

GENERAL DATA PROTECTION REGULATION

*A toolkit for charities, voluntary organisations and
community groups*

Readership

VODA's remit is to support Voluntary and Community Sector groups that are based or which operate within North Tyneside, a vast majority of which are small or micro groups. In preparing this Toolkit we have concentrated on these groups and their limited resources and have attempted to make compliance with GDPR as easy as possible

Further Advice

North Tyneside Voluntary and Community Sector groups may contact us with specific problems or issues relating to data protection and the GDPR by sending an e-mail to admin@voda.org.uk Regretfully we are unable to assist groups based elsewhere.

Disclaimer

We have tried to be as accurate and as clear as possible in this brief review of the GDPR but the information in this document should not be regarded as legal advice. Whilst we have taken every care VODA cannot be held responsible for any errors or omissions. Please bear in mind that data protection is forever changing and you should consult the ICO's website for the latest information and guidance: ico.org.uk

The ICO's website also has checklists and other tools to help you better manage the data you hold.

Copyright and Distribution Rights

This document is the copyright of VODA which also holds the sole distribution rights. You should not make copies or redistribute this document. If you know of a group that would like a copy please refer them to us: admin@voda.org.uk

Version

V1.1 - 22 May 2018

© Copyright 2018 North Tyneside Voluntary Organisations Development Agency

Queen Alexandra Campus, Hawkeys Lane, North Shields NE29 9BZ Tel: 0191 632 2626



Contents

Introduction	3
How to use this Toolkit	3
1. What you need to know	
• The Six Principles	5
• Greater accountability	6
• Greater rights	7
2. Preparatory work	
• Do I need to register with the ICO?	7
• Data Controllers	7
• Data Processors	9
• Data Audit	10
• Privacy by Design and Default	10
• Review Current Privacy Notices / Statements	11
• Data Protection Officer (DPO)	11
• Keeping Records	12
• Security	12
• Awareness	12
3. Collecting and Processing Data	
• Consent	13
• Sensitive Data	14
• Privacy Notices / Statements	16
• Children	17
4. Access to Data	
• Subject Access Request (SAR)	18
• Data Subject's Rights	18
5. If it all goes wrong	
• Data Breach Notification	20
6. Glossary	21
7. Annexes	
A: Key Elements of a Data Protection Policy	23
B: Checking Compliance with the Six Principles	24
C: Guidance for Data Controllers and Data Processors	25
D: Undertaking a Data Audit	31
E: Undertaking a Data Protection Impact Assessment (DPIA)	33
F: Lawful Basis for Processing	35
G: Template for Writing a Privacy Statement	39
H: Procedure for dealing with a Subject Access Request (SAR)	47
I: Procedure for dealing with a Data Breach	50

Introduction

The EU-wide General Data Protection Regulation (GDPR) comes into force on 25 May 2018 but the good news is that you do not have to have everything in place by then. Providing you are abiding by the UK's own Data Protection Act 1998, and you can demonstrate that you are making sufficient progress towards GDPR, then you have a strong defence should the worst happen. GDPR should not be applied retrospectively.

You may be wondering if it is worth the UK changing to the GDPR. After all, aren't we leaving the EU in a couple of years? The reality is that the GDPR is very likely to remain largely intact, will be absorbed into UK law through the Government's Data Protection Bill and may even be strengthened in certain areas.

GDPR is not about rebuilding data protection from the ground up. It is an evolution of what already exists and replaces the 1995 European Data Protection Directive. Over the last 23 years there have been huge changes in the way we collect, store and use personal data, driven by developments in IT – computers, tablets, mobile phones and, of course, the Internet – and by a growing realization that information about individuals is precious and vulnerable to exploitation, whether it is unwanted marketing e-mails or criminal gangs trying to illegally access bank accounts. The new Regulation takes into account these developments, the greater risks that new technology brings, and the concerns of the public over the security of their personal details. As a result, you may have to improve your approach to data but this toolkit should make that task a lot easier.

This booklet will provide you with a basic understanding of the new Regulation and how it may affect your organisation, but it is mainly intended to give you the practical tools to help you work towards compliance. For more detailed information try the Charity Finance Group's excellent publication *General Data Protection Regulation: A Guide for Charities* available from www.cfg.org.uk

GDPR comes into force on 25 May 2018.

“25 May is not the end. It is the beginning.”

**Elizabeth Denham,
Information Commissioner**

How to use this Toolkit

This Toolkit is in two parts. The first part provides background information which may help you in deciding how to complete the various templates that make up the second part of the Toolkit. The templates are listed as Annexes.

The table below may help.

<ul style="list-style-type: none"> ○ Essential information about the GDPR. ○ Definition of “data” ○ Individuals’ rights ○ Accountability 	<ul style="list-style-type: none"> ● Section 1: What you need to know ● Annex A: Key Elements of a Data Protection Policy
<ul style="list-style-type: none"> ○ The Principles on which the GDPR is based. 	<ul style="list-style-type: none"> ● Section 1: What you need to know ● Annex B: Checking Compliance with the Six Principles
<ul style="list-style-type: none"> ○ Registering with the ICO. ○ Roles and responsibilities of Data Controllers and Data Processors. 	<ul style="list-style-type: none"> ● Section 2: Preparatory Work ● Annex C: Guidance for Data Controllers and Data Processors
<ul style="list-style-type: none"> ○ Taking stock of what data you have. 	<ul style="list-style-type: none"> ● Section 2: Preparatory Work ● Annex D: Undertaking a Data Audit
<ul style="list-style-type: none"> ○ Protecting people’s privacy. ○ Keeping records. 	<ul style="list-style-type: none"> ● Section 2: Preparatory Work ● Annex E: Undertaking a Data Protection Impact Assessment (DPIA)
<ul style="list-style-type: none"> ○ When you are allowed to collect and process data. 	<ul style="list-style-type: none"> ● Section 3: Collecting and Processing Data ● Annex F: Lawful Basis for Processing
<ul style="list-style-type: none"> ○ What you must tell people about the data you collect and process. ○ Special considerations when dealing with children and those who may be unable to give consent. 	<ul style="list-style-type: none"> ● Section 3: Collecting and Processing Data ● Annex G: Writing a Privacy Statement
<ul style="list-style-type: none"> ○ Individuals’ rights to access the data you hold about them. 	<ul style="list-style-type: none"> ● Section 4: Access to Data ● Annex H: Procedure for dealing with a Subject Access Request (SAR)
<ul style="list-style-type: none"> ○ What to do if someone illegally accesses your data, you lose a laptop or USB containing data or you lose data. 	<ul style="list-style-type: none"> ● Section 5: If it all goes wrong ● Annex I: Procedure for dealing with a Data Breach

1. What you need to know

The GDPR will apply to all organisations that are holding personal data on individuals in the EU including the UK. The GDPR has greater transparency and accountability at its core than the existing European Data Protection Directive. A major change is that data processors – any organisation or person that processes data on your behalf – can be liable to prosecution if they do something wrong, whereas previously they were immune. Other aspects of the new Regulation are given below.

Definition of Data

The definition of “data” is often given as facts or figures, or information that is stored in or used by a variety of different forms. For the purposes of the GDPR, the term is used to mean “personal data” – any information relating to an identified or identifiable individual (such as a name, an identification number, location data, an online identifier or to information specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person).

You should already have a Data Protection Policy in place which governs the use of personal data within your organisation. The Policy should be reviewed at regular intervals – at least every three years and more frequently if there has been an incident, a change in the way you process data or a change in the law. **Annex A** outlines Key Elements of a Data Protection Policy.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible.

The Six Principles

The GDPR is based on six guiding principles:

1. Lawfulness, fairness and transparency
 - Data should be processed lawfully, fairly and in a transparent manner.
2. Purpose limitation
 - Data should only be collected for specific, explicit and legitimate purposes.
3. Data minimisation
 - Data should be adequate, relevant and limited to what is necessary.

4. Accuracy
 - Data should be accurate and, where necessary, kept up to date.
5. Storage limitation
 - Data should be kept only for as long as is necessary.
6. Integrity and confidentiality.
 - Data should be processed in such a way as to ensure the integrity of the data and the confidentiality of the data subjects.

Further details of how these Six Principles are used in conjunction with the GDPR are given at **Annex B**.

Greater Accountability

The onus is very much on organisations to understand the risks that they create for data subjects, and to mitigate those risks. You are expected to create a culture of privacy and put in place comprehensive but proportionate governance measures. Appropriate technical and organisational measures should be implemented such as passwords, the encryption of electronic files, internal audits of processing activities, policy reviews and staff training.

Processing activities should be documented and these records must be kept up to date.

Additional accountability measures are required for:

- public bodies
- high risk processing
- organisations that employ more than 250 staff.

As part of the emphasis on greater accountability, failure to process data legally can result in a fine of up to €20m (approximately £17m but subject to change) or 4% of total turnover, whichever is the greatest amount. However, the Information Commissioner's Office (ICO) points out that fines are only issued as a last resort and, of the 17,300 cases investigated in 2016-17, only 16 resulted in fines. The ICO has a number of other sanctions it can impose, such as warnings, reprimands and corrective orders, and will work closely with organisations to help them bring their data protection measures up to the required standard.

Greater rights

The GDPR includes a number of important rights for individuals including the right to...

- rectification where data is erroneous.
- erasure where the data no longer serves a useful purpose.
- restrict processing to prevent, for example, unwanted marketing material.
- data portability to enable data subjects to switch between service providers such as health and social care providers, banks, utility companies, etc
- object to the processing of data because of the above mentioned rights.
- object to automated decision making such as profiling.

2. Preparatory Work

Do I need to register with the ICO?

The Information Commissioner's Office provides a quick and easy online assessment to help you determine whether you need to register with the ICO:

<https://ico.org.uk/for-organisations/register/self-assessment/>

Identify your Data Controllers and Data Processors

You need to identify your Data Controllers and Data Processors. As the names imply, the Data Controller controls why and how personal data should be processed, whilst the Data Processor carries out the actual processing of the information.

Data Controllers

A Data Controller can be either an individual or an organisation, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. It can sometimes be difficult to distinguish between the Data Controller and the Data Processor: *control*, rather than *possession*, of personal data is the determining factor.

From a practical, day-to-day aspect of running a charity or community group it makes sense to appoint someone to lead on data protection and who will instigate change when required. Leaving data protection to 'the organisation' could mean that changes are not implemented and you run the risk of falling foul of the law.

Data Controllers have duties and obligations. To comply with obligations under the GDPR, Data Controllers have to take appropriate organisational and technical measures to protect data subjects and their rights. They need to demonstrate that they have

implemented such measures to ensure data protection by design (i.e. built-in technical safeguards) and by default (processing only personal data which are necessary for a specific purpose).

Data Controllers' obligations may include:

- The maintenance of records of all processing activities.
- Consulting and co-operating with supervisory authorities.
- Ensuring a level of security.
- Notifying the Information Commissioner's Office (ICO) in the event of a data breach.
- Conducting a Data Protection Impact Assessment *but only where the loss or misuse of data could have serious consequences for the data subjects*. Data Controllers have to ensure that a Data Protection Impact Assessment has been carried out on any 'high risk' processing activities before those activities begin.
- Appointing a data protection officer if the organisation is a public body or are involved in large scale monitoring
- Assisting data subjects with exercising their rights to privacy and data protection.

There are also specific obligations regarding the transfer of data outside the EU. If you use Office 365 or Google Docs, Facebook or Twitter, to name but a few, then you may well be transferring data abroad without realizing it.

Data controllers need to consider the risks to data that are transferred outside of the EU (which, for data protection purposes, includes Norway, Liechtenstein and Iceland).

The European Commission has so far recognized Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate data protection. The USA is also recognized but limited to the Privacy Shield framework (visit the following site: <https://www.privacyshield.gov/welcome>, follow the links to Privacy Shield companies and type in, for example, Microsoft).

The ICO has a Controller's Checklist which will help you to think about some of the issues involved in this role:

<https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/>

Data Processors

Data Processors process personal information about data subjects on behalf of the Data Controller (but the term does not apply to staff directly employed by the Data Controller). If you store your digital data on a third party computer, e.g. on 'the cloud', then the third party is the processor.

Data Processors act on documented instructions from the Data Controller to;

- Ensure confidentiality, assist with legal compliance of the Data Controller and respond to requests from data subjects.
- Make available all information necessary to demonstrate compliance of the Data Controller.
- Take measures to assist the Data Controller with ensuring security of processing.
- Treat personal data after processing as per the instructions of the Data Controller.

Data Processors cannot make decisions on the choice of purposes and means in data processing. Processors are required to maintain records of personal data and processing activities.

You could be both a Data Controller and a Data Processor. For example, if you work in partnership with another organisation you may have to process data on people which the other organisation refers to you, e.g. monitor and report on beneficiaries' progress, making you a Data Processor. But you are also likely to be a Data Controller in that you may employ your own staff and perhaps run your own projects with other beneficiaries. You therefore need to determine whether you are a Data Controller, a Data Processor or both. If you are a Data Processor, make sure you draw up a formal agreement with the Data Controller allowing you to process the data and take responsibility for that processing. The bullet points in this and the previous section will help you structure your agreement.

In some situations you may be a joint Data Controller with another organisation. This could happen where you are involved in helping to move people closer to the employment market, for example. Another organisation may be responsible for the recruitment of the beneficiaries but they may hand them over to you for training or as a volunteer placement, at which point their responsibilities end. You are both Data Controllers and, again, you should draw up a formal agreement specifying who does what. Think about, for example, who is responsible for criminal record checks, if needed.

Again, the ICO provides a useful checklist for Data Processors:

<https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/processors-checklist/>

Further details on the processes that you need to undertake to designate a Data Controller and/or Data Processor are given at **Annex C**.

Data Audit

You should undertake an audit of all personal data that you hold. In particular consider...

- Personnel files including staff and volunteers.
- Attendance lists, e.g. people who have visited your building, participated in a class or project, been involved in an activity, etc.
- Membership information.
- Newsletter subscriber information.
- Recipients of marketing material.
- Surveys and evaluations that identify individuals either at the point of data collection (i.e. people filling in their personal details as part of a survey) or at the analysis stage (i.e. people mentioned in evaluations such as in case studies).
- Correspondence, complaints, e-mails, etc.
- IP addresses of people accessing your website.
- Whether the information is shared with third parties such as a funder.

The GDPR cannot be applied retrospectively. However, being aware of how you have collected and processed data in the past may highlight weaknesses that you should address in the future.

Consider whether the information you hold is:

- Necessary – are you collecting information but not doing anything with it?;
- Current – is the information so old as to be effectively obsolete?; and...
- Secure – are you keeping personal information under lock and key, password protected or encrypted, and how do you ensure only authorised people have access?

Further details of the steps to take in carrying out a Data Audit are provided at **Annex D**.

Privacy by Design and Default

When considering your data audit you should always ask yourself whether there is start-to-end protection for people's privacy. And when you introduce new systems, privacy measures should be an integral part of the basic design. This could include, for example, restricting who has access to personal data perhaps by password protecting the relevant files. If beneficiaries provide information to you online then ensure that it is encrypted so that, even if your website is hacked, the information will be unreadable.

Consider privacy at its most basic level. Do you get people to sign in when they visit your premises? If you are providing, for example, debt advice then your beneficiaries may not want to be identified: so that simple signing in sheet does nothing to protect their privacy. Do you call out their names when it is time to see the adviser? Again, their privacy is compromised. What happens if you are recruiting new staff? Can they see the names of previous candidates who have signed in? And do you space out the candidates so no two people from the same organisation are likely to bump into each other?

Does your photocopier retain a memory of what's gone through it? Will the supplier wipe that memory when you give up the machine and provide you with a certificate to confirm that it has been wiped? Similarly with your computers. Do you just throw them away without electronically shredding all the files on the hard drive?

Do you still have a fax machine? How do you destroy the carbon film that produces the faxes? This type of data is often overlooked and you should have procedures in place to guarantee privacy.

If you carry out bulk or high risk processing in which a data breach could have serious consequences for the security, freedoms and rights of individuals then you must carry out a Data Protection Impact Assessment (DPIA) – see [Annex E](#).

Review Current Privacy Notices / Statements

Review your current arrangements for providing information to beneficiaries about how you use their information – see *Privacy Notices / Statements* in the next section.

Data Protection Officer (DPO)

The appointment of a Data Protection Officer is required only if

- Processing is carried out by a public authority or body.
- The core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale.
- The core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Now whilst this would exclude most charities you do need to be aware that if you have a contract with a public body involved in the activities stated above then you may be subject to the DPO's authority. DPOs monitor compliance with the GDPR, advise whether training is required and suggest improvements to data protection, among other things.

Keeping Records

In order to demonstrate compliance with GDPR you should keep records of:

- Data audits
- Processing including written procedures and guidance for staff to follow (but see below)
- Policies relating to data protection and reviews of policies and procedures
- Induction records for new staff
- Relevant training records
- Records of incidents: what happened, how the incident was handled and the outcome
- Data Protection Impact Assessments
- Contracts that exist between yourselves and your data processors

Article 30 of the GDPR obliges Data Controllers to maintain records of all processing activities. These records need to be in writing (including in electronic form) and must be made available to the ICO on request.

Data Controllers can be exempted from this obligation when they have no more than 250 employees except where

- a) the processing may pose a risk to Data Subjects' rights and freedoms
- b) the processing is not occasional
- c) the processing includes special categories of personal data (Article 9) or...
- d) the data relate to criminal convictions and offences (Article 10).

Security

You should be able to demonstrate that you have appropriate and proportionate security measures in place and that they are periodically updated and tested. This could involve proving that anti-virus software is regularly updated, that passwords are changed regularly and that the integrity of individual files has not been compromised. Think also about keeping only the minimal amount of data – the more data you collect, the greater the risk – and that you have anonymized records where appropriate.

Awareness

Finally, you should make your staff – both employees and volunteers – aware of key aspects of the new Regulation such as the need to issue privacy statements, keeping data up to date, etc. Make sure you keep records of any data protection training.



3. Collecting and Processing Data

Consent

Organisations, if challenged, will be required to prove that they have obtained the necessary consent of the data subject to process their personal data.

“Opting-out” is banned: people must “opt-in” and you may need to give this some consideration.

Example of what is and what is not acceptable

We will send you regular updates about our charity and the work we do. If you do not wish to receive this information please tick here: <input type="checkbox"/>	
If you wish to receive regular updates about our charity and the work we do please tick here: <input type="checkbox"/>	

If you deal with children then the consent of an appropriate adult, such as a parent or legal guardian, may need to be obtained. Only children aged 13 or over are able provide their own consent (this is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). See the section on **Children** below.

You should also think about how you are going to obtain consent from other people who may not easily be able to give it, in particular people...

- with disabilities
- who have learning difficulties
- who are unable to understand English
- who use a different alphabet, such as Cyrillic
- who have mental health issues including those who have phobias, e.g. those who have an irrational fear that you are collecting their information in order to harm or manipulate them.

You should avoid the use of “vital interests” as justification for processing data: this is reserved for life and death situations where information is disclosed to a hospital or medical professionals.

Obtaining explicit consent is not the only legal basis for processing data. There are six categories in all shown below with their GDPR clause identifier:

6(1)(a):	Consent of the data subject.
6(1)(b):	Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
6(1)(c):	Processing is necessary for compliance with a legal obligation.
6(1)(d):	Processing is necessary to protect the vital interests of a data subject or another person.
6(1)(e):	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(1)(f):	Processing is 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.

Remember, GDPR cannot be applied retrospectively. This means that if you have previously obtained consent from beneficiaries then you are not required to obtain consent again, e.g. if you have a database of beneficiaries or donors then you should be able to continue to use it. However, you can only use the data for the purpose for which it was collected, so if that purpose has changed then you should obtain new consent. Furthermore, you are required by data protection laws – both the GDPR and the UK Data Protection Act – to keep data up to date so now is a good time to cull your databases.

Sensitive Personal Data

What used to be called “sensitive personal data” - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership genetic data, biometric data used to uniquely identify natural persons (e.g. voice recording), health data, data concerning an individual’s sex life and sexual orientation – are now referred to as “sensitive personal data.”

In order to process sensitive personal data you must satisfy one or more of the following conditions in addition to consent (the codes in the left hand column relate to the sections in the GDPR):

9(2)(a):	Explicit consent of the data subject has been given, unless reliance on consent is prohibited by EU or Member State law.
9(2)(b):	Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
9(2)(c):	Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
9(2)(d):	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
9(2)(e):	Processing relates to personal data manifestly made public by the data subject.
9(2)(f):	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
9(2)(g):	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
9(2)(h):	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
9(2)(i):	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
9(2)(j):	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

See also **Annex F: Lawful Basis for Processing**

Privacy Notices / Statements

You are now required to provide a privacy statement to data subjects, and this must be done when you collect their personal data. That could be, for example, when someone...

- becomes a member of your organisation
- agrees to donate funds on a regular basis
- provides personal information such as gender, age, etc, say for equalities monitoring
- signs in as part of your fire safety procedures
- applies for a vacancy
- accesses your website

You may provide a short statement that covers the basics of why you collect the information, what you do with it and how the data subject can access it, but you must also provide a more detailed statement or, at the very least, easy access to one. This detailed privacy statement should include:

- the identity and the contact details of the Data Controller and Data Protection Officer (if applicable)
- the purposes of the processing for which the personal data are intended
- the legal basis of the processing
- where applicable, the legitimate interests pursued by the controller or by a third party
- where applicable, the recipients or categories of recipients of the personal data;
- where applicable, that the Data Controller intends to transfer personal data internationally
- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period
- the existence of the right to access, rectify or erase the personal data,
- the right to data portability
- the right to withdraw consent at any time
- and the right to lodge a complaint to a supervisory authority

If the data is provided by a third party then you also need to provide:

- details of the source from which the personal data originate
- the existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

That may seem like a lot of information to give someone but our ***Writing a Privacy Statement*** template, **Annex G**, should help.

Think about your membership application process, especially if people can join online. The Regulation requires you to ensure that potential members are aware of their rights and why you process their details. You should consider a system in which the application process cannot be completed until the applicant has accessed and accepted the privacy statement.

If you electronically capture someone's IP address – the unique Internet Protocol number that identifies every device linked to the Internet – then you are potentially identifying an individual. For example, the cookies¹ you use on your website might record someone's IP address. In these circumstances you need to tell people that you are using cookies and what information the cookies capture. Some cookies do not record IP addresses. Speak to the person or company who designed your website so you have a clear understanding as to how your cookies work.

Your privacy statement should be written in plain, easy to understand language: legalese is definitely out!

Children

GDPR provides significantly improved protection for children, particularly online. Children are often less aware of the risks of sharing their data and may be more susceptible to marketing.

You should ensure that any privacy notices specifically aimed at children can easily be understood by the relevant age group.

The GDPR has a default age of 16 years for children but the UK Government wishes to lower the age to 13 years. The Government is proposing that children aged 13 years and older may give their consent, providing they have the mental capacity to do so, e.g. you should consider whether they may have learning difficulties. Children under the age of 13 cannot give consent except where a charity is offering preventative or counselling services directly to children. If you rely on a '*legitimate interest*' in order to process children's data then you must strike the right balance between the rights and freedoms of children (who should always be regarded as being vulnerable) and the need for your charity to deliver a service.

¹ Cookies are small files which hold data about a website's visitors, such as which pages they have viewed. They are often used for analysis and tracking.

The GDPR makes specific mention of information society services – online services such as social media, shopping, mobile apps, etc – and stresses that, if you are offering such services, not only should you obtain parental consent for children who are underage but that you are required to make ‘reasonable efforts’ to ensure that consent is genuine.

4. Access to Data

Subject Access Requests

As with previous data protection legislation data subjects may request copies of all data held on them. However, the £10 administration fee has been abolished in most cases and the information should now be provided free of charge except for repeated and excessive requests where a reasonable fee may be charged.

Information should be sent to the data subject within one month of the request, except for complex requests which have a two month limit. You should let the data subject know if the information will take longer than a month to provide.

You must make reasonable efforts to ensure that the person requesting the information is the data subject, or someone representing the data subject who has obtained the necessary authority.

The process for dealing with a Subject Access Request is detailed at [Annex H](#).

Data Subjects’ Rights

Data Subjects have certain rights including the right...

- of access to a copy of the information held on them;
- to restrict the processing of data;
- to object to processing that is likely to cause or is causing damage or distress;
- to prevent processing for direct marketing;
- to object to decisions being taken by automated means;
- to data portability;
- in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- to withdraw consent at any time;
- to lodge a complaint with the Information Commissioner’s Office;
- to claim compensation for damages caused by a breach of the Regulation.

Notes:

- a) The right of access. Data Subjects have the right to obtain from Data Controllers confirmation as to whether or not their personal data are being processed. They may access their personal data and find out the purposes of the processing.
- b) Data Subjects are entitled to know the categories of personal data being collected, stored and processed.
- c) There is the right to know the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- d) Data Subjects are entitled to know the period for which the Data Controller is planning to store the personal data. If this is not possible, they should be advised of the criteria that will be used to determine the retention period.
- e) Data Subjects have the right to request from the Data Controller rectification or erasure of personal data, or restriction of the processing of personal data, or to object to such processing.

There are six grounds on which the Data Subject may request erasure of their personal data:

1. Retention of the data is no longer necessary in relation to the purposes for which the data were collected or processed.
2. The Data Subject withdraws their consent, and there is no other legal ground for processing.
3. The Data Subject objects to the processing, and there are no overriding legitimate grounds for this processing.
4. Personal data have been unlawfully processed.
5. Personal data must be deleted in order to comply with the legal obligation in European Union law or the law of EU Member States to which controllers are subjected.
6. Personal data have been collected in relation to the offer of information society services to children.

This right to erasure is, however, not applicable...

- When the processing is necessary for the exercise of the right to freedom of expression and information.

- When the processing is required for compliance with a legal obligation of the Data Controller under European Union Law, or that of its Member States, that requires the processing, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in a Data Controller.
- For reasons of public interest in the area of public health and for achieving purposes in the public interest, scientific or historical research purposes, or statistical purposes.
- For the establishment, exercise, or the defence of legal claims.

5. If it all goes wrong

Data Breach Notification

A “data breach” covers a breach of security leading to the destruction, loss, alteration, unauthorised or accidental disclosure of, and access to, personal data. You must notify the Information Commissioner’s Office if the breach is likely to result in a risk to the rights and freedoms of individuals such as being discriminated against, reputational damage, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Notification should be within 72 hours of the breach being discovered. You may also be required to notify the data subjects. For further details see the ***Procedure for Dealing with a Data Breach*** at **Annex I**.

The ICO only issues fines in the most serious of cases – less than 0.1% - preferring instead to work with organisations to bring their data protection up to the required standard. If you contact the ICO early, are able to demonstrate that you take data protection seriously, you have identified the risks and taken steps to mitigate them, you stay on top of developments and you are able to show the ICO the completed necessary paperwork when asked then this will all count in your favour.

6. Glossary

Data Breach

A breach of security leading to the destruction, loss, alteration, unauthorised or accidental disclosure of, and access to, personal data.

Data Controller

An individual, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data Portability

The right for an individual to obtain and reuse their personal data for their own purposes across different services. The transfer of personal data should be easy, safe and secure without affecting its usability.

Data Processor

An individual, public authority, agency or any other body which processes personal data on behalf of the *Data Controller*. This definition does not include employees of the Data Controller.

Data Protection Impact Assessment (DPIA)

A systematic method of assessing the potential impact on data subjects of processing bulk or high risk data that could affect an individual's security, freedom and rights.

Data Subject

An individual to which the data or information relates.

ICO

Information Commissioner's Office (see below).

Information Commissioner's Office (ICO)

The UK's regulatory body established to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

Legal Person

A private or public organisation (see also *Natural Person*).

Natural Person

A person who is a human being (see also *Legal Person*).

Personal Data

Any information relating to a living person who can be directly or indirectly identified because of the information.

Privacy Shield

A data protection framework to which US companies must comply in order to satisfy current EU requirements.

For further information visit <https://www.privacyshield.gov/welcome>

Privacy Notices / Statements

Information made available to data subjects advising them of how you process their data and what rights they have in relation to processing, retention or data, withdrawal of permission, etc. The language should be simple enough for a 13 year old to understand.

Process / Processing

Operations performed on personal data, or on sets of personal data, by manual or automated means. This could involve:

- Obtaining it.
- Recording it.
- Storing it.
- Updating it.
- Sharing it.

Sensitive Data or Sensitive Personal Data

Now called *special categories of personal data* (see below).

Special Categories of Personal Data

Previously called *sensitive data* these categories include information relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data used to uniquely identify natural persons
- health data
- data concerning an individual's sex life
- sexual orientation

Annex A: Key Elements of a Data Protection Policy

You should have a data protection policy in place which should be reviewed at regular intervals – at least every three years and more frequently if there has been an incident, a change in the way you process data or a change in the law.

There are 16 key elements to a good data protection policy. The policy should specify:

1. What data your organisation processes.
2. Who has access to the data.
3. What format the data is in, how it is stored and how it is backed-up.
4. Why you process the data.
5. To what types of data the policy applies.
6. Who is responsible for processing the data.
7. The main data risks faced by the organisation.
8. Key precautions to keep the data safe.
9. How the data is kept up to date.
10. The retention period for the data, if known.
11. How data will be destroyed.
12. How to deal with a Subject Access Request (SAR).
13. Under what circumstances will the organisation disclose data and to whom.
14. How the organisation keeps the data subjects informed about the data it holds.
15. How to deal with a data breach.
16. A policy review schedule.

Annex B: Checking Compliance with the Six Principles

You should check the data you hold against the Six Principles that underpin the General Data Protection Regulation:

1. Lawfulness, fairness and transparency
 - a. Data should be processed lawfully, fairly and in a transparent manner.
 - Think about the legal basis for processing the data – use the procedure provided in this toolkit.
2. Purpose limitation
 - a. Data should only be collected for specific, explicit and legitimate purposes.
 - Are you clear on these issues? Have you documented the limitations?
3. Data minimisation
 - a. Data should be adequate, relevant and limited to what is necessary.
 - A data audit should include the criteria in 2 and 3.
4. Accuracy
 - a. Data should be accurate and, where necessary, kept up to date.
 - How do you keep data accurate? Personal data typically degrades – goes out of date – by about 30% per year, so a contact database could contain largely obsolete data in just three years. Do you have a systematic method of updating the data? Have you budgeted for updating the data?
5. Storage limitation
 - a. Data should be kept only for as long as is necessary.
 - Have you specified retention limits on each of your data sets? Who checks the data against these limits?
6. Integrity and confidentiality.
 - a. Data should be processed in such a way as to ensure the integrity of the data and the confidentiality of the data subjects.
 - What safeguards do you have in place to protect the data and the Data Subjects? How do you dispose of obsolete data? Simply deleting a file from a computer does not actually destroy it.

Annex C: Guidance for Data Controllers and Data Processors

You need to determine who the Data Controller and who the Data Processor is for the various data streams within your organisation. If you are a small constituted community group and the only data you hold is a list of members then this process is likely to be fairly simple: the group is probably the Data Controller and you process your own data, but if you use Office 365 or Google Docs then the information you send to those sites is processed by them – so they are the Data Processors. If the group is not constituted then the Data Controller may be the chair, president or some other such office.

For larger organisations the situation is more complex and you are likely to have to look at each data stream in some detail. For example, your bank may process data relating to payments to your staff. E-mails may be virus and content checked by software that feeds data back to the software company; Facebook processes the information you post on your pages and Twitter processes your tweets. If you subscribe to a voicemail service that operates from The Cloud then the processing will be by the company who provides that service. And if you use a travel agent to buy rail or air tickets for staff then the travel agent will be the processors of any information you pass to them that contains details of the traveler.

You could also be a Data Processor. For example, if you are involved in moving people toward employment then you could have a situation whereby another organisation recruits the beneficiaries and then passes their details to you so you can train them.

The list below is by no means exhaustive but will help you think about areas where personal information is processed and whether you are the Data Controller or Data Processor.

Area	Notes
Advice	You are likely to be the Data Controller for advice given to people who have approached you directly, but you could be the Data Processor if you are part of a partnership to which beneficiaries are referred for advice.
Banking	Think about any transactions that identify your staff and other individuals. The bank is the Data Processor.
Blogs	Do you use a third party service, such as WordPress, to publish your blogs and are readers encouraged to add their comments? The third party will be the Data Processor.
CCTV	If you have CCTV to protect your staff and premises is it on a live feed to a security company? The security company will be the Data Processor.

Area	Notes
Complaints	Do you use an external arbiter to deal with complaints? The arbiter is the Data Processor.
Contact Database	Is your database on The Cloud? The provider of cloud services is likely to be the Data Processor.
Contracts	If you are contracted to provide services to specific individuals then <i>you</i> are likely to be the Data Processor for any personal information with which you are provided.
E-mails	Are your e-mails virus and content checked and is this information sent back to the e-mail provider? The software company may be the Data Processor.
Event Management	Do you use an event management site such as Doodle or Eventbright? The event management site is the Data Processor.
Facebook	Facebook is the Data Processor.
Funders	Do you provide personal data to your funders? The funder may be the Data Controller if they specify the purposes and means of processing the data.
Health Provider	e.g. BUPA, Simply Health, etc, They are the Data Processors.
Helpline	If you provide a helpline do you capture the caller's telephone number and is that information processed by the provider of your phone service? The phone service provider is likely to be the Data Processor.
Live Chat	You may use a third party provider to process any live chat facility you have, in which case they are the Data Processor.
Marketing Information	Do you use a third party to send out your marketing literature? They are the Data Processor
Mobile Phones	Where mobile phones are provided to staff their locations can be tracked. They mobile phone company is the Data Processor
Office 365	Microsoft is the Data Processor.

Area	Notes
Online Backup	If you back up your files from your PC or server to an off-site location then the provider of the backup is the Data Processor.
Online Surveys	Do you use Survey Monkey or some other web-based survey company? The survey company is the Data Processor.
Payroll	Do you use a payroll bureau? The payroll bureau is the Data Processor.
Pension Provider	Who provides the pension scheme for your staff? The pension provider may be the Data Controller is the determine the purpose and means of collecting the data and you may be the Data Processor (it is the who Data Subject is in a contract with the pension provider).
Personnel Records	Are your personnel files shared with an HR contractor? The contractor is the Data Processor.
Publication subscribers	Are your e-publications sent out via MailChimp, Adestra, etc? Are your hard copy publications dispatched by a fulfilment company? These companies are Data Processors.
Recruitment	Do you use a recruitment agency to help you find staff or a temp agency to fill temporary vacancies? The agency is the Data Processor.
Social Media	Perhaps you use a third party to manage your social media? They are the Data Processor.
Student placements and interns	You are likely to be the Data Processor for students' details that are on placement with you.
Suppliers	Do you send suppliers contact details of staff? Do you use translators? These companies are Data Processors.
Travel arrangements	A travel agent may process various information about your staff from just their name, if they require a train ticket, to passport number if they need to fly. The travel company is the Data Processor.
Twitter	Twitter is the Data Processor.

Area	Notes
Vehicle Tracking	Do you have any vehicles and are they tagged to allow them to be tracked? This information could identify an individual's location. The tracking provider is the Data Processor.
Voicemail	If you have voicemail on your phone system are the recordings held on your computer or on the computers of the voicemail provider? If the messages are stored on a computer belonging to another company then they are the Data Processor.
Volunteer Files	You are almost certainly the Data Controller for the data you hold on your volunteers.
Website, cookies, hosting, page processing, etc	<p>If personal data is passed through or posted on your website then consider who hosts the website as the Data Processor.</p> <p>What data do your cookies collect? Do they capture visitors IP addresses which could identify individuals? This is likely to be processed by Google Analytics.</p>

Step 1: Look at the list above. Which apply to you? Are you the Data Controller or the Data Processor? Complete this table (leave the last column for now).

Data Area	Controller or Processor?		Contract?
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Data Controller's Obligations

Data Controllers control data processing and determine the *purposes and means*. With this come duties and obligations. You should have a Role Description for the Data Controller based on the information below (if there is more than one Data Controller you must be specific about their areas of responsibility).

Controllers must take appropriate organisational and technical measures to protect data subjects and their rights (GDPR Article 24). They need to demonstrate that they have implemented such measures to ensure data is protection by design (i.e. has built-in technical safeguards) and by default (processing only personal data which are necessary for a specific purpose).

Typically, Controllers' obligations include:

- To maintain records of all processing activities (Article 30).
- To cooperate and consult with supervisory authorities such as the Information Commissioner's Office (Article 31).
- To ensure an appropriate level of security (Article 32)
- To notify the Information Commissioner's Office in the event of a data breach (Article 33).
- To conduct a Data Protection Impact Assessment *but only where* the loss or misuse of data could have serious consequences for the Data Subjects. Controllers are to ensure that a Data Protection Impact Assessment has been carried out on any '*high risk*' processing activities before they begin (Article 35).
- To appoint a Data Protection Officer if required. This is only applicable to public bodies and large scale or regular monitoring of Data Subjects (Article 37).
- To assist Data Subjects with exercising their rights to privacy and data protection (GDPR Chapter III).
- There are specific obligations when personal data is transferred outside the EU (GDPR Chapter V).

Responsibilities of Data Processors

Data Processors also have responsibilities and these should be included in a Role Description: Typically, Data Processors:

- Act on documented instructions from the Data Controller.
- Ensure confidentiality.
- Assist with legal compliance of the Data Controller and make available all information necessary to demonstrate compliance of the Data Controller.
- Take measures to assist the Data Controller with ensuring the security of processing.
- Respond to requests from Data Subjects.
- Follow the instructions of the Data Controller once the data has been processed, e.g. safe storage, destruction, etc.

Step 2: Check existing contracts and implement new contracts where none exist.

The Controller - Processor Contract

Where another organisation processes the data then a contract should be in place between you covering the Data Processor role descriptions given above. In many cases, if you buy into or use an established service, such as Officer 365, then you automatically accept the contract on offer – though it is always a good idea to read through the contract.

If you are working in partnership with another organisation, perhaps on a new contract for which you have been awarded funding, then you can fashion your own contract in line with the responsibilities shown above. If you use a fundraising organisation the Fundraising Regulator has issued guidance on contracts at:

www.fundraisingregulator.org.uk/4-0-working-third-parties

Step 3: Go back to the table above (page 28) and tick the *Contracts?* column once a contract is in place.

Annex D: Undertaking a Data Audit

Undertaking a Data Audit is a key element of good data protection. Your initial thoughts are probably that you have a good idea of how much data your organisation holds, but you may be surprised once you start to unpick the data.

Step 1: Consider what personal data you hold

There are several personal data areas that you need to consider, including:

- Employees and potential employees
- Volunteers and potential volunteers
- Contact database e.g. for marketing, keeping track of funders, etc
- Advice provision
- Practical help
- Accounts and payroll
- Training and workshops

Perhaps the best way to undertake an audit is to sit down with each member of staff and record what data the access and how they use it. Bear in mind that staff sometimes create their own data sets. For example, they may put together an e-mail distribution list of details of beneficiaries or a set of mailing labels. Or they may keep notes about their experience with individual beneficiaries. That then raises the question as to whether your beneficiaries have given their permission for their data to be used in this way.

Step 2: Create a table of what personal data you hold, how it is used and who can access that personal data

Once you have gathered the data you then need to put it into a format that makes sense to you and, equally important, to the Information Commissioner’s Office should they wish to see it. The easiest way is to construct a table as shown in the examples below. This could also help you with Subject Access Requests when you need to find all the data you have on a particular individual.

Example: Data Audit of Advice Service

What data we hold	Where the data came from	What we use the data for	Where the data is held	Who has access to the data
For people who approach us for advice, either as individuals or on behalf of an organisation, we may hold: <ul style="list-style-type: none"> • The enquirer’s 	Provided by the enquirer by: <ul style="list-style-type: none"> • E-mail • Phone • Web form 	We use the information given to assess the nature of the enquiry and to provide appropriate advice.	<ul style="list-style-type: none"> • In-house server Backup at ABC Ltd. • Office 365 (encrypted). • E-mail system. 	<ul style="list-style-type: none"> • All appropriate staff involved in providing advice or compiling statistics.

What data we hold	Where the data came from	What we use the data for	Where the data is held	Who has access to the data
name. <ul style="list-style-type: none"> • Contact details including phone number, e-mail address, postal address and details of other methods of contact. • The date of the enquiry. • The nature of the enquiry. • The advice we give. • Subsequent outcome (if known). 		We may share the information among our staff to ensure the enquirer benefits from specialist advice. With the enquirer's permission we may share the information with external people and organisations.		

Example: Data Audit of Employees

What data we hold	Where the data came from	What we use the data for	Where the data is held	Who has access to the data
Personnel records relating to: <ul style="list-style-type: none"> • Recruitment • Support and supervision • Sickness • Performance • Disciplinary • Grievance • Salary including bank details • Redundancy • Attendance • Holidays • Training 	Application form submitted by the employee. References from previous employers. Recruitment agency.	Personnel records are held to effectively manage the employment of staff.	Hard copies of personnel files are held in a secure filing cabinet in the HR office. Password protected and encrypted digital files are stores on Office 365.	<ul style="list-style-type: none"> • CEO • Line Manager • Staff Member • Chair of the Board of Trustees • Payroll Administrator (salary information) • Bank (payment of wages and expenses)

Tip: Although some people use Excel spreadsheets to compile tables like the ones shown above, using Word is a less risky option. First, Excel is not really designed for storing text data – spreadsheets are really for calculations – and, second, it is so easy to delete the contents of a cell without realizing it.

Annex E: Undertaking a Data Protection Impact Assessment (DPIA)

You may need to carry out a Data Protection Impact Assessment (DPIA) where the processing is likely to result in a "high risk" to the rights and freedoms of data subjects. This is likely to apply to extensive automated processing and largescale use of special categories of data, i.e. sensitive personal information. The obligation to conduct a DPIA is on the Data Controller. The DPIA should be carried out at an early stage in any new project or planned change in processing methods. Not only is it an integral part of privacy by design it is a key component in helping you demonstrate compliance with the Regulation.

The types of processing requiring you to undertake a DPIA include, for example, when you intend to use systematic and extensive evaluation using automated methods, process large amounts of special categories of personal (i.e. sensitive) data, and the monitoring of public areas on a large scale.

Step one:

Explain what the project aims to achieve, describe the processing operation and its purpose. Assess the necessity and proportionality of the processing and what the benefits will be to the organisation, to individuals and to other parties.

Step two:

Describe the information flows. You should describe how information is collected and from whom, how it will be stored and processed, with whom it will be shared, and how it will be disposed of when it is no longer required. A flow diagram may make this easier to explain. Specify how many people are likely to be affected by the project

You should explain what steps you need to take to identify and address privacy risks such as consultation with both internal and external stakeholders. Think in terms of the risks to the rights and freedoms of data subjects. Insert these steps into your project planning and management.

It is good practice to consult on the practical implications with people who will be using the information.

Step three:

Identify key privacy risks and any other related risks such as compliance and reputational risks (see table on next page).

Privacy Issue	Risk to individuals	Compliance risk	Other risks
Explain what the issue is.	Who is going to be affected and how? Consider, for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.	Conduct a compliance check against the GDPR and other relevant legislation such as the Privacy and Electronic Communications Regulations (PECR), Human Rights Act, etc	Assess the organisational risks, including regulatory action and fines, reputational damage and the loss of public trust.

Step four:

Identify privacy solutions. Explain what needs to be done to minimize the risks and show compliance with the GDPR. If it is not possible to adopt measures to mitigate the risks then you must consult the Information Commissioner’s Office.

Risk	Solution(s)	Result	Evaluate
State the risk. Use full sentences such as <i>“Unauthorised access to special categories of beneficiary data puts them at risk of bogus phone calls and visitors”</i> : don’t just put <i>“Data hack”</i> .	Devise ways to reduce or eliminate privacy risks. Apply the 4T method of Risk Management: <ul style="list-style-type: none"> • Transfer the risk e.g. to a specialist. • Terminate the risk e.g. by not doing whatever is causing the risk. • Treat the risk e.g. by putting safeguards in place • Take the risk e.g. where other methods of risk management would be out of proportion to the risk. 	Describe what the result is likely to be by implementing the solution. Bear in mind that you may only be able to offer a partial solution and residual risks may remain.	Assess whether the final impact is justifiable, compliant and proportionate. Be prepared to change tack if a better solution becomes apparent. Regard risk management as an ongoing process. Review at regular intervals.

More guidance can be found at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

Annex F: Lawful Basis for Processing

Step 1: Make sure you have a lawful basis for processing personal data

Before you can process data you must have a lawful basis for doing so. There are six criteria that allow you to lawfully process data, but if you also intend to process sensitive personal data then you must also satisfy at least 10 conditions.

Six Criteria for the Lawful Processing of Personal Data	
6(1)(a)*:	Consent of the Data Subject.
6(1)(b):	Processing is necessary for the performance of a contract with the Data Subject or to take steps to enter into a contract.
6(1)(c):	Processing is necessary for compliance with a legal obligation.
6(1)(d):	Processing is necessary to protect the vital interests of a Data Subject or another person.
6(1)(e):	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(1)(f):	Processing is 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.

*These codes refer to the relevant clauses in the GDPR legislation.

In many cases you will rely on the first criterion, that of consent of the Data Subject. You must, however, make sure that consent is freely given; that the request for consent is clear and intelligible and not presented in impenetrable legalese; and that it is clearly distinguishable from other matters. It must be as easy to withdraw consent as it is to give it.

Relying on the last clause, 6(1)(f) legitimate interests, is often problematic in that any negative impact on the rights and freedoms of an individual can invalidate the lawful basis for processing. Any charity found to be spuriously applying this clause could face at least reputational damage and a possible claim for damages.

Step 2: Make sure you have a lawful basis for processing any ‘*sensitive personal data*’

Certain data is regarded as ‘*sensitive personal data*’ or more correctly ‘*special categories of personal data*’. This is data on:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data used to uniquely identify natural persons
- health data
- data concerning an individual’s sex life
- sexual orientation

If you intend to process ‘*sensitive personal data*’ then, in addition to the six criteria in the table above, you must also satisfy at least 10 conditions as shown in the table below.

Ten Conditions for the Lawful Processing of Sensitive Personal Data	
9(2)(a)*:	Explicit consent of the data subject has been given, unless reliance on consent is prohibited by EU or Member State law.
9(2)(b):	Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
9(2)(c):	Processing is necessary to protect the vital interests of a Data Subject or another individual where the Data Subject is physically or legally incapable of giving consent.
9(2)(d):	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
9(2)(e):	Processing relates to personal data manifestly made public by the Data Subject.
9(2)(f):	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
9(2)(g):	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
9(2)(h):	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical

Ten Conditions for the Lawful Processing of Sensitive Personal Data

diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

9(2)(i): Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

9(2)(j): Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

*These codes refer to the relevant clauses in the GDPR legislation.

In some circumstances you are likely to find that processing is covered by more than one criterion or condition from the tables above. Take, for example, your employment records. These are typically covered by:

Criterion / Condition	Explanation
6(1)(a): Consent of the Data Subject	The recruit has completed an application form and other documents explicitly giving you consent to process their employment data.
6(1)(b): Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.	You are clearly entering into an employment contract with the recruit and need to process their data to fulfil that contract.
6(1)(c): Processing is necessary for compliance with a legal obligation.	As an employer you are subject a number of legal obligations such as the provision of earnings information to HM Revenue & Customs, personal data to your pensions and health service provider, etc.
9(2)(a): Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.	May be required for the staff member to pursue Trades Union duties, or providing health information to protect those working in areas where there is a risk to health.
9(2)(b): Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.	Similar to 6(1)(c).

Step 3: From your data audit construct a similar table to record the Lawful Basis for Processing of Personal Data as shown below:

What data we hold	What we use the data for	Lawfulness & Conditions ⁽¹⁾	Notes
Personnel records relating to: <ul style="list-style-type: none"> • Recruitment • Support and supervision • Sickness • Performance • Disciplinary • Grievance • Salary including bank details • Redundancy • Attendance • Holidays • Training 	Personnel records are held to effectively manage the employment of staff.	<p>6(1)(a) – Consent of the data subject.</p> <p>6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.</p> <p>6(1)(c) – Processing is necessary for compliance with a legal obligation.</p> <p>9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.</p> <p>9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.</p>	<p>By completing and signing:</p> <p>a) a Job Application Form</p> <p>b) a letter confirming acceptance of the Terms & Conditions of Employment and</p> <p>c) a Payroll form...</p> <p>...the Data Subject is deemed to have accepted [6(1)(a) & 9(2)(a)] the need for the charity to collect and process information about them [6(1)(b)] in order for the organisation to perform its legal and contractual obligations as a responsible employer [6(1)(c) & 9(2)(b)].</p> <p>Some data is obtained from external sources, e.g. Tax Code from HMRC, pension details from pension provider.</p> <p>Retention</p> <p>6 years after termination of employment except for:</p> <p>Pension records,</p> <ul style="list-style-type: none"> • 12 years after benefits cease. <p>Employment dates, Workplace accidents, Medical reports (COSHH), Sickness records,</p> <ul style="list-style-type: none"> • 40 years after termination of employment.

⁽¹⁾You don't have to record each criterion in full; you just need to make sure that others understand what criteria you are relying on. You could just use the clause identifiers, e.g. 6(1)(a), or shorten the description to "Consent", "Contract", "Legal obligation" etc.

Having identified the lawful criteria and conditions for processing you also need to specify how these are met in practice: e.g. how is consent actually obtained? Detail this in the Notes column and also add information on retention.

Step 4: Consider how long personal data is to be kept

The GDPR does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that *“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”*. You should therefore review the length of time you keep personal data and record how long that information will be kept in the Notes column. You should be aware, however, that there are legal requirements on the retention of certain records relating to employees. Fire Warden training records, for example, should be retained for 6 years after termination of employment (Fire Precautions [Workplace] Regulations 1997) as should medical reports (Medical Reports Act 1998), etc.

Annex G: Template for Writing a Privacy Statement

When you collect data about your beneficiaries, visitors and even staff you must provide them with a privacy statement. Initially, you may provide an abridged privacy notice covering the basics, but you must also provide a more detailed privacy statement or at least easy access to one. Privacy notices and statements should be written in plain language and be clear enough for a 13 year old to understand.

The example below shows you how to construct a full privacy statement. The *Requirement* column is simply the criteria you must include: it is only the information in the Privacy Notice column that you would actually publish.

Example: Simple Privacy Statement for a Small Organisation

Requirement	Privacy Statement
The identity and the contact details of the Data Controller and Data Protection Officer (if applicable).	<p><i>North Shields Hobnobblers (NSHN)</i> takes your privacy very seriously. This Privacy Statement explains why and how we collect information about you, how we use it and what we do with it when we are finished. If you have any questions or concerns please contact our Data Controller:</p> <p>Data Controller: North Shields Hobnobblers Name of Charity: North Shields Hobnobblers Address: 100 Any Street, North Shields NE30 0AA</p> <p>Phone number: 0191 123 4567 E-mail address: chief.officer@northshieldshobnobblers.mail.co.uk</p>
The purposes of the processing for which the personal data are intended.	<p>When you approach us to become a Member we need to gather some basic information about you. This is to ensure that we provide information and services that meet your needs.</p> <p>“Data Subjects” i.e. people who become Members of NSHN, will be asked to provide/confirm their personal and/or sensitive personal data as required. By providing this information the Data Subject consents to NSHN collecting, processing and storing this information.</p> <p>We may also collect other personal sensitive information about you such as your gender, ethnicity, etc. We do this</p>

Requirement	Privacy Statement
	<p>for monitoring purposes to prove to our funders that we are reaching a broad cross-section of the local community. When we collect this type of sensitive information we anonymize it. We keep your name and address separate from the sensitive data so no one can link the data to you.</p> <p>Appropriate security measures are or will be in place to ensure that all personal and sensitive personal data is held and processed confidentially.</p>
<p>The legal basis of the processing</p> <p><i>(Where applicable, the legitimate interests pursued by the controller or by a third party).</i></p> <p><i>(If the data is provided by a third party then you also need to provide [a] details of the source from which the personal data originate and [b] the existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject).</i></p>	<p>We will ask you to give us permission to collect and process your information. We do this by asking you to sign a consent form.</p>
<p>Where applicable, the recipients or categories of recipients of the personal data.</p>	<p>NSHN handles personal data in compliance with the General Data Protection Regulation and recognises the importance of correct and lawful processing.</p> <p>The personal data you provide will only be used for official NSHN business.</p> <p>NSHN discloses information to a variety of third parties; these include but are not limited to:</p>

Requirement	Privacy Statement
	<ul style="list-style-type: none"> ○ Relevant authorities dealing with emergency situations at NSHN. ○ Any other authorised third party to whom NSHN has a legal/contractual obligation to share data with. <p>Disclosure of certain personal data may also be made to other entities not listed above. This will only ever be done in accordance with the GDPR. Your consent will be sought where necessary.</p>
Where applicable, that the controller intends to transfer personal data internationally.	NSHN uses computerised records linked to “The Cloud”: computer servers based overseas which enables our staff to access your records, even when they are not in the office. This helps us to provide you with an efficient service. This means that we may transfer your data abroad but only to Member States of the European Union, countries recognized by the European Commission as having adequate data safeguards in place and to US companies that are part of the EU-US Privacy Shield.
The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period.	We will keep your records for two years following after your Membership ceases. We will then shred your paper records and electronically destroy your computerized records. If, for some reason, we wish to keep your records longer we will contact you for your permission.
The existence of the right to access, rectify or erase the personal data.	<p>Your Rights under Data Protection legislation.</p> <p>As a Data Subject you have a number of rights which includes the right to:</p> <ul style="list-style-type: none"> ○ Access the personal data NSHN holds about you. ○ Have inaccurate data corrected. ○ Prevent the processing of information which may cause you harm or distress. ○ Prevent unsolicited marketing. ○ Prevent automated decision-making. <p>NSHN strives to ensure that your personal data remains accurate. To assist us with this you should notify us of any changes to information we hold about you. If you become</p>

Requirement	Privacy Statement
	<p>aware of any inaccuracies in the data we hold please inform us as soon as possible so it can be amended accordingly.</p> <p>Your Right to Access Personal Data As a Data Subject you have a right to request a copy of the information NSHN holds about you. This is known as a 'Subject Access Request' (SAR). SARs should be made in writing, if possible, to the Data Controller at the address given above.</p> <p>There is usually no charge for this information. However, NSHN reserves the right to charge in accordance with legislation a reasonable fee to cover administration costs where the request is manifestly unfounded or excessive, particularly if it is repetitive.</p> <p>For more information on your rights please visit the Information Commissioner's website: www.ico.org.uk</p>
The right to data portability	If you wish to use services provided by another charity we may be able to transfer your information to them, but not without a request from you.
The right to withdraw consent at any time	You may also ask us to stop processing or erase your information. If we do this then we will be unable to provide you with any of our services.
The right to lodge a complaint to a supervisory authority	<p>We hope you found our services satisfactory. However, if you have any concerns or complaints you should contact our Data Controller as soon as possible. The address is given above.</p> <p>If you are unhappy with our response you may be able to ask the Information Commissioner's Office to intervene. You can contact them by visiting:</p> <ul style="list-style-type: none"> • Visiting their website at www.ico.org.uk • Calling their helpline on 0303 123 1113 • or send an e-mail to casework@ico.org.uk

The finished statement is shown on the next page.

Privacy Statement for Members of the North Shields Hobnobblers

North Shields Hobnobblers (NSHN) takes your privacy very seriously. This Privacy Statement explains why and how we collect information about you, how we use it and what we do with it when we are finished. If you have any questions or concerns please contact our Data Controller:

Data Controller:	North Shields Hobnobblers
Name of Charity:	North Shields Hobnobblers
Address:	100 Any Street, North Shields NE30 0AA
Phone number:	0191 123 4567
E-mail address:	chief.officer@northshieldshobnobblers.mail.co.uk

When you approach us to become a Member we need to gather some basic information about you. This is to ensure that we provide information and services that meet your needs.

“Data Subjects” i.e. people who become Members of NSHN, will be asked to provide/confirm their personal and/or sensitive personal data as required. By providing this information the Data Subject consents to NSHN collecting, processing and storing this information.

We may also collect other personal sensitive information about you such as your gender, ethnicity, etc. We do this for monitoring purposes to prove to our funders that we are reaching a broad cross-section of the local community. When we collect this type of sensitive information we anonymize it. We keep your name and address separate from the sensitive data so no one can link the data to you.

Appropriate security measures are or will be in place to ensure that all personal and sensitive personal data is held and processed confidentially.

We will ask you to give us permission to collect and process your information. We do this by asking you to sign a consent form.

NSHN handles personal data in compliance with the General Data Protection Regulation and recognises the importance of correct and lawful processing. The personal data you provide will only be used for official NSHN business.

NSHN discloses information to a variety of third parties; these include but are not limited to:

- Relevant authorities dealing with emergency situations at NSHN.

- Any other authorised third party to whom NSHN has a legal/contractual obligation to share data with.

Disclosure of certain personal data may also be made to other entities not listed above. This will only ever be done in accordance with the GDPR. Your consent will be sought where necessary.

NSHN uses computerised records linked to “The Cloud”: computer servers based overseas which enables our staff to access your records, even when they are not in the office. This helps us to provide you with an efficient service. This means that we may transfer your data abroad but only to Member States of the European Union, countries recognized by the European Commission as having adequate data safeguards in place and to US companies that are part of the EU-US Privacy Shield.

We will keep your records for two years following after your Membership ceases. We will then shred your paper records and electronically destroy your computerized records. If, for some reason, we wish to keep your records longer we will contact you for your permission.

Your Rights under Data Protection legislation

As a Data Subject you have a number of rights which includes the right to:

- Access the personal data NSHN holds about you.
- Have inaccurate data corrected.
- Prevent the processing of information which may cause you harm or distress.
- Prevent unsolicited marketing.
- Prevent automated decision-making.

NSHN strives to ensure that your personal data remains accurate. To assist us with this you should notify us of any changes to information we hold about you. If you become aware of any inaccuracies in the data we hold please inform us as soon as possible so it can be amended accordingly.

Your Right to Access Personal Data

As a Data Subject you have a right to request a copy of the information NSHN holds about you. This is known as a ‘Subject Access Request’ (SAR). SARs should be made in writing, if possible, to the Data Controller at the address given above.

There is usually no charge for this information. However, NSHN reserves the right to charge in accordance with legislation a reasonable fee to cover administration costs where the request is manifestly unfounded or excessive, particularly if it is repetitive.

For more information on your rights please visit the Information Commissioner’s website: www.ico.org.uk

If you wish to use services provided by another charity we may be able to transfer your information to them, but not without a request from you.

You may also ask us to stop processing or erase your information. If we do this then we will be unable to provide you with any of our services.

We hope you found our services satisfactory. However, if you have any concerns or complaints you should contact our Data Controller as soon as possible. The address is given above.

If you are unhappy with our response you may be able to ask the Information Commissioner's Office to intervene. You can contact them by:

- Visiting their website at www.ico.org.uk
- Calling their helpline on 0303 123 1113
- or send an e-mail to casework@ico.org.uk

Annex H: Procedure for dealing with a Subject Access Request (SAR)

Key Points

- A Data Subject can request confirmation that you are processing their information.
- A Data Subject may also request copies of their personal information including supplementary information (usually specified in your Data Privacy statement).
- You must make reasonable efforts to ensure that the person who is requesting the information is entitled to it. This often requires the Data Subject to prove their identity but, in cases which the Data Subject does not have the physical or mental capacity to make the request themselves, an appropriate person may represent them.
- Proof of identity may include, for example, government issued photo ID, such as a passport or driver's license, personal knowledge of the Data Subject as a long-term beneficiary, a utility or Council Tax bill, etc.
- The information which the Data Subject requests should be supplied within 1 month, or within 2 months in cases where the requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the request will take longer to process.
- Organisations may choose to refuse to hand over data relating to current management issues such as restructuring or redundancies, confidential health records, communications with lawyers or personal data that is processed for purposes relating to criminal justice and taxation.

Proof of Identity

- All reasonable care should be taken to verify the identity of the person making the Subject Access Request (SAR).
- Only the Data Subject, or a person appointed by them in the cases of limited physical or mental capacity, may request a copy of the information held on them.
- If the Data Subject is under 13 years of age then the request must be made by an appropriate adult such as a parent or guardian. This should preferably be the person who gave the original permission on behalf of the Data Subject.

- If the request is by e-mail, try to verify the e-mail address by comparing it to the e-mail address which is already on record (if any). People often change their e-mail address so a mismatch is not necessarily indicative that the person requesting the information is not the Data Subject.
- If necessary, request further proof such as photo ID in the form of a passport or driving license, a utility bill or Council Tax bill that shows residency.

Request Procedure

1. The request should be sent to the Data Controller.
2. The Data Controller will verify the identity of the Data Subject as above.
3. Once the identity check has been completed the Data Controller will assemble, or will appoint someone to assemble the data.
4. The Data Controller or appointed person will send an e-mail to all staff, including Management Committee or Trustee Board Members, requesting copies of any information they hold on the Data Subject and any relevant correspondence. This should include:
 - E-mails and correspondence exchanged with the Data Subject.
 - E-mails and correspondence that identify the Data Subject either by name, position or by an identification code.
 - Any document completed by or on behalf of the Data Subject such as job application forms, volunteer registration forms, contact database forms, attendance sheets, monitoring, assessment and evaluation forms, etc.
 - Any electronic record that identifies the Data Subject such as a contact database entry, monitoring records of service provided to the Data Subject, reports, memoranda, diary entries, mailing lists and personal notes.
 - Any financial records that identify the Data Subject such as payroll information, expenses claims, payment and invoicing records, etc
5. The information should be provided to the Data Controller, or appointed person, within 7 days of the Data Controller's request.

6. Where other individuals are identified in the records it may be necessary to redact the information relating to the other individuals. The Data Controller will consult with staff and, if required, those also mentioned in the records.
7. The assembled information will be sent to the Data Subject by e-mail or, in the case of files that are too large for the mailing system, will be sent via a third party mailer.

Annex I: Procedure for dealing with a Data Breach

Definition of a Data Breach

A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (ICO definition). This means that a breach is more than just losing personal data.

Notifying the supervisory authority

If the breach is *unlikely* to result in a risk to the rights and freedoms of individuals, no notification is required. Otherwise...

- Notify the Information Commissioner's Office (ICO) within 72 hours.
 - Phone the ICO Security Breach Helpline on 0303 123 1113 (Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give you advice about what to do next *or* e-mail casework@ico.org.uk
- The notification should be accompanied by the following information:
 - Nature of the data breach, categories of personal data affected and number of Data Subjects and personal records concerned;
 - Name and contact details of the Data Controller or Data Protection Officer;
 - The likely consequences and measures taken or proposed to be taken.

If it is not possible to provide the above information at the same time as the notification, the information may be provided in phases without unduly delaying the notification to the ICO.

The Data Controller should document any breaches and related issues. These documents can be used to demonstrate legal compliance to the ICO.

Notifying the Data Subject

The Data Controller has an obligation to let the Data Subject know, without undue delay, about the personal data breach if the breach *is likely to result in a high risk to the rights and freedoms of the individual*

The communication to the Data Subject needs to be clear, plain and understandable and should include the same information given to the ICO as listed above. The Data Controller is not obliged to notify the Data Subject if:

- Appropriate measures have been implemented and applied to protect the personal data (for example encryption); or
- Subsequent measures have been taken to prevent a high risk to the rights and freedoms of the Data Subject; or
- The effort is disproportionate. If this is the case, a public communication or similar measure to inform Data Subjects is likely to be sufficient

Notifying the Charity Commission

If the data breach is sufficiently serious you must also inform the Charity Commission. Serious breaches include:

- Personal data has been accessed by an unknown and/or unauthorised person.
- A laptop, computer, tablet, memory stick or mobile phone containing personal data has been stolen or lost.
- The charity's funds have been stolen perhaps due to a 'phishing' scam.

For further guidance go to:

www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity