Advice For the Voluntary Sector CIC
www.afvs.org.uk

Data Protection Policy and General Data Protection Regulations (GDPR)

Daryl Martin

Revised
September 2017

Contents

Part 1: Data Protection Regulations

Introduction

As I write this introduction, I just called up a news report I sent out on Twitter last week; 11 charities have received fines ranging from £6,000 to £18,000. The Regulator wanted the fines to be higher given the gravity of the offences, but being mindful that these fines would come out of the pockets of donors, kept them low. It gets worse; the Charity Commission is now weighing in by making their own investigations into the offending charities. At least one charity is complaining about it being unfair; the others are, I suspect, getting their systems and practices overhauled.

The Fundraising Regulators Code of Conduct runs to almost 80 pages, with regular updates coming out. I have summarised it down to a dozen or so pages, still 5,500 words to get to grips with. You can find a copy of our summary on our website. We have included a Complaints Policy template in the Appendix. As a trustee or administrator, you need a working understanding of the Code and how it affects your charity. I also recommend you register with the Regulator. It is voluntary, but will put you in a better light if you do get a complaint against you.

Very important points to remember:

1. **Do not ever forget that data subjects have the legal right to see every reference to them that you have stored in your records (there are some opt outs in the small print, but nothing you should rely on). Do not ever put anything in writing that you would not wish them to see. (Charities are not covered under the Freedom of Information Act, but are covered under Data Protection law.)**

2. **Remember that your policy should include information stored on personal laptops, home computers and Smartphones. Policing them can be very difficult, so it is important that your team of staff and volunteers are well trained and well briefed.**

Part 1 of this publication is a draft Data Protection Policy. This is based on the Data Protection Act 1998. Next year when GDPR becomes law (A bill has just been introduced to merge the Data Protection Act and GDPR), this policy will need to be revised. We'll be aiming to come up with a fresh draft policy for you to look at.

This is a Data Protection Policy template, taken from the HMRC website.

(Name of Charity)

Data Protection Policy and Procedures

Introduction

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data).

Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The board, staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

Board members staff and volunteers who have access to personal information, will be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the [charity] commitment and procedures for protecting personal data. The board regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s),

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary,

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information [Group] will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

Data Subject/Service User – The individual whose personal information is being held or processed by [Group] (for example: a service user or a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

(a) racial or ethnic origin of the data subject
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) trade union membership
(e) physical or mental health or condition
(f) sexual orientation
(g) criminal record
(h) proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioners Office (ICO) about the data processing activities of the [Group]. Note: Not-for-profit organisations are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group.

Applying the Data Protection Act within the charity

Whilst access to personal information is limited to the staff and volunteers, Volunteers may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Responsibilities

The [charity] is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information.
b) Meet its legal obligations to specify the purposes for which information is used.
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
d) Ensure the quality of information used.
e) Ensure that the rights of people about whom information is held, can be fully exercised under the Act.
   These include:
   i) The right to be informed that processing is being undertaken
   ii) The right of access to one's personal information
   iii) The right to prevent processing in certain circumstances, and
   iv) The right to correct, rectify, block or erase information which is regarded as wrong information
f) Take appropriate technical and organisational security measures to safeguard personal information,
g) Ensure that personal information is not transferred abroad without suitable safeguards,
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
i) Set out clear procedures for responding to requests for information.

The Data Protection Officer on the management committee is:

Name _____

Contact Details _____

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
b) Everyone processing personal information is appropriately trained to do so
c) Everyone processing personal information is appropriately supervised
d) Anybody wanting to make enquiries about handling personal information knows what to do
e) Dealing promptly and courteously with any enquiries about handling personal information
f) Describe clearly how the charity handles personal information
g) Will regularly review and audit the ways it holds, manages and uses personal information
h) Will regularly assess and evaluate its methods and performance in relation to handling personal information

All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Data collection: Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Data Subject:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

Procedures for Handling Data & Data Security

Under the data protection act 1998, companies and charities have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the data protection act.

It is therefore important the all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and

observe the guidance given below.

Operational Guidance

Email:

All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use.

Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed,
  be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.

- Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.

Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of site, preferably in the boot. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords:

Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

- Common sense rules for passwords are: do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Information Regarding Employees or Former Employees

Information regarding an employee or a former employee, (or volunteer or trustee for that matter should be kept indefinitely). If something adverse did come up many years later you might want to refer back to a job application or other document to check what was disclosed at the time.

I recommend that the trustees decide what their policy will be, minute their rationale, and stand on it. This should keep them safe as far as insurers or the law are concerned.

Data Subject Access Requests

Members of the public may request certain information from public bodies under the Freedom of Information Act 2000. The Act does not apply to charities, but we are still required to respond to requests for information under the Data Protection laws.

Disclosure

We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person
b) The Data Subject has already made the information public
c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
d) Monitoring for equal opportunities purposes – i.e. race, disability or religion
e) Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. If a customer is housebound and receives regular visits from a volunteer – ensure the list is securely stored and remove customer details when they change or the customer no longer receives the service. We will review the list annually, and will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to the charity please contact the Data Protection Officer:

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

Part 2: Preparing for and Implementing GDPR

Briefing No.1: General Data Protection Regulations (GDPR): Setting the Scene

Guest blog by Dr Gary Wills, Southampton University

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. The UK Government has confirmed that Brexit will not affect the implementation of the GDPR, the Great Repeal Act means it is likely to be converted into British Law.

The GDPR is applied to organisations that are either controllers of the data or those processing the data. As in the current DPA if you are a controller you are responsible for how and why personal data is processed and as a processor you are responsible to act on the controller's behalf. However, in the GDPR the processor now has a specific legal obligation to maintain records on what personal data they are processing and the processing activities. Therefore, under GDPR both the controller and processor now have defined legal responsibilities. For most charities, they are both the controller and owner.

There has been a lot in the press about the scale of the fines that can be levied against organisations. Whilst true, they are mainly referring to large corporations, however the Information Commissioner's Office (ICO) do fine charities and in April 2017, they announced that they had fined 11 charities between £6,000 and £18,000. These were '*significantly reduced'* so as not to cause stress to donors, but under the GDPR it is said to increase substantially.

In the GDPR, personal data has been redefined and is now covers a much wider scope, including new areas such as IP addresses, CCTV, biometrics. The GDPR also covers a 'special category of personal data, referred to as sensitive data and may only be processed only within a limited number of circumstances. The principle that underpin GDPR are ones that we would all hope that people will carry out with our own data. From Article 5, personal data shall be (paraphrased):

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes;
c) adequate, relevant and limited to what is necessary;
d) accurate and, where necessary, kept up to date;
e) kept for no longer than is necessary;
f) processed in a manner that ensures appropriate security of the personal data.

Buried in these principles are some very important new requirements. For example, Informed consent, that the information on which the consent was given is informative, unambiguous, and is given freely. In addition, consent can be withdrawn. Data from children (under 16) requires authorisation from a parent or guardian, and the controller is to make all reasonable efforts to obtain this.

There are now a number of rights of the individual:

1. Right to be informed: we must provide 'fair processing information',

2. Right to Access: confirmation that their data is being processed; access to their personal data; and other supplementary information
3. Right to rectification: people can correct incorrect information.
4. Right to erasure: that is to be forgotten.
5. Right to restriction of processing: we can store but not process the data
6. Right to portability: to take and reuse their personal data across a range of services
7. Right to object.
8. Right to decision making: people can object if a human is not in the loop on a decision about them.

As part of the GDPR, charities must provide a Data Protection Impact Assessment (DPIA). The DPIA identifies the specific risks to personal data as a result of processing activity and must be undertaken whenever there is a change in processes, technology, or new activity within the charity.

A Data Protection Officer (DPO), is not required by a charity unless it is processing a large amount of Data and then it could share the service of a DPO. Unfortunately, the word 'large' is not very well defined and could mean as little as 500 data subjects. However, a DPO does provide several functions that a charity may want to consider: a single point of contact for data subjects, independence from the operation, conduct audits, provide advice on data protection impact assessments.

There are two interrelated processes required for the implementation GDPR.

1. Design of systems and processes which secure the data
2. Design of systems and processes, which ensure that data is managed properly.

The ICO will accept an organisation complying with Cyber Essentials as meeting the requirement for securing the data. Cyber Essentials is a scheme developed by the UK Government (with advice from GCHQ) and industry to give a clear statement of the basic controls to mitigate against internet based threats.

The Information Assurance for Small and Medium Enterprises (IASME) Governance standard was developed in order to create a cyber security standard which would be an affordable and achievable alternative to the international standard, ISO27001. IASME Gold has been used by many charities to demonstrate that they have the systems and processes, which ensure that data is managed properly. Included in this standard is the assessment against the GDPR requirements, enables charities to say they are **GDPR READY**.

Service provided by Cyber Essentials: we spend one whole day with your organisation to identify:

- The key areas of security that you need to address and explain how to address these and give support in answering the question on the portal.
    - To identify the areas within the management process that will show that you have an information assurance process that is committed to 'privacy by design'
    - The organisation's responses to the questions are managed through our secure on-line portal, enabling the organisations to complete the assessment with ease and a pace that suits them.

On successfully completing the assessment, the organisation can display the Cyber Essentials badge and the IASME Gold logo on their website and other publicity material.

The organisation is entitled to the complimentary cyber security insurance.

This is the first of a series of briefings on GDPR.

This briefing was prepared for AFVS by Dr Gary Wills BEng, PhD, CEng, MIET, PHEA, and Carl Wills, Forti5 Technologies (Pvt) Ltd

Briefing No.2: GDPR Overview

You'll be hearing a lot about GDPR over the coming months. It's effective from May 2018, but charities must start to get prepared now. It's going to affect every charity that collects and stores personal data. Bigger charities, and those that store a lot of personal data will need to appoint their own Data Protection Officer (DPO), whose job it will be to see that the charity is compliant with the regulations. The DPO can be someone on staff or an outside consultant or company. The requirement for a DPO is that they are competent and have sufficient independence to be able to operate effectively.

To help small to medium charities prepare for GDPR, AFVS will be issuing a series of numbered briefings. to guide you through to an understanding of what needs to be done to stay safe. If you need specific guidance please write or telephone and we will do our best to help.

This briefing is general guidance to put you in the picture.

What's the current legal framework? The Data Protection Act 1998. This will be superseded by General Data Protection Regulation which comes into force on May 1st, 2018

What's the significance of GDPR? It's not in fact a huge departure from the Data Protection Act; rather it updates and adds to the existing framework. The major changes are:

Requirements for consent are more rigorous

Consent is a very hot topic, especially within fundraising. The GDPR seeks to ensure that consent is given and given freely, which means the subject must have a choice and isn't forced to give unnecessary details in the process of a transaction. Consent must be informed and specific, with clarity on how to opt in and out, and about how the data will be used. Lastly, a subject must actively confirm that they provide consent.

Requirement to delete data at the subject's request

GDPR implementation will bring with it the 'right to be forgotten' and the 'right to object'. All organisations must understand these rights and have processes in place to react to subjects invoking their rights, including, but not limited to, removing their consent and securely deleting their data.

Requirement to notify authorities within 72 hours of any data breach

There'll be a requirement on all organisations to report any personal data breach to the relevant authorities and, in some cases, to the individuals affected by the breach. The requirement to notify is for breaches that may result in a risk to the rights and freedoms of individuals and this includes events that, for example, may lead to financial loss, discrimination or loss of confidentiality. This means you will need to think carefully about how you store data.

Increased fines for failure to comply

There are two tiers of fines: 2% of total annual turnover or €10 million (whichever is higher) and, for the more serious infringements, 4% of annual turnover or €20 million (again, whichever is higher). **In practise, charities are not going to be hit with these levels of fines, unless they've been very silly indeed.**

GDPR will apply to all organisations, no matter where they are based and their size, if they offer goods or services (even if free) to individuals in the EU. In addition, despite Brexit, the ICO have confirmed that they are likely to implement similar rules after we have left the EU, to allow the United Kingdom to operate on a level playing field with the continent. All organisations should plan for, and be ready to comply with, the GDPR.

Briefing No.3: Preparing for GDPR: Twelve Steps to be Taken Now

1. Awareness

Are your trustees and operations team aware of the impact of the new regulations? They should at least be reading this series of briefings and GDPR should be on the agenda at board meetings. It's important that everyone understands the impact of what their actions on the overall impact of GDPR. For example, the fundraising team must factor the implications of GDPR in any plans they make; IT need to understand how any changes they might need to make affect GDPR. Everyone needs to understand what to do if they receive a SAR (in whatever guise it comes)

2. Data Protection Officer

Someone to be designated to take responsibility for compliance. Bigger organisations will need a formal appointment. Responsibility can be delegated but ultimate accountability will be held by the board. The person needs to be sufficiently competent and have sufficient independence to be able to be effective.

3. Information You Hold

You need to document what personal data you hold and why you hold it, where it came from and who you might share it with. You should also document how it is held, and how secure it is. An audit of storage and security will be needed, including passwords, shared uses, firewalls etc. Don't forget that laptops, smartphones, iPads, memory sticks and personal equipment used away from the office and in homes must be included. Appropriate and proportionate encryption is vital. Your IT manager will play a big part in gathering this information.

4. Communicating Privacy Information

Your privacy notices should be reviewed and plans made to make any changes needed.

5. Individual's Rights

Procedures to be checked to ensure that individuals' right are covered, including how you delete an individual's data, and how you provide them with data electronically.

6. Subject Access Requests

There are serious penalties for getting this wrong. A separate briefing has been issued (GDPR 4.) Might be worth running a 'mystery SAR' project to see that it works.

7. Lawful Basis for Processing Personal Data

Identify, document and update your privacy notice to explain

8. Consent

Review how you seek, record and manage consent, and make any changes needed. Refresh existing consents where necessary. All consents must be kept and accessible.

9. Children

Do you need systems put in place to verify ages and obtain parental/ guardian consent where necessary?

10. Data Breaches

Do you have systems to detect and report and investigate any breaches? (A separate briefing will be issued)

11. Data Protection by Design and Data Protection Impact Assessments

You should be familiar with the ICO Code of Practice and latest guidance from the Article 29 Working Party, and plan implementation.

12. International

If your charity operates across more than one EU member state you need to identify where the primary responsibility lies (i.e., the UK Regulator). Article 29 Working Party will help if more is needed on this.

Briefing No.4: Subject Access Requests (SARs)

In my last briefing, I mentioned that I'd be dealing with Subject Access Requests (SARs) in a future briefing. I can't do any better than use an excellent blog from the pen of Val Surgenor, charity law specialist at MacRoberts LLP. There's less than a year to go now before the GDPR comes into force, therefore you should act now to make sure you are GDPR compliant! It's important to understand SARs because they can impact any charity at any time and there are penalties if they aren't handled properly.

What is a SAR?

A SAR is a request for personal information that your Charity may hold about a data subject i.e. an individual. If an individual wishes to exercise their subject access right, the request must be made in writing. The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Act (DPA), individuals have the right to obtain confirmation as to whether personal data about them is being processed by your Charity. If personal information is being processed, they are entitled to access:

- **the reasons why their data is being processed;**
- **the description of the personal data concerning them;**
- **A copy of all records including e-mails where they are mentioned (see Appendix);**
- **information about anyone who has received or will receive their personal data;**
- **details of the origin of their data if it was not collected from them.**

Charities need to be mindful that the rules on subject access apply to any individual. Charities are likely to hold and process personal data about its trustees; its employees; service users; members; donors, volunteers and many others. Each category will have the same access rights.

Key Changes to SARs under GDPR

Under the GDPR, the procedure for making a SAR is similar to the procedure under the DPA. However, there are some key changes your Charity needs to be aware of which may require you to make changes to Charity's procedures:

Fees:

Under the DPA, your organisation can charge up to £10 for a SAR. **Under the GDPR, a request for personal information is free** unless the request is 'manifestly unfounded or excessive.' Your organisation can charge a 'reasonable fee' for multiple requests.

Impact: This may have a significant effect on your organisation where you receive large volumes of requests and this may result in an increase in administrative costs on your organisation. At present, there is insufficient guidance on what is meant by

“manifestly unfounded or excessive” and therefore your organisation should approach this with some caution.

It should also be recognised that the £10 fee may have acted in the past as an impediment to making a request and as a result, charities may see an increase in requests as a result.

Response time:

Under the DPA, you must respond to SARs within 40 days of receipt of the written request. Under the **GDPR, your organisation must respond to SARs within one month of receipt**. This deadline can be extended by a further two months where there are a number of requests or the request is complex but you must contact the individual within a month of receipt, explaining why the extension is necessary.

Impact: Charities will have a shorter time to deal with SARs; therefore, having an effective procedure in place will ensure that you are able to comply with the new reduced timescales. Being able to recognise a subject access request and pass it to the correct person in your Charity will be critical if you are to comply with the reduced timescales. Remember, for it to be a valid request, it doesn’t need to say it is a subject access request or even mention the DPA.

If staff have personal e-mail accounts where a SAR could be made to, these should be monitored when the member of staff is out of the office (for example when on holiday or on secondment) to ensure that SAR’s are dealt with quickly. Remember you will only have up to one month to respond, your Charity needs to have good procedures to make sure it complies on time and is able to provide the information that it needs to. **The ICO will take a serious view of any delay in providing the information if a complaint is made either to you or to the ICO.**

Provision of Information:

Individuals can make a SAR electronically. If they do so, the information provided should be in a commonly-used electronic format, unless otherwise requested. But remember your Charity must verify the individual’s identity prior to granting access to information. This can sometimes take a little time especially if it is a guardian or someone acting under a power of attorney who are seeking the information about a data subject.

In responding to a subject access request, the Charity will need to advise the data subject of:

- **the purposes of the processing;**
- **the categories of personal data concerned;**
- **who are the recipients to whom your Charity discloses the information;**
- **where possible, how long you will hold onto the information or what categories your Charity uses to decide how long the personal information will be held for;**
- **the right to request rectification, erasure or restriction of the processing,**
- **the right to lodge a complaint to the ICO;**

- **where the personal data are not collected from the data subject, the source from where your Charity obtained the data;**
- **and finally, the existence of any automated decision-making.**

Impact: Where your Charity doesn't already have a procedure for staff to identify a SAR and/or know how to escalate this to be dealt with – put a procedure in place and train staff accordingly.

Does your Charity have a data retention or data destruction policy? If not, put one in place – think about what data you hold and why – how long do you really need to hold it, and hold all of it? Be careful to consider why you want to hold onto data "just in case"? If your Charity has thought about what data it holds and how long it needs to hold it, this will assist in complying with the new information provisions.

Right to withhold Personal Data:

Under the GDPR, organisations can withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others.' It will be up to the UK government to introduce any further exemptions to SARs such as for national security, defence and public security. Charities should take advice if they are proposing to withhold information on this basis as your organisation will need to carefully consider its applicability and its use should not act to result in a refusal to provide all information.

Next steps

Design and implement template response letters so that you can ensure that all requirements of a response to a SAR are complied with under the GDPR.

Design and implement policies and procedures for handling SARs and ensure these take into account new timescales (including implementing a new data retention policy if your Charity doesn't already have one).

Ensure that employees are trained in dealing with SARs and that they can recognise when an individual has made a SAR and how this is to be dealt with.

Consider GDPR best practice and perhaps consider incorporating a 'data subject access portal' (where appropriate) which can allow an individual to access their information quickly easily and remotely.

Future briefings in this series will be issued to provide further guidance. Contact us for specific support and assistance.

Below is a further briefing on a specific report prepared for AFVS when we were working with a client charity to deal with a complaint which had escalated until a SAR was requested. As you will see it involved a considerable amount of time and also financial cost. A robust complaints policy will keep such unfortunate events to a minimum in your charity.

Subject Access Request: Briefing Note for a Charity Client (Identifying detail redacted)

This note has been prepared for the X in response to a subject access request from Y. It summaries the Charity's duties in responding to the request and sets out a suggested process for proper handling of the request in accordance with applicable statutory requirements and best practice guidance from the Information Commissioner's Office (ICO).

The note comprises the following sections

- Summary of the process for handling the request
- Timetable for complying with the request
- What aspects of the request are within the scope of a subject access request?
- What constitutes personal data?
- Finding and retrieving the relevant information
- In what circumstances may personal data be withheld?
- How should the information be given to the applicant?

Process

In handling a subject access request, the basic process is:

- Consider the scope of the request to determine exactly what information is being requested (see Section 3)
- Undertake a thorough search for all personal data within the scope of the request and collate all information that may potentially have to be disclosed (see Section 5)
- Consider whether any exemptions to disclosure apply (see Section 6)
- Once the information that will be disclosed has been identified, consider the appropriate form of disclosure (see Section 7)
- Disclose the information to the applicant (or in this case, to Z as the applicant's nominated representative)

Timetable

Organisations must comply with subject access requests 'promptly' and in any event within 40 calendar days. In this case, because it was necessary to obtain written confirmation that the applicant approved the request which Z had submitted on his behalf, the 40 days runs from the date on which that confirmation was received – 20 October 2016. This means that the full and final response to the request must be issued by no later than Tuesday 29 November 2016. ***Please note that in GDPR the 40-day period is reduced to one month; means you have no time to waste.***

What information was requested and what aspects of the request are within the scope of a subject access request?

The request can be broken down into three parts:

1. The policy and procedure that sets out the rules for suspension and expulsion: This is not within the scope of a subject access request as, to the extent that such policies and procedures exist, they are of general applicability and do not contain any

information that specifically relates to the applicant. However, any such policies and procedures could be disclosed voluntarily (outside the request) if desired

2. Minutes of the meetings in which the decisions to suspend and in effect expel X from the charity were made:
To the extent that the any meeting minutes relate to the applicant, those sections of the minutes will likely be within the scope of a subject access request and it will be necessary to consider whether such information must be disclosed.

3. Disclosure of all files, electronic and paper, notes, records including agendas and minutes of meetings, all records of telephone conversations that were in any way about or making reference to Y and his concerns:

To the extent that such records exist and contain personal data about the applicant they will be within the scope of a subject access request and it will be necessary to consider whether this information must be disclosed. Note however that the scope of the request is relatively narrow – i.e. in my view, it is not a request for all information held by the Society in respect of the applicant; but only for information held which relates to the applicant in the context of the concerns that he raised (and the subsequent dealings/ correspondence with the Society).

What constitutes personal data?

In most cases, it should be fairly straightforward to identify whether particular information constitutes personal data. There are two key factors to consider:

Is it 'data'? In this context, there are essentially two types of information that will be regarded as data:

- Information in electronic form;
- Information in manual form, held in a filing system. In determining whether information is part of a 'filing system' the key consideration is whether there is a structure to the record keeping which facilitates ready access to information and an understanding that the structure will be used whenever a new record is added to the information set.

Is it 'personal' data? For information to be personal data, it must relate to a living individual and allow that individual to be identified (either on its own terms or when considered alongside other information which the organisation holds or is likely to hold)

In collating the relevant information, it would be better to err on the side of caution in determining what is or may be personal data, and then make a more considered judgement in any cases of doubt.

Finding and retrieving the relevant information

In this case, given the fairly specific nature of the request and the fact that it relates to recent events, it should hopefully not be too difficult to collate all of the information required. It is suggested that a specific individual within the Society be given responsibility for handling the request, coordinating the search for information within the scope of the request and leading the consideration of any exemptions on disclosure that may apply.

In terms of finding and retrieving the relevant information, a common-sense approach should be utilised – however, this must be suitably thorough:

- Where might one reasonably expect to find information within the scope of the request?
- Which individuals within the Society should be asked to check for information held?
- What manual filing systems exist that might hold information?
- What electronic searches can be undertaken to find information within the scope of the request?
- It is very important to ensure that any information within the scope of the request is not amended, deleted or deliberately ignored or overlooked.

It is important to note that the duty to search for and identify personal data in response to a subject access request is broad in nature and the ICO's guidance repeatedly emphasises that an organisation is not permitted to exclude information from its response to a subject access request merely because it is difficult to access. The guidance states that organisations should be prepared to make extensive efforts to find and retrieve the requested information. There is some degree of caveat in that organisations are not required to do things that would be unreasonable or disproportionate to the importance of providing subject access to the information – however, there is a high threshold in determining that certain actions would fall into this category.

Further information about searching for relevant information is set out in Schedule 1.

Exemptions: In what circumstances may personal data be withheld?

There are exemptions which mean that personal data within the scope of a subject access request can legitimately be withheld. In most cases, there is discretion over whether to use an exemption – generally, you may choose to fully comply with a subject access request even if an exemption is available. If information is withheld in reliance on an exemption, it would be good practise to explain in the response to the applicant that information has been withheld and the reasons why. It is worth noting that in this specific context, there is perhaps a risk that seeking to rely on an exemption will exacerbate the situation and increase the likelihood of further challenge.

Several of the exemptions that are available apply only in specific contexts that are not likely to be relevant here. The main exemptions which may need to be considered are:

- Information containing personal data about a third party;
- Management information (personal data that is processed for management forecasting or management planning);
- Negotiations with the applicant (a record of intentions in negotiations with the applicant).

It is generally easier to consider exemptions in the context of specific information as they must be applied on a case-by-case basis in respect of each piece of information within the scope of the request. I would be happy to provide further advice on the applicability of exceptions in respect of specific information if that would be helpful, once the necessary information has been collated.

How should the information be given to the applicant?

A person making a subject access request only has the right to see their own personal data, rather than a right to see copies of the documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but you are not obliged to do this.

Once the personal data that is relevant to the request has been located and retrieved, it must be communicated it to the applicant in intelligible form. In most cases, the information must be supplied in permanent form.

Schedule 1: Searching for Information

The ICO has given guidance on specific types of records and how the duty to locate personal data in response to a subject access request applies in these contexts:

Archived information and back-up records in electronic form:
To the extent that an organisation's search mechanisms allow it to find archived or backed-up data for its own purposes, the same effort should be used to find information in order to respond to a subject access request

Information contained in emails:
The contents of emails stored on computer systems are a form of electronic record to which the general principles apply. For the avoidance of doubt, the contents of an email should not be regarded as deleted merely because it has been moved to a user's 'Deleted items' folder

Deleted information:
Information is 'deleted' when you try to permanently discard it and you have no intention of ever trying to access it again. If personal data held in electronic form is deleted by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean you must go to such efforts to respond to a subject access request

Information stored on personal computer equipment:
If staff, trustees or volunteers hold personal data on their own devices, they may be processing that data on behalf of the organisation, in which case it would be within the scope of a subject access request. In general, individuals do not need to be asked to search their private emails or personal devices in response to a subject access request unless there are good reasons to believe they are holding relevant personal data

Other records:
Whether information in hard-copy records is personal data accessible via the right of subject access will depend primarily on whether the non-electronic records are held in a 'relevant filing system'. Broadly speaking, a relevant filing system exists where information about individuals is held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.

Briefing No.5: Consent

1. The End of Passive Consent

1.1 One of the most significant impacts is the strengthened requirement for getting consent from someone to hold their data. Previously consent was defined as any freely given specific and informed indication of their wishes. In practice charities often relied upon the person's failure to opt out as evidence of his consent.

1.2 GDPR requires a positive, unambiguous, affirmative action. Anything less won't be acceptable. A ticked box will still work (not a pre-ticked box!), as will an active opt in. Consent must be capable of being withdrawn at any time.

1.3 Data controllers must now capture each consent, together with the version of the privacy notice that accompanied the consent, and hold it on file for later inspection. If only partial consent is given, the system must be capable of screening out any unauthorised use.

1.4 Note that 'Grandfather' consents won't be allowed, so any existing consents that don't meet GDPR requirements won't be valid after May 2018 and must be re-acquired.

1.5 Consents which depend on services which are conditional on the giving of consents will not be valid. (I can see this posing problems to big organisations.)

2. Legitimate Interests

2.1 As the consent rules become more stringent charities are likely to want to consider whether they can capture the data under the banner of legitimate interests. GDPR does allow legitimate interest processing but the tests are more stringent than before. For example, is it necessary for the performance of a contract or to comply with the law. It's a balancing act between the subjects right to privacy and the organisation's interests.

2.2 GDPR adds 2 requirements; transparency and internal documentation. The subject must be explicitly informed at the time of the purpose for which the data is collected and the legitimate interest which pertains. This must be embodied in the privacy notice. All this must be documented and kept as in 1.3 above together with the rationale for using a legitimate interest as the lawful basis for collecting the data.

Someone to be designated to take responsibility for compliance. Bigger organisations will need a formal appointment. Responsibility can be delegated but ultimate accountability will be held by the board. The person needs to be sufficiently competent and have sufficient independence to be able to be effective.

3. Transparency

3.1 GDPR focuses on the importance of transparency. Consent must be based on a written explanation couched in clear and plain language in an accessible form.

3.2 **This is a list of information to be included:**

- The controller's identity and contact information;
- The Data Protection Officer's (DPO) contact information;
- The purposes and legal basis of the processing;
- Details of the legitimate interests (if relied upon);
- Recipients of the personal data;
- Any intended transfer to a non-EU country and why;
- How long the data will be stored;
- Data subject rights;
- Ability to withdraw consent;
- Right to lodge a complaint and who to go to;
- Whether provision of data is required and consequences for failure;
- Whether automated decision-making is involved and the consequences to the data subject.

4. Subject rights

4.1 **Existing rights**

- Right of access;
- Right of rectification;
- Right to object;
- Right to object to direct marketing;
- Right not to be subject to automatic processing (Unless necessary to fulfil a contract or required by law).

4.2 **New or expanded rights**

- Right to be forgotten without undue delay;
- Right to restrict processing, especially where accuracy of data is contested, or no longer needed;
- Right of data portability (in a commonly used format);
- Right to object to processing for scientific, historical, or statistical processes.

5. Accountability and Requirement of a Data Governance Programme

5.1 Whereas the concept of accountability has until now been implied, it must now be evidenced. The evidence must be kept and available for inspection.

5.2 Every consent must be kept and available for inspection (1.3 above.) The record keeping will need to be extensive.

5.3 **Data Protection Officer (DPO)** A formal DPO must be appointed if a core activity of the charity consists of regular and systematic monitoring or processing of sensitive or criminal data on a large scale. (What is large scale is not defined but some authorities believe 500 entries to be 'large'). DPOs must have appropriate knowledge and skills and sufficient independence to perform their duties. Their duties will consist of advising colleagues, performing PIAs (Privacy Impact Assessments) and audits, monitoring compliance, cooperating with DPAs and serving as a contact point for data subjects.

5.4 The Data Controller (DC) must conduct a PIA for any processing that is likely to pose a high risk to individuals' rights. This must include a description of the planned processing, an analysis of the necessity for it, an assessment of the risks to privacy, and the measures that may be put in place to mitigate the risks to the rights and freedoms of the data subjects. If the risk is high the DPO must be consulted before any processing.

5.5 Privacy must be built into the design of the charity's products and services.

5.6 GDPR record keeping requirements are strict. They must include:

- Names and contact details of officials involved - DPO and DC;
- Categories of processing;
- Purposes of processing;
- Who will see the data;
- Retention periods;
- Description of security measures in place;
- Details of any cross-border transfers of information.

6. Data Breach Notifications

6.1 Under GDPR a data breach must be reported within 72 hours unless the controller can demonstrate that it's unlikely to result in risk to data subjects.

6.2 If there's a serious risk to data subjects they must also be notified. The risk would be the likelihood of fraud, or extreme distress or embarrassment.

6. Encryption is a likely panacea for breach notification obligations. If all breached data is encrypted the controller would not normally need to report it.

7. Summary

7.1 For the first time data processors have specific obligations. These will include the requirement to implement appropriate security measures and keep detailed records.

7.2 Under GDPR and violations carry the risk of fines and private rights of action.

With acknowledgements to Cameron Stoll, legal counsel and DPO for Blackbaud.
Blackbaud provide free resources including videos, blogs, and webinars to help charities be compliant.

Briefing No.6: Preparing for GDPR: FAQs Answered to Deepen our Understanding

1. When is the GDPR coming into effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive, it does not require any enabling legislation to be passed by government; meaning it will be in force May 2018. The government has just introduced a bill; presumably due to Brexit.

2. In light of an uncertain 'Brexit' - I represent a data controller in the UK and want to know if I should still continue with GDPR planning and preparation?

The simple answer is Yes. The UK will want to stay in step with the EU on this.

3. Who does the GDPR affect?

It will apply to all companies and charities processing and holding personal data.

4. What are the penalties for non-compliance?

Organisations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data, or violating the core of Privacy by Design concepts.

There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach, or not conducting impact assessment.

It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

5. What is personal data?

Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. This is a more comprehensive list than the existing Data Protection definition.

6. What is the difference between a data processor (DP) and a data controller (DC)?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

7. Do DPs need 'explicit' or 'unambiguous' data subject consent - and what is the difference?

The conditions for consent have been strengthened, as organisations will no longer be able to utilise long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous.

Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. However, for non-sensitive data, “unambiguous” consent will suffice.

8. What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent, but this will not be below the age of 13.

9. What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how.

It is important to note that the GDPR is a regulation, in contrast the previous legislation, which is a directive. When the UK bill becomes law, it will of course be binding.

10. Does my organisation need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of: (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data (Art. 37). If your organisation doesn’t fall into one of these categories, then you do not need to appoint a DPO.

Having said that, you must have someone in control of your processes, and they may as well be called the DPO, even though they may not carry the legal responsibilities of a formally appointed DPO. Also, I’ve not seen any definition of ‘large scale’. I’m advised that a Spanish court put it at 500 records; hardly large scale, but there we are.

11. How does the GDPR affect policy surrounding data breaches?

Data breaches, which may pose a risk to individuals, must be notified to the DPO within 72 hours and, if necessary, to affected individuals without undue delay.

Risk means physical, i.e. disclosing confidential home addresses, and risk of fraud etc. by 'losing' sensitive information.

Briefing No.7: Data Protection: What is Changing?

We already have pretty good Data Protection regulations in place. Why do they need changing and exactly what is being changed?

I shan't spend any time on the first question; they needed strengthening and they're being strengthened. This initiative is EU driven, but post-Brexit we will still want to make common cause with our EU friends.

The more important question is, what is new when the GDPR legislation is passed. It's still only a bill at present, but the final form isn't going to change much.

An overview of the main changes under GPDR and how they differ from the current regulations. This briefing is specifically for small to medium charities.

1. Increased Territorial Scope

Possibly the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR. It will apply to all organisations processing the personal data of data subjects residing in the EU, regardless of their location. Previously, territorial applicability of the directive was ambiguous and has led to a number of court cases. GPDR makes it very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.

The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to:

- offering goods or services to EU citizens (irrespective of whether payment is required), and
- the monitoring of behaviour that takes place within the EU.

Non-Eu businesses processing the data of EU citizens will have to appoint a representative in the EU.

2. Penalties

Organisations in breach of GDPR can be fined up to 4% of annual turnover. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

There's a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach, or not conducting impact assessment.

It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

3. Consent

The conditions for consent have been strengthened, and charities will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

4. Breach Notification

Breach notification will become mandatory where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, **“without undue delay”** after first becoming aware of a data breach.

5. Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

This change is a dramatic shift to data transparency and empowerment of data subjects. An SAR request must be actioned within 30 days (previously it was a month). This will require all charities to have a plan to put in place quickly whenever an SAR is received. (see earlier briefing).

6. Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

7. Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

8. Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall implement appropriate technical and organisational measures in an effective way. in order to meet the requirements of this Regulation and protect the rights of data subjects'.

Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

9. Data Protection Officers

This is actually a simplification; possibly the only one! The current requirements are a bureaucratic nightmare for big organisations. Under GDPR there will be internal record keeping requirements, and DPO appointment will be mandatory only:

- where there's regular and systematic monitoring of data subjects on a large scale, or
- of special categories of data, or
- data relating to criminal convictions and offences.

The DPO:
- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices. Small charities can be proportionate on this requirement.
- May be a staff member or an external service provider.
- Contact details must be provided to the relevant DPA.
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge.
- Must report directly to the board of trustees.
- Must not carry out any other tasks that could result in a conflict of interest. (Common-sense must prevail in a small charity.)

Briefing No.8: Legitimate Interests

As the consent rules become more stringent, charities are likely to want to consider whether they can capture the data under the banner of legitimate interests. GDPR does allow legitimate interest processing, but the tests are more stringent than before. For example, is it necessary for the performance of a contract, or to comply with the law? It's a balancing act between the subjects right to privacy, and the organisation's interests.

One of the six lawful grounds for personal data processing is the 'legitimate interests of the controller or third party'.

We'll look at general examples of legitimate interests, and more specific examples.

What are the six lawful grounds for data processing?

1. **Consent** of the data subject

2. Processing is necessary for the **performance of a contract** with the data subject, or to take steps to enter into a contract

3. Processing is necessary for compliance with a **legal obligation**

4. Processing is necessary to **protect the vital interests of a data subject, or another person**

5. Processing is necessary for the performance of a task carried out **in the public interest,** or in the exercise of official authority vested in the controller

6. Necessary for the purposes of **legitimate interests** pursued by the controller, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

What does 'legitimate interests' mean and how might it apply?

The term refers to the stake that the company processing the personal data may have in that processing. This may imply a benefit inherent in processing for that company itself, or perhaps for wider society.

A legitimate interest 'must be real and not too vague'. For example, it may apply to an organisation's data processing as part of fraud protection, security measures or transferring that data between different parts of an organisational group. Some of this may already be part of legal compliance.

These sorts of interests may seem reasonable to the average reader, and indeed the expectations of users is one of the elements that the ICO guidance earmarks for

consideration when a data controller is deciding whether to rely on legitimate interests.
Would or should a user expect the processing to take place? If there is an expectation, then the impact of the processing is arguably less than if no expectation was possessed.

1. Direct marketing

The GDPR states, 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

This may be where consent is not viable or not preferred, though organisations will still need to show that there is a balance of interests – their own and those of the person receiving the marketing.

Of course, any individual can object to direct marketing, and it is one of the examples of legitimate interests for which objection is already fairly well understood and easy to action (often by an unsubscribe link or by contacting the company in question).

2. Relevant and appropriate relationship

This may be a direct appropriate relationship, such as where the individual is a client or a member. Care needs to be taken on the content of the data collected. Most small charities such as churches, will simply collect names and addresses and any information needed to process gift aid claims. There'd need to be a rationale for information collected over and above this minimum. Small charities relying on legitimate interest need to carefully audit what information they hold and why. They might 'think' they hold minimum information, perhaps just simple names, addresses, phone numbers, e-mail addresses, but over time it's remarkable how much additional information can creep in, bank details, ethnic information, health details and so on. It may be that a certain amount of cleansing is needed.

3. Reasonable expectations

As previously discussed, if a controller understands individuals have a reasonable expectation their data will be processed, this may help to make a case for legitimate interests.

How about some more specific examples?

Aside from some of the more obvious cases where legitimate interests may apply – risk assessment, checking children's age, processing data to afford individuals rights – here are four specific example that may be pertinent for small charities:

1. **Members, subscribers, or customers will expect charities to hold their details.** This is legitimate as long as care is taken over what information is held.

2. **Suppression:** If a user objects to direct marketing, for example, a company may need to hold some personal data, however limited, in order to ensure no more information is sent to this user. This could be regarded as a legal obligation.

3. Direct marketing: Legitimate interest could include direct mail from a charity to existing supporters updating them on details of upcoming events.

4. Web analytics: For example, a social media platform using diagnostic analytics to assess the number of visitors, posts, page views, reviews and followers in order to optimise future marketing campaigns.

Web analytics is one area though where changes to the ePrivacy Directive of 2002 (to bring it in line with the GDPR) may complicate matters. Some Data Protection specialists feel that cookie consent is needed for third-party platforms such as Google Analytics:

Exemption for analytics cookies: Like the leaked draft, the Commission's [ePrivacy Directive] proposal retains an exemption from the cookie consent requirement for analytics. However, the exemption applies only for first-party analytics, not third-party analytics – so websites and apps using third-party analytics platforms like Google Analytics etc. will still need consent (even if, for the techies amongst you, the cookie is technically served from a first-party domain – third party here refers to the provider of the analytics service, not the domain from which the cookie is served).

5. Updating member/customer details and preferences

For example, a retailer using an external service provider to verify the accuracy of customer data. Controllers have to be careful here as to how such activity is carried out.

Significant fines have been handed out by the ICO to Flybe, Morrisons and Honda, which each broke the existing Privacy and Electronic Communications Regulations (PECR) flouting customers' marketing wishes, sending emails asking whether users want to change said marketing permissions (and even incentivising the behaviour).

How can charities be sure legitimate interest applies?

Though the GDPR doesn't list all circumstances in which legitimate interests may apply, it does specify that any processing under this banner must meet the balance of interest's condition – are the interests of the controller overridden by the interests or rights of individuals?

Individuals can object to data processing for legitimate interests (Article 21 of the GDPR) with the controller getting the opportunity to defend themselves, whereas where the controller uses consent, individuals have the right to withdraw that consent and the 'right to erasure'. This may be a factor in whether charities rely on legitimate interests.

If you are unsure about whether legitimate interests applies, your data protection officer will likely be undertaking a Legitimate Interests Assessment (LIA). We can help you with this.

In short, an LIA is split into three steps:

- The assessment of whether a legitimate interest exists;
- The establishment of the necessity of processing; and

- The performance of the aforementioned balancing test.

Regarding step three, factors under consideration include:

- the nature of the interests (such as the reasonable expectations of the individual);
- the impact of processing;
- any safeguards which are or could be put in place.

Privacy notices must provide clarity to the user

One of the main threads of the GDPR is providing clear and transparent information to individuals about the data collected, how it is processed, and the lawful basis for this processing.

This is no different where legitimate interests applies. It should also be made clear that individuals have the right to object to processing of personal data on these grounds.

Note that this article is not intended to construe legal advice or offer comprehensive guidance.

Acknowledgements to Ben Davis, www.econsultancy.com for parts of this briefing

Acknowledgements

The Open Government Licence:
https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

Dr Gary Wills BEng, PhD, CEng, MIET, PHEA, and Carl Wills, Forti5 Technologies (Pvt) Ltd

Cameron Stoll, legal counsel and DPO for Blackbaud.

Ben Davis, www.econsultancy.com

Advice For the Voluntary Sector CIC
Sovereign Centre, Poplars, Yapton Lane, Walberton, West Sussex BN18 0AS.
Email: support@afvs.org.uk – Web: www.afvs.org.uk