DATA SUBJECTS

41

FINANCIAL DATA AND THE GDPR – CROWE CLARK WHITEHILL

MANAGING FINANCIAL DATA

4.1 WHAT CHANGES WILL CHARITIES HAVE TO MAKE FROM THE DATA PROTECTION ACT?

The GDPR will give individuals more control over their data and therefore charities will have more obligations, including a requirement to be accountable as a data controller and processer of data, and to demonstrate the accountability in documentation, policies and procedures.

Charities will need to assess their financial processes against GDPR requirements, identify any deficiencies and design new processes in order to comply with GDPR. Charities that are already compliant with the UK's Data Protection Act will be able to adapt more easily to the requirements introduced by GDPR.

Charities may benefit from setting up a GDPR program team to conduct a gap analysis, assess the need for a Data Protection Officer and manage the transition to the GDPR.

CHARITIES MAY BENEFIT FROM SETTING UP A GDPR PROGRAM TEAM TO CONDUCT A GAP ANALYSIS, ASSESS THE NEED FOR A DATA PROTECTION OFFICER AND MANAGE THE TRANSITION TO THE GDPR

The GDPR will oblige charities to make sure that their financial processes comply with the principles of GDPR:

- Oblige charities to comply with the provisions, and to demonstrate compliance through the accountability principle;
- Ensure that a clear legal basis is identified in advance for the processing of personal data;
- Oblige charities to provide all data subjects with more information about what is happening to their data, including children who must be given this information in an easy to read format;
- Oblige charities to have a system in place to allow parents to provide consent on behalf of children under the age of 13;
- Requires contracts with any organisation processing data on the charity's behalf to be updated with significant new terms required along with due diligence and monitoring.

The following table summarises the overall tasks charities should consider as part of their efforts to become GDPR compliant, along with additional considerations in respect of financial data:

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING FINANCIAL DATA
Awareness: *You should make sure that decision makers and key people in your organisation who handle your financial data are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.*	– Are people aware that the law is changing to the GDPR? – Where is GDPR and financial data captured within the risk management framework?	GDPR could have significant resource implications, especially for larger and more complex organisations. Addressing the requirements of the change to organisation's systems and processes should not be underestimated and requires senior buy-in and leadership. Compliance may be more difficult if preparations are left until the last minute. Financial data under the GDPR needs to be clearly defined and understood by the organisation.
Information you hold: *You should document what financial data you hold is classified as personal data, where it came from and who you share it with. You may need to organise an information audit.*	– What personal data does your finance team hold? Where did it come from? Who have you shared this information with? – Are information records given to third parties correct? If not, you need to inform the third party so that it can correct its records. Third parties might be your pension provider, or an external pay roll provider. – Can you demonstrate how you comply with data protection principles? – Is the data safe and secure, if not, how can it be made so?	Effective policies and procedures documenting any processes involving any financial data that would be classified as personal data must be in place. A key challenge for many organisations is being able to understand what data is held and being clear as to how this is processed and shared, both within the charity and with third parties. **Overall, there is a clear need to understand what personal financial data is held, covering manual and electronic records. This may necessitate the completion of a data audit of all records, covering (but not limited to):** • **Employee records, including salary, credit applications, pension records;** • **Volunteer records, including personal financial details and expenses;** • **Supporter and fundraising data, including donation(s), support provided and any additional financial linked data, such as property;** • **Supplier information, including email addresses or contact information of those that are providing goods or services to your charity; and** • **Beneficiary financial data, such as grants made, financial assessments for bursary/ grant purposes and/or salary records.** The data audit is a key step in understanding what data is held, where it is and the basis on which it has been obtained. In addition, the charity needs to be clear where it is the responsibility of the data controller and processor, and if any third parties are holding such data on your behalf, such as a payroll or pensions provider, that they are clear with regards to their responsibilities. A data audit process could be achieved through a number of mediums, including: • Introductory presentations to key staff; • Questionnaires being sent to all business/ operational units to capture the personal data held; • Consideration of whether all financial data held remains relevant for the purpose for which it was obtained; • How the records (if at all) have been stored and disposed of. This needs to be supported by a clear and understandable policy and procedural framework – this should set out on what basis data is collected, what it is used for and how long it is to be retained, which again, needs to be communicated to all processors of data – whether within your charity or a third party.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING FINANCIAL DATA
Communication privacy information: *You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.*	– Have you reviewed your current privacy notices? Are any changes required? – Is this information provided in concise, easy to understand and clear language?	GDPR requires organisations to tell people additional things. For example, your lawful basis for processing the data, data retention periods and those individuals that have the right to complain to the ICO (and the process by which they can do this). This needs to be addressed and applied consistently, so ensuring all media (electronic and hard copy) is aligned, including communications with all parties for which personal financial data is held.
Individuals' rights: *You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal financial data or provide data electronically and in a commonly used format.*	– Do your procedures cover all the rights individuals have under GDPR? – How would you react if someone wanted their data deleted? Can your system locate and delete the data? Who will make decisions about deletion?	GDPR includes the following rights for individuals: • Right to be informed; • Right of access; • Right of rectification; • Right to erasure; • Right to restrict processing; • Right to data portability; • Right to object; and • Right not to be subject to automated decision making including profiling. Data portability is a new right. It only applies to: personal data provided to a controller; where processing is based on consent or for the performance of a contract; when processing is automated. Otherwise, these rights are the same as under the DPA but with significant increased risk attached for organisations, not least due to the size in potential fines. If the organisation is geared up to give individuals their rights now, the transition to GDPR should be relatively easy.
Subject Access requests: *You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.*	– If you handle a large number of requests, how will you handle having to deal with requests more quickly? – Have you considered developing a system to allow individuals to access their information online?	You will need a policy for how your charity handles subject access requests, for example from a contractor or former employee. This is especially important if you choose to refuse or charge for requests that are manifestly unfounded or excessive. You must tell the individual why you have refused the request and inform them they have the right to the supervisory authority and to a judicial remedy, within one month. There could be an increased number of subject access requests as well as more of an administrative burden for any organisation which handles a large number of requests.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING FINANCIAL DATA
Lawful basis for processing personal data: *You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.*	– What is your lawful basis for processing personal data? Have you documented this so that you comply with the GDPR's 'accountability' requirements? – Are you aware of modifications to individual's rights, for example stronger rights to have data deleted if consent is your lawful basis for processing?	Organisations will need to explain their lawful basis for processing personal data in their privacy notice and when they respond to a subject access request. The lawful bases in GDPR are broadly the same as the conditions for processing in the DPA. For personal financial data, this should generally be processed in accordance with the Legitimate Purposes of the organisation. For example, employee salary and bank account information, if held on the basis of paying salaries correctly for its staff. However, the following should be considered: • Is any personal financial data held which is no longer relevant? This is in line with the DPA but often organisations hold data over more than a seven year period (for taxation purposes) and as such, it should be considered whether financial records over this period are required; • In addition, if a bank account has been changed, it should be considered whether the prior records are still required; • Charities should clarify within employment contracts the personal financial data it holds for its employees, the purposes for which it is held, the duration for which it is to be held and the process by which it is to be disposed; • If the data is to be used for another purpose, such as modelling the charity's workforce as part of an organisation review, then unless this can be anonymised (in line with the definition within the GDPR) then employee consent should be obtained. In general, controlling and processing employee and volunteer financial data would be for the legitimate purposes of the charity. However, there needs to be specific assessment of any data considered sensitive, such as specific health and medical conditions which may impact the salary of the individual.
Consent: *You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consent now if it does not meet the GDPR standard.*	– Does your current consent meet GDPR standard? – Have you read the guidance on consent under GDPR published by the ICO? – How are you gaining consent? Through an opt-in or opt-out and is this separate from other terms and conditions? Is consent verifiable?	If you rely on consent, it needs to meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn (commonly referred to as 'explicit opt-in consent') – areas requiring consent for the use of financial data should be clearly set out.
Data Breaches: *You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.* *Key considerations of whether to report the breach to the ICO include whether the data is sensitive and if electronic, if the data is encrypted.*	– Are there processes in place to detect, report and investigate a personal financial data breach? – Are these processes documented? – Has an assessment of the types of personal financial data held been completed? Have cases been identified where you would be required to notify the ICO, or individuals affected, if there was a breach?	The GDPR requires all organisations to report certain types of data breach to the ICO and individuals in some cases. As well as reporting to the ICO, it should be assessed what personal financial data held would contravene the privacy risks to the individual and require the individual to be informed, as well as articulating what would be defined as "undue delay". In general, unless the data has been subject to pseudonymisation it may be a prudent view to take the perspective that all personal financial data would constitute a risk to the privacy rights of the individual. Make sure that your finance team knows who to report suspected breaches to. In addition, there needs to be a process to ensure how electronic data can be encrypted.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING FINANCIAL DATA
Data Protection by Design and Data Protection Impact Assessments: *You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments (PIAs) as well as the latest guidance from the Article 29 Working Party* ***http://bit.ly/GDPRArticle29****, and work out how and when to implement them in your organisation.*	– Have Data Protection Impact Assessments (DPIA) been completed where data processing is likely to result in high risk to individuals? – Have you assessed the situations where it will be necessary to conduct a DPIA? Who will do it? Does anyone else need to be involved? Will the process be run centrally or locally? – Have you familiarised yourself with the guidance ICO has produced on PIAs as well as guidance from the Article 29 Working Party?	**GDPR makes privacy by design an express legal requirement. Previously this was only good practice.** If a DPIA indicates that the data processing is high risk and you can't sufficiently address those risks, you must consult the ICO to seek its opinion on whether the processing operation complies with GDPR. In respect of financial data and the GDPR, a protocol needs to be clearly established for any key systems which incorporate personal financial data – this would typically comprise new Payroll/ Human Resources System implementation and/or changes in Pension Scheme administrator third party providers. Any change in systems and the associated DPIA should also consider how the data is to be retained securely and for what period, including how the data can be accessed in the event of a subject access request.
Data Protection Officers: *You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.*	– Have you designated responsibility for data protection compliance to someone? Does this person have the knowledge, support and authority to carry out their role effectively? – Have you assessed where this role sits within your organisation structure and governance arrangements? – Are you required to formally designate a Data Protection Officer (DPO)?	**Organisations must designate a DPO if they are:** • A public authority; • An organisation which carries out regular and systematic monitoring of individuals on a large scale; • An organisation that carries out large scale processing of special categories of data, such as health records, or information about criminal convictions.
International: *If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.*	– Do you operate in more than one EU member state? If yes, have you determined your lead data protection supervisory authority and documented this?	This is only relevant for organisations that carry out cross border processing, i.e. processing is carried out which substantially affects individuals in other EU states. If this is applicable, the organisation should map out where the most significant decisions about its processing activities are made. This will help establish their 'main establishment' and therefore their lead supervisory authority. When processing personal financial data, it should be considered whether this is to be transferred outside the EU – this may require clarity to be obtained from any third party processing data on your behalf. Where this is the case, it should be considered what safeguards are in place within the non EU country and whether you need to obtain consent for the data to be processed outside the EU. The European Commission has produced further information and guidance for organisations that transfer data outside of the EU and the EEA. This can be found at **http://bit.ly/EUinternational**

4.2 REPORTING FINANCIAL DATA

The requirements in respect of reporting financial data (under GDPR) are broadly in line with the DPA. In general, the majority of financial reports completed for wider distribution are either anonymised (for example, payroll expenditure reporting) or have a degree of psydomisation applied (where employee records are referenced in a report but these do not contain names/ addresses) and as such, would require additional information in order to establish the individuals involved.

Key differences are in the types of report which clearly list out personal financial data – whilst procedures would already have been in place to manage security, under GDPR there are the reporting timelines in terms of reporting breaches and the greater potential for increased regularity fines. As such, **it should be considered good practice to be very clear as to who can produce such reports and to be able to track their production, dissemination and disposal when no longer required.**

The policy and procedural framework should also be clear in this area – where the data is processed as part of the Legitimate Purposes of the organisation, this should be clear so that if there are any requests in respect of the "Right to be forgotten" that the requests can be refused or processed efficiently.

4.3 DISPOSAL OF FINANCIAL DATA

The disposal of financial data should be in line with the policy framework in place, acknowledging the legal retention periods in place (e.g. HMRC and Gift Aid). Once disposed of, there should be assurances that the disposal process has been secure and monitored to ensure that data is not lost through either poor practice or an ineffective third party.

WHILST PROCEDURES WOULD ALREADY HAVE BEEN IN PLACE TO MANAGE SECURITY, UNDER GDPR THERE ARE THE REPORTING TIMELINES IN TERMS OF REPORTING BREACHES AND THE GREATER POTENTIAL FOR INCREASED REGULARITY FINES

5

BENEFICIARY DATA AND THE GDPR – CROWE CLARK WHITEHILL

PROTECTING YOUR DATA, PROTECTING YOUR BENEFICIARIES

5.1 WHAT CHANGES WILL CHARITIES HAVE TO MAKE FROM THE DATA PROTECTION ACT?

The following table summarises the overall tasks that should be considered as part of charities efforts to become GDPR compliant, along with additional considerations in respect of beneficiary data:

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING BENEFICIARY DATA
Awareness: *You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.*	– Are people aware that the law is changing to the GDPR? Such as key staff, trustees, supporters and beneficiaries. – Where is GDPR captured within the risk management framework?	GDPR could have significant resource implications, especially for larger and more complex organisations. Addressing the requirements of the change to organisation systems and processes should not be underestimated and requires senior buy in and leadership. Compliance may be more difficult if preparations are left until the last minute. Beneficiary data under the GDPR needs to be clearly defined and understood by the organisation, including any third parties the charity is working with. Recognising the significance of this, particularly when considering demonstrating impact and work undertaken, is key.
Information you hold: *You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.*	– What personal data do you hold? Where did it come from? Where is this information stored? Who have you shared this information with? – Are information records given to third parties correct? If not, you need to inform the third party so that it can correct its records. – Can you demonstrate how you comply with data protection principles? – Is it safe and secure, if not, how can it be made so?	Effective policies and procedures documenting any processes involving personal data must be in place. A key challenge for many organisations has been being able to understand what data is held and being clear as to how this is processed and shared with third parties. Overall, there is a clear need to understand what personal data is held for beneficiaries, covering manual and electronic records. This may necessitate the completion of a data audit of all records, covering (but not limited to): • Beneficiary records held, including the duration of time that the records will be held for; • The location and types of records held and what work has been undertaken to obtain and cleanse the records; • Clarity as to what records are held which may constitute sensitive data, including data relating to children and medical conditions; • The processes by which the beneficiary data has been obtained and where it is held, including whether there is a duplication between electronic and locally held manual records; • Beneficiary financial data, such as grants made, financial assessments for bursary/ grant purposes and or salary records; • Countries outside of the EU and EEA thats data may be transferred to/ from; and • Individuals responsible for the data at each stage of the process. The data audit is a key step in understanding what data is held, where it is and the basis on which it has been obtained. In addition, the charity needs to be clear where it is the data controller and processor, and if any third parties are holding such data on your behalf, that they are clear with regards to their responsibilities. A way for organisations to work through the data audit process is through a number of mediums, including: • Introductory presentations to key staff; • Questionnaires being sent to all business/ operational units to capture the personal data held; • Consideration of whether all beneficiary data held remains relevant for the purpose for which it was obtained; and • How the records (if at all) have been disposed of. This needs to be supported by a clear and understandable policy and procedural framework – this should set out on what basis data is collected, what it is used for and how long it is to be retained, which again, needs to be communicated to all third party processors of data.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING BENEFICIARY DATA
Communication privacy information: *You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.*	– Have you reviewed your current privacy notices? Are any changes required? – Is this information provided in a concise, easy to understand and clear language?	GDPR requires organisations to tell people additional things. For example, your lawful basis for processing the data, data retention periods and those individuals that have the right to complain to the ICO (and the process by which they can do this). This needs to be addressed and applied consistently, so ensuring all media (electronic and hard copy) is aligned, including communications with all parties for which personal data is held. Communication of privacy information can be considered during a DPIA where and how notice is provided to individuals and how the risks associated with individuals being unaware of the additional requirements are mitigated.
Individuals' rights: *You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.*	– Do your procedures cover all the rights individuals have under GDPR? – Do your procedures cover how beneficiaries can exercise their individual rights? – How would you react if someone wanted their data deleted? Can your system locate and delete the data? Who will make decisions about deletion?	**GDPR includes the following rights for individuals:** • Right to be informed; • Right of access; • Right of rectification; • Right to erasure; • Right to restrict processing; • Right to data portability; • Right to object; and • Right not to be subject to automated decision making including profiling. Data portability is a new right. It only applies to: personal data provided to a controller; where processing is based on consent or for the performance of a contract; when processing is automated. Otherwise, these rights are the same as under the DPA but with some significant enhancements. If the organisation is geared up to give individuals their rights now, the transition to GDPR should be relatively easy.
Subject Access requests (SAR): *You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.*	– The new timescales mean you will have a month to comply rather than 40 days. If you handle a large number of requests, how will you handle having to deal with requests more quickly? – Have you considered developing system to allow individuals to access their information online? – How will you record, track and monitor SARs?	In most cases you won't be able to charge for complying with a request. You can refuse or charge for requests that are manifestly unfounded or excessive but you must tell the individual why you have refused the request and inform them they have the right to the supervisory authority and to a judicial remedy, within one month. There could be an increased administrative burden for any organisation which handles a large number of requests. Under the GDPR, organisations can withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others.' **Actions to prepare for SARs include** • Design template response letters so that you can ensure that all requirements of a response to a SAR are complied with; • Develop policies and procedures for handling SARs and ensure these take into account new timescales; and • Ensure that employees are trained in dealing with SARs and that they can recognise when a beneficiary has made a SAR and how this is to be dealt with.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING BENEFICIARY DATA
Lawful basis for processing personal data: *You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.*	– What is your lawful basis for processing personal data? Have you documented this so that you comply with the GDPR's 'accountability' requirements? – Are you aware of modifications to individual's rights, for example stronger rights to have data deleted if consent is your lawful basis for processing? – Have you produced a Legitimate Impact Assessment template?	Organisations will need to explain their lawful basis for processing personal data in their privacy notice and when they respond to a subject access request. The lawful bases in GDPR are broadly the same as the conditions for processing in the DPA. For personal beneficiary data, this should generally be processed in accordance with Consent, Legitimate Interest and Vital Interest principles. For example, a beneficiary may consent to the processing of provide personal data to enable receipt of services that a charity may provide. **However, the following should be considered:** • Is any personal beneficiary data held which is no longer relevant? This is in line with the DPA but often organisations hold data over more than a seven year period such as, for taxation purposes, and as such, it should be considered whether beneficiary records over this period are required; • In addition, if personal data has been changed, it should be considered whether the prior records are still required; • Charities should clarify within contracts the personal beneficiary data it holds, the purposes for which it is held, the duration for which it is to be held and the process by which it is to be disposed; • If the data is to be used for another purpose, such as for research or assessing the charities success in delivering a project as part of an organisation review, then unless this can be anonymised (in line with the definition within the GDPR) then beneficiary consent should be obtained. In general, controlling and processing beneficiary data, consent would have been received and would also be for the legitimate purposes of the charity. **However, there needs to be specific assessment of any data considered sensitive, such as specific health and medical conditions which may impact the individual.** Overall, the charity needs to be clear and consistent in its approach – whilst aspects of personal data may be obtained and processed in accordance with different lawful bases – this should be clear to the beneficiary. In addition, this has to be clear to staff and volunteers who act as data processors. Consent may not always need to be received to process beneficiary data. In many cases, this may be processed on the Legitimate Interest basis. For example, if beneficiary data has been obtained under legitimate interest purposes this should be clearly articulated as part of any privacy note and any material communicated to the beneficiary. From the charities perspective, there is a need to be able to demonstrate to funders the work that has been undertaken and provide an audit trail of its work which can be validated. However, if the beneficiary data obtained is to be used for any other purpose than which it was collected (e.g. to use the personal data of the individual in marketing material) then consent should be obtained.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING BENEFICIARY DATA
Consent: *You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.*	– Do your current consents meet GDPR standard? – Have you read the guidance on consent under GDPR published by the ICO? – Is consent gained through a positive opt-in and is this separate from other terms and conditions? Is consent verifiable? – Have you considered how long consent will last? – Have options other than consent been considered?	If you rely on consent, it needs to meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn – areas requiring consent for the use of beneficiary data should be clearly set out, including how the data is to be held, what it is to be used for and how long it will be retained. For example, does the beneficiary only want to be contacted about certain services? Do they have particular ways that they want to be contacted? Where a legitimate or vital interest is the basis for processing, records should be maintained, to show that the charity properly considered the rights of data subjects. Both the issue of consent and legitimate interest are detailed further below.
Children: *You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.*	– Do you need to put systems in place to verify individual's ages? If yes, how would you go about getting parental or guardian consent? – Have you reviewed privacy information given to children to ensure it is appropriate for a child? – Do you keep up to date with relevant codes of conduct which might affect any associations or groups your charity might participate in?	GDPR will introduce special protection for children's personal data, in particular commercial internet services such as social networking. Organisations which offer online services to children and rely on consent to collect information will be directly affected and must ensure language is tailored for the target audience. Processing of data related to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct. Under Article 8(2) GDPR, charities will need to make "reasonable efforts" to verify that consent has been given or authorised by the holder of parental responsibility. However, charities will not need to seek the consent of parental figures when the processing is related to preventive or counselling services offered directly to the child. Children "may be less aware of the risks, consequences and safeguards" of handing over their personal data. 'Legitimate interests' as a lawful basis instead of consent could also be considered but should be documented. This will help ensure charities assess the impact of data processing on children and consider whether it is fair and proportionate.
Data Breaches: *You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.*	– Are there processes in place to detect, report and investigate a personal data breach? Are these processes documented? – Have staff been trained on how to identify a data breach? – Has an assessment of the types of personal data held been completed? Have cases been identified where you would be required to notify the ICO, or individuals affected, if there was a breach?	The GDPR requires all organisations to report certain types of data breach to the ICO and individuals in some cases. The ICO must be notified of a breach if it is likely to result in a risk to the rights and freedoms of individuals, i.e. a significant economic or social disadvantage; in most cases you will also need to inform the individual. As well as reporting to the ICO, it should be assessed what personal beneficiary data held would contravene the privacy risks to the individual and require the individual to be informed, as well as articulating what would be defined as "undue delay". **As you may hold sensitive information about a beneficiary, for example, medical, criminal or other such information, it is very important to put in place clear procedures for contacting beneficiaries.** In general, unless the data has been subject to pseudonymisation, it may be a prudent view to take the perspective that all personal data would constitute a risk to the privacy rights of the individual.

KEY STEP	QUESTIONS TO CONSIDER	IMPLICATIONS / DETAILED ACTIONS REGARDING BENEFICIARY DATA
Data Protection by Design and Data Protection Impact Assessments: *You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party* ***(http://bit.ly/GDPRArticle29)****, and work out how and when to implement them in your organisation.*	– Have Data Protection Impact Assessments (DPIA) been completed where data processing is likely to result in high risk to individuals? – Have you assessed the situations where it will be necessary to conduct a DPIA? Who will do it? Does anyone else need to be involved? Will the process be run centrally or locally? – Have you familiarised yourself with the guidance ICO has produced on PIAs as well as guidance from the Article 29 Working Party? – Has GDPR been considered at the inception of new policies, procedures and systems? – Do you have a privacy impact assessment template which can then be filled in for each new system which comes into place?	GDPR makes privacy by design an express legal requirement. Previously this was only good practice. If a DPIA indicates that the data processing is high risk and you can't sufficiently address those risks, you must consult the ICO to seek its opinion on whether the processing operation complies with GDPR. In respect of beneficiary personal data and the GDPR, a protocol needs to be clearly established for any key systems which incorporate personal beneficiary data – this would typically comprise new Beneficiary Management System implementation and/or changes in third party providers. Any change in systems and the associated DPIA should also consider how the data is to be retained securely and for what period, including how the data can be accessed in the event of a subject access request. Data collection techniques including cookies should be revised to ensure that excessive data collection is not occurring and that automated deletion processes are in place to remove personal data after a set period of time. Agreements with third parties should set out the liability and risk allocation between parties for these requirements, to minimise large-scale issues occurring.
Data Protection Officers: *You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.*	– Have you designated responsibility for data protection compliance to someone? Does this person have the knowledge, support and authority to carry out their role effectively? – Have you assessed where this role sits within your organisation structure and governance arrangements? – Are you required to formally designate a Data Protection Officer (DPO)? – Have you documented your internal analysis if you decide not to appoint a DPO?	**Organisations must designate a DPO if they are:** • A public authority; • An organisation which carries out regular and systematic monitoring of individuals on a large scale; • An organisation that carries out large scale processing of special categories of data, such as health records, or information about criminal convictions.
International: *If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.*	– Do you operate in more than one EU member state? If yes, have you determined your lead data protection supervisory authority and documented this?	This is only relevant for organisations that carry out cross border processing, i.e. processing is carried out which substantially affects individuals in other EU states. If this is applicable, the organisation should map out where the most significant decisions about its processing activities are made. This will help establish their 'main establishment' and therefore their lead supervisory authority. When processing personal data, it should be considered whether this is to be transferred outside the EU – this may require clarity to be obtained from any third party processing data on your behalf. Where this is the case, it should be considered what safeguards are in place within the non EU country and whether you need to obtain consent for the data to be processed outside the EU.

INTERNATIONAL CHARITIES

International charities are complex and often have unique structures. These examples highlight where the GDPR applies for different international charities:

1. The charity is headquartered in the EU but transfers personal data to a third country. Data that is gathered in either the UK or the third country needs to meet GDPR standards. The charity needs to put into place appropriate safeguards and data can be transferred on the condition that the data subject rights are enforceable and that effective legal remedies for data subjects are available. It is important when gaining consent for processing from data subjects they are aware of their data being transferred to a third country;
2. The charity is headquartered in a country based outside the EU but engages with supporters or beneficiaries in the EU. This organisation will need to meet GDPR requirements and may need to appoint a representative in the EU;
3. The charity is headquartered in a third country and does NOT transfer, process or store any data belonging to EU residents. The GDPR does not apply to this international charity as long as EU data is not transferred to it.

CFG believes that it is best practice for any charity who operates overseas to ensure that all staff and volunteers, irrespective of location, abides by the GDPR.

The European Commission has produced guidance for organisations that transfer data outside of the EU and the EEA; **http://bit.ly/EUinternational**

5.2 CONSENT AND THE GDPR

The concept of consent is clearly defined within the Data Protection Act, however, the GDPR sets a higher standard for consent. In essence, consent in this context means beneficiaries understand that their data is being collected, the purpose it will be used for, and the type of data processing required to fulfil that purpose. Beneficiaries must agree that their data can be used as intended and communicated by the charity. Under GDPR, consent must meet the following criteria:

- Specific;
- Informed;
- Withdrawable;
- Freely given;
- Involve a clear affirmative action; and
- Be verifiable.

It should be noted that consent is not the only method of lawfully processing beneficiary data. Other grounds to process beneficiary data exist under GDPR. Processing may be necessary for the

- Performance of a contract with the data subject;
- Compliance of a legal obligation;
- Protection of vital interests of the data subject;
- Performance of a task carried out in the public interest; and
- Purposes of legitimate interest of the data controller.

Most are very specific and do not apply to charities but one, the legitimate interest condition, is likely to be commonly used to process data.

The ICO has recently published further guidance to help organisations who process children's personal data under the GDPR. This guidance can be found at **http://bit.ly/ICO-children**

CONSENT FROM VULNERABLE BENEFICIARIES

CFG advises charities to think carefully about how to gain consent from vulnerable beneficiaries who may not understand their rights under the GDPR. You may need to explain to them what the rules are and how it impacts them. This could mean ensuring the language you use is simple and clear for vulnerable beneficiaries to understand. This will ensure that vulnerable beneficiaries are making informed decisions when they give you their data.

5.3 LEGITIMATE INTEREST

This allows the processing of the data when it is in the charity's legitimate interests, provided it does not override the rights and freedoms of the beneficiary who owns it. Currently, there are not explicit definitions of what is legitimate in every context.

Legitimate interest covers data collection for purposes such as:

- Network security,;
- Fraud prevention;
- Maintaining existing client relationships;
- Direct marketing and more.

It is important to consider the following before using legitimate interest as a legal basis for processing personal data:

CONSIDERATION	DETAILED CONSIDERATION
Data Subject Interests	Legitimate interest should take into consideration the interests of the data subject, meaning that the purpose of processing should not harm the interests of the data subject
Reasonable processing	Legitimate interest is not applicable in situations where data subjects would not reasonably expect further processing
Objections	The data subject has a "Right to object", meaning processing based on legitimate interest must be stopped if a data subject objects. (Unless compelling legitimate grounds can be proven)
Right to be informed	Data subjects must be informed if their data is being collected under 'legitimate interest'. The data subject should also be informed about the purpose of collection and the right to object
Public Authorities	Legitimate Interest does not provide a legal basis for processing by public authorities

CFG BELIEVES THAT IT IS BEST PRACTICE FOR ANY CHARITY WHO OPERATES OVERSEAS TO ENSURE THAT ALL STAFF AND VOLUNTEERS, IRRESPECTIVE OF LOCATION, ABIDES BY THE GDPR

LEGITIMATE INTEREST TEST AND BALANCE

When relying on Legitimate Interests it is good practice to complete a Legitimate Interest Assessment (LIA).

In short, an LIA comprises three steps:

1. The assessment of whether a legitimate interest exists;
2. The establishment of the necessity of processing; and
3. Undertaking a balance of interests test.

A balance of interest test will assess whether the interest of the data controller or any third parties is overridden by those of the individual whose data is to be processed and how this applies to beneficiary data:

STEP		ACTIONS AND CONSIDERATIONS
1	**The assessment of whether a legitimate interest exists**	Is there a legitimate interest in processing the data? Why is the data important to the objectives of your organisation? In this case it should be clearly defined, but for work undertaken there is a need to be clear as to whom beneficiaries are in order to demonstrate that work is being undertaken in line with the charitable objects of the organisation. Has the legitimate interest been communicated to the individual? This should be undertaken at the point of service delivery and communicated in a manner in which is understandable to the individual and/or their parent/guardian representative.
2	**The establishment of necessity of processing**	Is processing the data necessary? Are there alternatives to processing the data? From a beneficiary perspective, there are unlikely to be alternatives to processing the data. Charities have previously encountered issues whereby the work undertaken cannot be demonstrated. Are there other ways to achieve the objective? If so, you may need to consider a DPIA.
3	**The performance of the aforementioned balancing test**	Consider whether an individual's rights would override you organisation's legitimate interest. **Nature of the interest** Would the individual expect the data processing to take place? Is the legitimate interest a fundamental right, public right or other type of interest? Would the individual also share the same interest in the data process? Would there be any unnecessary harm caused by processing the data? Is the data sensitive, related to a child or any other special category? If so, stricter rules may apply. **The impact of processing the data** Consider any impact on the individual and any bias to the organisation processing the data. What is the likelihood and severity level of the impact? How will the data be processed? e.g. profiling, data mining etc. **Consideration of Safeguards** Are controls in place to limit any negative impact on the individual? Consider additional weight to the rights of the individual if data relates to children or any other special categories. There may still be instances where it is considered that personal data for a beneficiary requires additional safeguards or may not be retained. For example, where there are instances of a beneficiary's personal safety being compromised, then the data may be held under pseudonymisation measures, or overall the data may be anonymised given the sensitivity of it.

EXAMPLES OF LEGITIMATE INTERESTS

Example 1 – Ethical

A charity may need to process potential beneficiaries data to determine whether they have the resources to assist the beneficiaries and if so, allocate these resources appropriately. The charity may also process potential beneficiary data to determine whether the beneficiary qualifies for receipt of services provided by the charity for financial assistance, such as grants. The processing of this data would be for the interest of the beneficiary and the charity.

Example 2 – Individual Rights

A charity may need to continue to process beneficiary data as an individual beneficiary may exercise their right to erasure. The charity will need to keep the minimum amount of personal data to identify that individual for the sole purpose of suppression. This suppression will ensure that the personal data of the individual beneficiary can no longer be processed. This would be in the best interest of the charity as well as the individual beneficiary.

Example 3 – Personalisation

A charity may rely on legitimate interest to justify analysis of personal data to determine its operational strategy and to enable it to decide on potential beneficiaries of its services.

Example 4 – Limited International Transfers

A charity may transfer personal data of its beneficiaries in the EU to a third party country (a country outside of the EU) that runs programmes to help such beneficiaries. In these instances, there needs to be measures in place to ensure the data is processed securely and in line with the GDPR principles, of the main establishments supervisory authority rather than the third party country's local requirements

Example 5 – Monitoring and Trends

A charity may ask its call centre to use software that deals with big data to identify trends or themes. The analysis may allow for the charity to optimise its services which will benefit the charity and the beneficiaries.

5.4 REPORTING BENEFICIARY DATA

The requirements in respect of reporting data (under GDPR) are broadly in line with the DPA. In general, the majority of management information reports completed for wider distribution are either anonymised (for example, research reporting) or have a degree of pseudonymisation applied (where beneficiary records are referenced in a report but these do not contain names/addresses) and as such, would require additional information in order to establish the individuals involved.

Key differences are in the types of report which clearly list out personal data – whilst procedures would already have been in place to manage security, under GDPR there are the reporting timelines in terms of reporting breaches and the greater potential for increased regularity fines. As such, it should be considered good practice to be very clear as to who can produce such reports and to be able to track their production, dissemination and disposal when no longer required.

This might either fall under your data protection policy, and/or through staff training/induction.

The policy and procedural framework should also be clear in this area – where the data is processed as part of the Legitimate Purposes of the organisation, this should be clear so that if there are any requests in respect of the "Right to be forgotten" that the requests can be refused or processed efficiently.

5.5 DISPOSAL OF BENEFICIARY DATA

The disposal of beneficiary data should be in line with your organisation's policy framework, acknowledging the legal retention periods that are in place. Once disposed of, there should be assurances that the disposal process has been secure and monitored to ensure that data is not lost through either poor practice or an ineffective third party.

6

EMPLOYEE DATA AND THE GDPR – BUZZACOTT

UNDERSTANDING YOUR RESPONSIBILITIES AS AN EMPLOYER

6.1 WHAT CHANGES WILL CHARITIES HAVE TO MAKE FROM THE DATA PROTECTION ACT?

Much of the work charities currently do with employee data under the Data Protection Act will continue to apply under the GDPR but there are some additional elements that charities will have to consider and implement.

One of the significant changes from May 2018 is that charities will not only need to say they comply with Data Protection legislation, but they will need to prove that they are complying. This will entail reviewing:

- What personal data on employees and volunteers a charity is holding and processing;
- How it is used; and
- What lawful basis will a charity rely on to continue to process employees' and volunteers' personal data.

Charities will need to create logs of data held and processed, which must be available for inspection by the ICO upon request.

Charities will need to identify someone who will have responsibility for ensuring compliance with the GDPR. Whether this individual is a dedicated Data Protection Officer will depend on the size of the charity and the amount of personal data processing it carries out. **Whoever is appointed will have responsibility for communication with the Regulator and needs to have sufficient authority and independence within the charity to monitor all data processing, as well as having experience in data protection legislation.**

To be able to process personal data, (which can include technical details such as employee number or IP address) a charity needs to determine on what legal grounds it will hold and process data. The following gives the list of lawful reasons:

- Consent of the individual;
- Processing which is necessary to fulfil the obligations of a contract with the individual;
- Processing to comply with a legal obligation;
- Processing to protect the vital interests of the individual or another person;
- Processing which is necessary for the purpose of the legitimate interests of the charity or a third party acting for the charity, unless overridden by the interests, rights or freedoms of the individual;
- Performance of a task carried out in the public interest.

Where a charity also holds sensitive data about an individual such as gender, health or biometric data, then the need to protect the data is greater.

6.2 SHOULD A CHARITY DEPEND ON EXPLICIT CONSENT OF THEIR EMPLOYEES TO PROCESS PERSONAL DATA?

Charities will need to consider how and when it gathers consent from an individual to hold and process data. Under GDPR consent is defined as "any freely given, specific, informed and unambiguous indication of the individual's wishes". It has to be an affirmative action rather than not ticking a box on a form. The concept of "freely given" means that charities will need to review their contracts of employment to match the new regulations.

> It will no longer be compliant to have a clause within an employment contract saying that by signing the contract the individual also agrees to the process of his or her personal data. This is not seen as freely given consent.

If a charity wishes to rely on consent it will need to have a separate form explaining the reasons for data processing, how data will be processed, that the individual has the right to withdraw consent at any time, and ask for explicit consent by either a signature or completing a tick box. Pre-ticked boxes or leaving a box blank will not be allowed.

For most employers it is actually more advisable to look to other lawful reasons to process individuals' data, such as to fulfil the requirements of a contract with the individual, compliance with a legal obligation or the legitimate interests of the charity. This can be done by use of a separate "Privacy Notice" which can be issued to all existing employees and new employees when they join the charity. The information required on a privacy notice is much the same as under current DPA, but will need additional information, such as:

REQUIRED UNDER THE DPA

- Who you are;
- The purpose/ purposes for which you will process their information;
- A consent statement if you intend to send the individuals marketing materials by email or text; and
- Anything else you need to include to ensure your processing of the information is fair such as who you may disclose the information to that the subject would not expect.

ADDITIONAL INFORMATION REQUIRED UNDER THE GDPR

- Details of the Data Protection Officer (or the individual tasked with data compliance);
- The basis on which the charity will rely to process data;
- Whether data is transferred or processed outside of the European Economic Area (EEA);
- The purposes of data processing;
- How long the data will be retained;
- The individual's rights to access;
- Modify or erase any personal data;
- Details of how an individual can complain to the regulator.

Where children's data is being processed, the UK government is considering 13 and under at which parental consent is also required, a lower age than specified in the GDPR.

Another key area which charities will need to review is the training given to employees and volunteers concerning data protection to ensure they are aware of the charity's increased accountability for data processing, as well as the potential for increased regulatory penalties.

6.3 HOW DOES GDPR CHANGE HOW CHARITIES HOLD AND PROCESS EMPLOYEE DATA?

Charities, like any other organisation, gather and retain personal data in a variety of ways such as information in personnel files, contractual forms, benefits applications as well as in email communication, computer log-in details and computer usage logs or records.

Under the main principles of GDPR, data must be collected for specific purposes, processed lawfully, accurately and fairly and must be retained in a form which could identify the individual for no longer than is necessary. Charities will need to review what data is currently stored about employees and volunteers and consider if it remains relevant to the legitimate interests of the charity and whether the data can be deleted or, if the charity wishes to retain the data, made less personal by anonymisation so that individual identification is no longer possible.

EMPLOYEE DATA AND THE GDPR

Until now charities have had no responsibility for any third-party organisation (e.g. a recruitment agency) to either process its data, or to supply data with individual's personal information. This change under GDPR means a charity will need to ensure that any third-party processor it uses complies with the regulations. There will need to be greater due diligence when choosing a third-party processor or supplier, and contractual arrangements will need to recognise the joint responsibility for GDPR compliance.

Many charities operate internationally and although GDPR is designed to harmonise data protection across the EU, there are elements of the regulations where Member States can apply country-specific amendments. One example can be seen in Germany where the monitoring of employees' emails is not allowed. A charity will need to be aware of such local amendments, as well as consider which Member States regulator has authority over the charity's data processing. If employees' data needs to be transferred outside of the EU, there are greater responsibilities imposed on the charity to ensure the security of the data.

6.4 WHAT MUST A CHARITY DO WITH EMPLOYEES' DATA?

Employees' data must be stored securely for as long as the data is required, in whatever format it is held. The data should be retained for no longer than is necessary in a format which can identify the individual. Therefore, charities will need to review current processes and ensure that employee data is reviewed for relevance on a regular basis. There are often legal obligations which mean that personal data needs to be kept for a specific period of time, such as for tax purposes, or to maintain records to be able to contest legal action, and these will continue to apply under GDPR.

As an example, with recruitment, charities can be unclear on what to do with the information gathered from applicants who were unsuccessful, and for how long it should be retained. In this situation, it is necessary to only hold the information for a limited period, say a maximum of six months, until it is clear that the unsuccessful applicant will not be offered a position with the charity.

Charities will need to ensure that there is a process to ensure such data cleansing is planned and then takes place. It is the charity's responsibility to ensure that all unnecessary data is either deleted or physically destroyed completely. Whilst there have been costly examples of organisations failing to dispose of personal information correctly, which have been widely published, the potential greater financial penalties allowed under GDPR makes this area one of vital importance.

WHAT TO DO WITH VOLUNTEERS?

CFG is aware charities are unique in working with volunteers and this can mean that charities will hold data on these individuals. Just as charities need to ensure GDPR compliance with employee data, the same requirements apply to personal information from volunteers. As with employees, charities need to communicate with their volunteers concerning any personal data gathered, how it is held and processed, how long it is retained and how it is disposed.

If you have volunteers who are processing your charity's data then you must ensure they are held to the same high standards as staff (especially where volunteers are essential for service delivery and support). In the eyes of the ICO and the Charity Commission a data breach occurring because of a volunteer error, or a staff error is treated the same.

Volunteers may still be subject to an organisation's rules on data protection and confidentiality even after the volunteering relationship has come to an end. Charities should take extra precautions where volunteers are essential for service delivery and might be responsible for sensitive data. A volunteer agreement is an ideal way of setting out what arrangements are made for volunteers who process data. This can be useful to clarify their responsibility, and any training that might be required for the volunteer's role. It is also important the agreement states where and how volunteers can report any suspected data breaches.

CFG, in partnership with Hempsons, have produced the *Employment Status Guide 2016* helping charities to understand the employment relationship and the issues you should consider when dealing with employees and volunteers. Download a copy at **http://bit.ly/employment2016**

OTHER USEFUL ORGANISATIONS AND RESOURCES

INFORMATION COMMISSIONER'S OFFICE

The ICO is the UK's independent body set up to uphold information rights. They have produced the *Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now* publication for organisations.

You can download this guide at **http://bit.ly/ICO12steps**.

You can contact the Information Commissioner at telephone: **0303 123 1113** or **01625 545 745**, or email at **casework@ico.gsi.gov.uk** or write to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF.

You can report a data protection breach at **https://ico.org.uk/for-organisations/report-a-breach/**

CHARITY COMMISSION FOR ENGLAND AND WALES

The Charity Commission is the independent regulator of charities in England and Wales. Since the Charities Act 2006, the Charity Commission has specific statutory functions which include identifying and/or investigating apparent misconduct or mismanagement in the administration of charities.
www.charitycommission.gov.uk
You can report a serious incident at **RSI@charitycommission.gsi.gov.uk**

HM REVENUE & CUSTOMS

HM Revenue & Customs (HMRC) is the government body responsible for Gift Aid and Tax. If a data breach could be responsible for Gift Aid or tax fraud you will need to report this to HMRC confidentially either online at **www.hmrc.gov.uk/reportingfraud** or by calling **0800 788 887** (for tax evasion – e.g. Gift Aid, Corporation Tax, VAT).

PUBLIC CONCERN AT WORK

Public Concern at Work is a registered charity which offers a free, confidential whistleblowing advice line for individuals concerned about crime, danger or wrongdoing at work.

www.pcaw.org.uk

You can telephone for advice at **020 3117 2520** or **020 7404 6609** or email: **helpline@pcaw.co.uk**

SPONSORS AND CONTRIBUTORS

BUZZACOTT

At **Buzzacott** we define ourselves by the needs of our clients. The relationships we build are both personal and enduring. They are founded on continuity of personnel, ease of access and a depth of specialist knowledge which in certain key areas leads the industry.

Charities are a very significant part of the Buzzacott client base – over one third of our business. Over the past 50 years, we have taken a leading role in the development and promotion of best practice in the sector and now act for over 300 charity and not-for-profit organisations in all parts of the sector, with particular concentration in education, faith-based groups, welfare, charities operating overseas and social enterprises.

If you ask our clients why they value Buzzacott, they will say it is our empathy with their work and understanding of the legal and accounting framework within which they operate.

We offer training for trustees and strategic advice to management. We provide a comprehensive tax, accounting, audit and financial advisory service, bespoke to need. We will design or review internal controls, and advise on risk and financial management, that is so critical for this sector.

For more information visit
www.buzzacott.co.uk

Buzzacott
CHARTERED ACCOUNTANTS

CROWE CLARK WHITEHILL

Crowe Clark Whitehill is a national audit, tax and advisory firm.

We are the UK member of Crowe Horwath International, the eighth largest global professional services network with 200 independent member firms operating from offices around the world.

We are trusted by thousands of clients for our head for figures, our specialist advice, and our readiness to give our clients added value.

Benefits of working with us:

1. Understanding the perspective of your key influencers

We can help present financial information in ways which not only comply with complex Regulators' requirements, but help stakeholders to grasp your story. This delivery can influence decisions made by funders, donors, trustees, beneficiaries and regulators.

2. Insights which tackle today and tomorrow's conversation

We have an extensive event programme which spans across all nine of our industries. Much of our training focuses on specific function perspectives e.g. fundraisers and trustees ensures that those attending leave not only with an understanding but practical guidance on how to fulfil their responsibilities.

3. Practical solutions to your issues

We have seen the challenges and opportunities of working in your operating environment and we are able to take pragmatic positions and make realistic assessments based on our demonstrable experience with each of our industries.

For more information visit
www.croweclarkwhitehill.org.uk

Crowe Clark Whitehill

KINGSTON SMITH

Running a not for profit organisation effectively is a challenging task in the current economic climate. The right professional advice can make all the difference, with the combined pressure of raising funds, managing your finances, meeting stakeholder demands and keeping on top of the constantly changing regulatory and legal framework.

Kingston Smith can help you meet all these challenges by delivering a comprehensive range of services specially tailored for the not for profit sector including auditing, accountancy, VAT and fundraising.

Kingston Smith have a multi-disciplinary, dedicated not for profit team which acts for over 700 charities and not for profit organisations of all types and sizes including:

- Grant giving trusts and foundations
- Arts and culture
- Overseas Aid
- Disability charities
- Religious organisations
- Medical/health
- Education

We can help your organisation develop and achieve its aims and objectives and will provide you with the right advice at the right time. We do this by providing you with a partner who is accessible, who will take the time to understand your organisation and who will lead a dedicated client service team to help you meet your objectives.

For more information visit
www.kingstonsmith.co.uk

Kingston Smith
Helping clients succeed

Charity Finance Group (CFG)
15-18 White Lion Street
London N1 9PG

0845 345 3192
info@cfg.org.uk
www.cfg.org.uk

Registered charity no. 1054914
Company no. 3182826