

Guide to GDPR for charity shops

A practical guide on how to comply with GDPR within charity shops



May 2018

About this guide

This guide has been written to assist charities with GDPR compliance specifically in the context of operating charity shops, in particular in relation to the operation of the Retail Gift Aid Scheme. The guide is intended to provide an overview of the law, and to identify specific actions that charities should take to ensure compliance with legal requirements in that context. For a more general guide to GDPR, please contact us to request our *Guide to GDPR*.

This guide is accurate as at the date of printing, but is not a substitute for legal advice and does not cover all areas of GDPR, data protection and privacy law and regulation, so should not be considered to be a general guide on the law and regulation applying to data protection. Similarly, it does not cover any other areas of law that are applicable to charity shops. However, it is hoped that charities will find the guide a useful resource and we invite any charity that feels it requires more tailored advice to contact us directly.

Contacts

Liz Brownsell

Senior Associate

Co-Head of Charities and Social Enterprise

+44(0)1473 406383

liz-brownsell@birketts.co.uk

Kitty Rosser

Senior Associate

Corporate and Commercial

+44(0)1603 756559

kitty-rosser@birketts.co.uk

Contents

1.	Introduction to the Retail Gift Aid scheme and data collection	4
2.	Retail Gift Aid: data processing and Information Notices	9
3.	Retail Gift Aid: record retention requirements and GDPR	16
4.	Retail Gift Aid: options for documentation	22
5.	Direct marketing: charity fundraising	29
6.	Sharing data: trading subsidiaries	35
7.	The right to be forgotten	38
8.	Using EPoS systems	42
9.	Staff and volunteers	45
10.	Promoting other fundraising events and social media issues	47
11.	Answering your questions	49
12.	Further guidance	52
13.	Birketts' Charities and Social Enterprise Team	54
14.	Birketts' data protection training	55
15.	Contacts	56

1. Introduction to the Retail Gift Aid scheme and data collection

When a person agrees to Gift Aid a donation to a charity, they provide the charity with personal data to enable the charity to process the Gift Aid claim with HMRC. This applies in respect of the Retail Gift Aid scheme, but due to its complexity, personal data is also collected for other purposes at the same time that the Gift Aid form is completed. For example, personal data must also be used to satisfy the HMRC requirement to notify donors as to the net proceeds of sale of their goods (this is explained in more detail below).

Many charities operate the Retail Gift Aid scheme via a trading subsidiary. For ease of reference throughout this guide, where a requirement applies to either the charity or the trading subsidiary (or both), depending upon which entity is being used for that particular purpose or which entity is collecting and processing personal data, we use the term 'charity shop'. For more information on the sharing of personal data between charities and their trading subsidiaries, and how to address this within Information Notices, please see chapter 6 of this guide.

In this chapter, we will provide a brief overview of the **Retail Gift Aid scheme** and the data that must be collected in order to comply with HMRC requirements for the scheme.

Overview of the Retail Gift Aid scheme

It is only legally possible for a charity to claim Gift Aid on donations of money. However, HMRC has approved a scheme to enable charities to claim Gift Aid in respect of donations of goods in charity shops. This is achieved by the charity shop acting as agent for the donor when selling the goods, so that the proceeds of sale belong to the donor at the point of sale. The donation to the charity is only made after completion of the sale of the goods, once the donor has a sum of money to donate (i.e. the net proceeds of sale: the amount for which the goods were sold less commission and VAT).

Key HMRC requirements

Personal data is collected for compliance with key HMRC requirements:

- Gift Aid Declaration
- written Agency Agreement
- letters to donors containing compulsory text.

In order for a donation to qualify for Gift Aid under this scheme, the donor must understand that the charity shop is selling the goods on their behalf as their agent. To ensure that this requirement is met, **HMRC requires as a condition of the scheme that a written agreement is entered into with the donor** when they sign up to the Retail Gift Aid scheme.

Another key requirement in order for a donation to qualify for Gift Aid under the scheme is that the donor has the right to keep all net proceeds of sale and has a choice as to whether or not to donate all or part of that money to the charity. To ensure that this requirement is met, **HMRC requires the charity shop to send letters to the donor containing certain compulsory text**. The timing and content of the letters to be sent to donors depends upon which of the three available methods is being operated: the Standard Method, Method A or Method B.

Standard Method

Under the Standard Method, after any goods are sold but before the charity makes the Gift Aid claim in respect of the net proceeds of sale, the charity shop must write (either by letter or by email) to the donor to notify them of the amount of the net proceeds of sale and explain that the charity will treat the amount as a donation unless within 21 days of the date of the letter or email the donor contacts the charity shop to say that they want to keep the proceeds.

Methods A and B

Under both Method A and Method B the donor is able to agree in advance (i.e. when signing up to the Retail Gift Aid scheme) that the net proceeds of sale of their goods **up to a specified amount** within a tax year may be automatically treated as a donation to the charity without the charity shop needing to first write to the donor to provide an opportunity for them to ask for the money back before it is treated as a donation to the charity and Gift Aid is claimed by the charity on that amount.

Therefore, under both Method A and Method B, the charity shop need not write to a donor during the tax year unless and until the net proceeds of sale of their goods exceeds the specified amount. Under Method A the maximum specified amount is currently £100 and under Method B the maximum specified amount is currently £1,000.

Once the specified amount is exceeded within a tax year, the charity shop has a choice of either writing to the donor (by letter or email) at that point and then writing again every time further goods are sold (i.e. in order that the net proceeds of sale in excess of the specified amount may, after the 21 day period has expired, be processed as a donation to the charity on which Gift Aid may be claimed); **or** waiting until the end of the tax year and sending a single letter detailing the total amount raised within that tax year before treating any of the net proceeds of sale above the specified amount as a donation to the charity on which the charity may then process a Gift Aid claim.

Regardless of which approach is chosen, all letters must explain that the charity will treat the amount over and above the pre-agreed specified amount as a donation unless within 21 days of the date of the letter or email the donor contacts the charity shop to say that they want to keep that amount (N.B. the donor may only claim the amount of the net proceeds of sale that is in excess of the pre-agreed specified amount).

In addition, all donors on either Method A or Method B must be sent an end of tax year letter in any event, informing them of the total amount raised from the sales of their goods in that tax year and the amount of Gift Aid that the charity was, therefore, able to claim.

NOTE: The Retail Gift Aid scheme is complex and it is outside the remit of this guide to provide detailed guidance on the scheme itself. However, the Charity Retail Association provides guidance on the scheme on its website and you can also find out more about the scheme by reading the detailed guidance produced by HMRC. See chapter 12 of this guide for links to useful HMRC guidance.

Personal data collected

Charities cannot claim Gift Aid without collecting personal data. In order for the charity to claim Gift Aid on the donation (i.e. the net proceeds of sale), it is necessary for the individual who owned the goods to make a **valid Gift Aid declaration**, and importantly HMRC states that this **must** be made “before the net proceeds of sale are donated to the charity”. It is, therefore, common for charity shops to obtain the necessary Gift Aid declaration when the donor brings the goods into the shop and agrees to sign up to the Retail Gift Aid scheme.

The personal data that is required to be collected in order for the charity to submit a Gift Aid claim to HMRC is as follows:

- title, first name and surname (as a minimum HMRC will accept the donor’s initial and surname)
- full home postal address (as a minimum HMRC will accept the house name or number and the full postcode, but it will be necessary to have the full postal address for notification letters).

In addition, charity shops commonly collect other personal data on a Gift Aid form, and even the model HMRC Gift Aid declaration form contains the option for donors to provide their home phone number, mobile phone number and email address (which can be used for the purpose of sending notification letters to donors, but is not required to be collected for this purpose). However, the only personal data that is mandatory for a Gift Aid claim is the data listed in bullet points above.

Depending on whether or not you have opted to deal with both the Agency Agreement and the Gift Aid declaration in the same document (see chapter 4 of this guide), there might be one or two documents containing the name, address and possibly also the phone number(s) and email address of the donor.

The documents that a charity shop must use and the records that a charity must keep to satisfy HMRC requirements will contain some information that most people would readily identify as personal data: names and home addresses. However, it is likely that the personal data held will actually be a little more extensive than this.

- Gift Aid declaration forms will indicate an individual's tax status.
- The identity of the charity to which a donation is made might give an indication of a person's interests, political affiliations or religious affiliations.
- Records held by a charity shop regarding particular items donated by an individual might give an insight into their tastes, preferences and wealth.
- A change of address might indicate changes in economic or family circumstances.

Whilst there is absolutely nothing wrong with collecting this information, it is important to only collect and use the information in a way which complies with the requirements of data protection laws. From a legal perspective, this will ensure that the charity shop does not face harmful penalties or enforcement actions. Taking a more practical view, complying with these rules will help the charity to develop lasting and rewarding relationships with its supporters based on principles of mutual respect and transparency.

2. Retail Gift Aid: data processing and Information Notices

As explained in chapter 1, it is necessary for charity shops to collect personal data in order to operate the Retail Gift Aid scheme. Although this data collection takes place because of legal requirements set out by HMRC, it is nevertheless necessary to comply with GDPR in respect of the collection and use of that data.

In this chapter, we will look specifically at the legal requirements that apply under GDPR in relation to the **collection and use of personal data** when a person signs up to the Retail Gift Aid scheme, including practical tips regarding **Information Notices** that should be provided.

GDPR requirements: processing personal data

The General Data Protection Regulation (GDPR) sets out the rules that a charity shop must follow whenever processing personal data. **'Personal data'** means any information at all that can be related to an identifiable individual. **'Processing'** covers everything that you might do with that personal data, from initial collection right up to when and how it is deleted once it is no longer needed.

The GDPR is based on **six fundamental principles or standards** that must always be adhered to when processing personal data:

- Only process personal data in a way that is fair, lawful and transparent.

As a general rule of thumb, charity shops should only use an individual's personal data in ways which that individual would reasonably expect. In particular, charity shops must ensure that the processing is lawful by identifying an applicable lawful basis of processing and must be transparent about how personal data is used by providing an Information Notice. Further detail on these particular obligations is given below.

- Only collect and use personal data for specified, explicit and legitimate purposes.

Collecting and using personal data to claim Gift Aid on donations to the charity is clearly a legitimate purpose for charity shops. Provided that your documents and processes follow HMRC guidance, the fact that you intend to use personal data for the purpose of claiming Gift Aid on donations to the charity will be abundantly clear to the donor. However, in practice charity shops might wish to use the personal data for purposes other than simply processing Gift Aid claims and these other purposes might not be so obvious to donors.

Charity shops routinely add names and addresses captured via Gift Aid declarations to the charity's marketing databases, and many Gift Aid declarations capture supplemental information, such as telephone numbers and email addresses, which charities wish to use specifically for fundraising purposes.

In itself, there is nothing wrong with adopting a 'multi-purpose' approach – it might actually offer a more streamlined experience for the donor – however, charity shops must be absolutely transparent with donors if they wish to use personal data for purposes in addition to compliance with the HMRC requirements for the Retail Gift Aid scheme and processing Gift Aid claims on donations to charities. Clear, carefully designed forms and scripts incorporating appropriate Information Notices can be used to achieve this (see below for further guidance on Information Notices).

- Ensure that the personal data collected is adequate, relevant and limited to what is necessary for those purposes.

When it comes to the Retail Gift Aid scheme, charity shops can most effectively meet this obligation by limiting the personal data that is collected to that specifically required by HMRC (which might include an email address for the purpose of sending the required letters under the Retail Gift Aid scheme). However, if a charity shop wishes to capture supplemental personal data to use for purposes other than the Retail Gift Aid scheme during the donation process, you should consider what those other purposes are and ensure that you only request the personal data that is actually needed for them. (Remember also that express consent is required if email addresses and/or mobile phone numbers will be used for any direct marketing

by email or SMS – please see chapter 5 of this guide for more detail about using personal data for direct marketing purposes).

Designing data collection forms and scripts to offer clarity and flexibility will assist in ensuring that only the relevant information is collected. For example, clearly distinguishing those fields that are being collected for the purpose of complying with HMRC requirements under the Retail Gift Aid scheme will limit the risk of an individual who does not wish to receive fundraising communications providing additional contact details that would only be used for that purpose.

- Ensure that the personal data is accurate and, where necessary, kept up to date.

Having a clear process in place to record updated name and contact information provided by donors across all relevant records and databases will meet both the HMRC and GDPR requirements. Consider how and when an individual may provide updated information and what steps you can take to ensure that all relevant records and databases are updated with the new details.

- Only keep personal data for as long as necessary for the purposes for which it is collected and used.

See below for guidance on the retention of personal data.

- Have appropriate security measures in place to keep personal data safe .

Security arrangements should be proportionate to the potential risks to individuals, taking into account the amount and type of personal data processed, as well as to the means and resources you have available.

When considering security you should think about technical measures (e.g. password, firewall and antivirus protection on computers), physical measures (e.g. records kept in a locked cabinet in a staff-only area of the shop) and organisational measures (e.g. limiting access to information on a need to know basis).

NOTE: Information on specific security measures is outside the remit of this guide, but more detailed guidance on security measures can be found on the Information Commissioner's Office website (www.ico.org.uk).

GDPR requirements: identifying a lawful basis of processing

In order to meet the requirement that processing of personal data is lawful, a charity shop needs to identify which of the six lawful bases of processing set out in the GDPR apply to its processing activities. The six lawful bases are:

1. **Consent:** the individual has given clear consent for the charity shop to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract the charity shop has in place with the individual, or because the individual has asked the charity shop to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for the charity shop to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task:** the processing is necessary for the charity shop to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for the charity shop's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The processing of personal data by a charity for the purpose of making a Gift Aid claim falls under the **legal obligation** ground.

The processing of personal data for compliance with HMRC requirements under the Retail Gift Aid scheme for an Agency Agreement to be entered into between the charity

shop and the donor and for letters containing compulsory text to be sent by the charity shop to the donor falls under the **contract** ground and the **legal obligation** ground. (N.B. this processing might be carried out by the charity or by its trading subsidiary, depending on whether or not you operate the Retail Gift Aid scheme via your charity's trading subsidiary).

In order for a charity shop to fulfil its obligations under the Agency Agreement (which is a legally binding contract) and satisfy HMRC's requirements under the Retail Gift Aid scheme, it is necessary for the charity shop to identify the goods donated as belonging to the donor who donated them (achieved by tagging the goods with an ID number specific to that donor), record the sales of those goods against that ID number, and write letters to the donor containing HMRC compulsory text (by post or email, depending on whether or not the donor has provided an email address for that purpose).

If, in addition to the processing of personal data for Gift Aid claims and compliance with HMRC requirements under the Retail Gift Aid scheme, you also intend to use the personal data collected for other purposes, you will need to consider and identify an applicable lawful basis for each additional purpose. Where personal data is also used for fundraising (e.g. by adding non-compulsory text to the letters that are sent to donors in order to inform donors about other opportunities to support the charity), the applicable lawful basis would be either **consent or legitimate interest**, depending upon the circumstances (see chapter 5 of this guide for further detail). You **must** consider and document which lawful basis can be relied upon **before** beginning processing.

GDPR requirements: providing compliant Information Notices

Individuals have a specific right to be informed about the collection and use of their personal data. In order to respect this right and to fulfil the requirement for transparency under the first data protection principal, charity shops must provide individuals with certain information when collecting their data under the Retail Gift Aid scheme.

The rules vary slightly depending upon whether personal data is collected from the individual directly or received from a third party. For the purpose of this guide, it is assumed that the charity shop will be collecting information from the individual directly. Further guidance about the rules that apply when personal data is received

from a third party can be found on the Information Commissioner's Office website (www.ico.org.uk).

The information that the GDPR requires charity shops to include within the Information Notices provided to donors includes:

- the name and contact details of the data controller (this might be the charity, or the trading subsidiary, or both (as joint data controllers))
- the contact details of the data controller's data protection officer (if applicable)
- the contact details of the data controller's representative (if applicable)
- the purposes of the processing
- the lawful basis for the processing
- the legitimate interests for the processing (if this is relied upon as a ground of processing)
- the recipients or categories of recipients of the personal data
- the details of transfers of the personal data to any third countries or international organisations (if applicable)
- the retention periods for the personal data
- the rights available to individuals in respect of the processing
- the right to withdraw consent (if consent is relied upon as a ground of processing)
- the right to lodge a complaint with a supervisory authority
- the details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable)
- the details of the existence of automated decision-making, including profiling (if applicable).

This information must be provided at the time that the personal data is collected. It must be presented in a way which is concise, transparent, intelligible, easily accessible and using clear, plain language. The Information Commissioner's Office guidance recommends using a **layered approach** to provide the relevant details at the most appropriate stage during the data collection process.

Information Notices: practical tips

When preparing and using Information Notices in a Retail Gift Aid context, particular consideration should be given to the following points.

- Using a layered approach to ensure the charity shop is providing appropriate amounts of information and relevant detail at the right time and in a way that will reassure the donor, rather than disrupting the donation experience.
- Aiming to embed key processing information, such as why you need different details and who personal data will be shared with, into the data collection forms themselves (or incorporate this information as part of the data collection script). Make sure all forms and scripts include a statement telling donors where they can find the charity shop's full Information Notice.
- Making it as easy as possible for people to get a copy of the full Information Notice. Have hard copies available in shops and include a soft copy (or a direct link to the relevant page on the website) when emails are sent confirming Retail Gift Aid arrangements.
- Keeping Information Notices as concise as possible and ensuring that they are easy to understand. Adopt the charity shop's usual tone and style rather than being tempted to use 'legalese'.
- Checking information notices are clear about the different legal entities that might be involved and how personal data will be shared between them, e.g. the charity, its trading subsidiary and HMRC.
- Ensuring that the charity shop is absolutely open about any other purposes for which personal data might be used in addition to the Retail Gift Aid scheme, including whether the individual can elect not to have their personal data used for those additional purposes.

3. Retail Gift Aid: record retention requirements and GDPR

Personal data collected by charity shops for the purposes of the Retail Gift Aid scheme must be retained by the charity in order to comply with HMRC record retention requirements. However, it is also necessary to comply with the data protection principle to “only keep personal data for as long as necessary for the purposes for which it is collected and used”.

In this chapter, we set out the **HMRC requirements** for record retention in relation to the Retail Gift Aid scheme and **how GDPR relates** to these requirements. We also include some practical tips on how to manage compliance with record retention requirements.

HMRC record retention requirements

It is a requirement of the Retail Gift Aid scheme that charities keep a record of each donor’s agreement to enter into a legally binding **Agency Agreement**. HMRC guidance states:

“There needs to be a written agreement between the individual and the charity, and the charity needs to keep a record of each individual’s agreement. The agreement can be a document signed by the donor, or a leaflet or information sheet given to the donor”.

In addition, in order for the charity to claim Gift Aid on the net proceeds of sale, it is essential that the charity is able to identify to which donor those funds relate. This can only be achieved by the charity shop **carefully labelling the goods** and keeping records to show the total amounts raised from the sale of goods on each donor’s behalf in each tax year. HMRC guidance therefore states:

“Charity shops must allocate a unique identity code or number to each donor and use this on the price labels attached to their goods so that the proceeds from the sale of each item can be linked to the correct donor. Goods sold on behalf of individuals must be identifiable from other goods or stock that has been bought in by the shop. This is usually done using different price labels on the goods.”

HMRC also requires charities to **retain all documentation associated with claims for Gift Aid** for audit purposes. HMRC guidance states that this includes:

- the donor's dated Gift Aid declaration
- a copy of any written agreement with the individual under which the charity shop is appointed as an agent to sell goods on the person's behalf
- records of any changes in process between the Standard Method, Method A or Method B and the movement of donors from one process to another
- records to show that the donor has been notified of the net sale proceeds where required
- records to show that end of tax year letters have been sent to all donors by charity shops operating either Method A or B
- records tracing Gift Aid claims back to the sales of donated goods by individual donors
- if goods are sold by a trading subsidiary of a charity, records to show how the net sales proceeds are transferred to the charity
- records of checks the charity has carried out on each of its shops to ensure that the Retail Gift Aid process is operated correctly.

There is a legal requirement for charities to “keep sufficient records to show that their tax reclaims are accurate”. In practical terms, **it is necessary to retain Gift Aid declarations and all associated documentation to enable you to show an audit trail** linking each donation to an identifiable donor who has given a valid Gift Aid declaration, and that all the other conditions for the tax relief are satisfied.

All records relating to a particular individual under the Retail Gift Aid scheme must be retained by the charity for the period of time required by HMRC. The guidance on retention of Gift Aid declarations is set out in chapter 3 of the HMRC guidance on Gift Aid, and is summarised below.

- If Gift Aid declarations are made without a specified end-date so that they will cover ongoing donations, then HMRC guidance says that they should be retained permanently. However, if and when donations cease, then time limits apply from the date of the last donation. (N.B. if the Gift Aid declaration that is made in respect of the Retail Gift Aid scheme is also used in respect of other donations made by a particular donor, it will therefore be important to check whether other donations are still being received even if donations under the Retail Gift Aid scheme have ceased).

- For all charities other than charitable trusts, the general rule is that tax records must be retained until six years after the end of the accounting period to which they relate. HMRC provides the following example:

“For example if a charitable company prepares its accounts to 31 December 2007 and makes a Gift Aid repayment claim for that period during 2008, it must keep the records until at least 31 December 2013.”

Additionally, if HMRC asks questions about a tax return or repayment claim, the charity will need to keep the records until the enquiries are finished.

- In respect of charitable trusts, the general rule is that tax records should be retained until the later of six years after the end of the tax year to which they relate or 12 months after the charity makes a Gift Aid repayment claim for that tax year. If the charity is asked to make a tax return there are different rules about how long records must be kept for.

If a charity fails to keep adequate records it might be required to pay back to HMRC the tax reclaimed, with interest. It might also be liable to a penalty under the Self-Assessment rules.

There are no particular requirements about whether records need to be kept in paper format or electronically. In practice, the format of your records will depend on the size of your charity, the number of donors and the kind of systems that you use.

GDPR requirements: retention of personal data

The HMRC retention requirements outlined above should be followed for all Retail Gift Aid records unless the charity can identify a clear business need to retain the records beyond the mandated period.

Where personal data is used for purposes other than just claiming Gift Aid, you will need to determine the retention periods applicable to any records created for these other purposes. Where personal data is used for multiple purposes, the charity shop should take particular care to ensure that the retention information provided within Information Notices identifies and lists the retention periods for all relevant records that might be created.

In practice, where personal data is used for additional purposes (the most common being fundraising), the relevant personal data tends to be duplicated to create a new record on the relevant database, making it relatively straightforward to operate different retention terms when the same personal data is used for multiple purposes. Other systems might involve using separate fields within one centralised database system for different purposes. Again, differing retention terms can be effectively implemented through deleting relevant fields as different retention periods expire.

In considering how to set retention periods, regard should be had to any mandated minimum period for retaining records, the duration of any potential legal liability arising from the processing activity and to the charity's general business requirements. Note that the GDPR requirement relates only to retaining personal data "in a form that permits identification" of the individuals to which it relates. Where personal data is required solely for business purposes, such as statistical analysis to identify changes and trends over time, anonymisation can be used to ensure that the retention requirements are met without the underlying value of the data set being lost.

Charities must have **effective and documented procedures** in place to ensure that all relevant paper and electronic records are actually identified and deleted (or anonymised) once the specified retention period has expired. Streamlining processing systems and avoiding fragmented, decentralised storage systems will assist in the practical implementation of retention procedures.

Record retention: practical tips

- As explained above under the heading 'HMRC record retention requirements' all records necessary to provide an audit trail for the purposes of the Retail Gift Aid scheme must be retained for six years after the end of the accounting period in respect of which a Gift Aid claim was last made relating to that individual (for charitable companies and unincorporated associations) or for six years after the last date on which an individual appeared on a Gift Aid claim (for charitable trusts). These requirements are not overridden by GDPR and you do not need consent in order to retain these records.
- Many charities comment that it is difficult to know when to delete records relating to a donor on the Retail Gift Aid scheme, because many donors go for long periods between donations and it is not easy to identify whether or not a donor has recently made a donation. However, it might be possible to achieve this by adjusting processes and procedures to assist you with compliance, for example:
 - Draft your Gift Aid declaration so that it only applies to the Retail Gift Aid scheme, and include a statement on the declaration that it will endure for so long as the individual continues to bring goods to the shop for sale under the scheme, and that it will expire if an individual does not bring goods into the shop for sale under the scheme for a specific period of time (e.g. three years). This will provide some certainty that a Gift Aid declaration has expired, and that a fresh one will be required if that donor wishes to donate goods under the scheme after a long period without making any donations.
 - Add to your Agency Agreement the right to dispose of goods donated under the Retail Gift Aid scheme (whether by ragging, scrapping or otherwise) if those goods have not sold within a specified period of time, and then implement processes to ensure that goods are regularly reviewed and removed from the shop floor if they have not sold.
 - Adjust your processes so that you know whether there are any goods currently on the shop floor under an individual donor's ID number (e.g. by tracking them when they are added to the shop floor and when they are removed, either as a result of a sale or because they have been disposed of). It is necessary to be able to trace back to the individual donor all of their goods sold in order to make a Gift Aid claim in respect of their donation, so it should be possible to ascertain whether or not there are any goods tagged with a donor's ID number on the shop floor.

- Implement a system so that you maintain a record of the last date on which a particular donor appeared on a Gift Aid claim under the Retail Gift Aid scheme (or the end of the accounting period to which that claim related), with an alert being issued if six years elapse since the last time a claim was made in respect of that donor.
- For any data held about a donor that is not required to be retained for the purposes of providing an audit trail for HMRC in relation to the Retail Gift Aid scheme, decide whether to keep that data on a separate database or whether to use separate fields within your Retail Gift Aid database. Ensure that the period of time for which records are actually retained reflects the retention period stated on your Information Notice, and put appropriate systems in place to assist with this.

4. Retail Gift Aid: options for documentation

As explained in chapter 1 of this guide, it is a requirement of the Retail Gift Aid scheme that the donor makes a valid Gift Aid declaration to the charity and also enters into a written agreement to appoint the charity shop as its agent for the sale of the goods.

Many charities opt to use a single hard copy document for both purposes, and this is acceptable to HMRC. Others prefer to keep the two documents separate. Additionally, many charities choose to operate the scheme using electronic devices (such as tablets or EPOS systems) to record data, and do not use any hard copy documents at all.

In this chapter, we will look at the relevant legal issues and **HMRC requirements** relating to documentation.

Gift Aid declaration

The requirements for the Gift Aid declaration for the purposes of the Retail Gift Aid scheme are broadly the same as for any other type of donation made to a charity by a donor who wishes to Gift Aid their donation.

HMRC guidance states that *“before a charity can reclaim tax on a donation received from an individual, it must have received a Gift Aid declaration from the donor. Without this declaration, a donation from an individual won’t qualify as a Gift Aid donation.”*

A Gift Aid declaration must state the donor’s name and home address, name the charity, identify the gift or gifts to which the declaration relates (either a specific gift or all donations) and confirm that the identified gift or gifts are to be treated as Gift Aid donations. In addition, the charity must be able to demonstrate that the donor has been given an adequate explanation of the personal tax implications associated with making a Gift Aid declaration. This explanation may be included on the form or it may be provided separately.

Gift Aid declarations can be given in writing (including by email, fax or text message), and there is **no requirement for a Gift Aid declaration to be signed by the donor**.

There is also no required format for Gift Aid declarations and charities may design their own (provided that the required information is obtained). There is no need to seek HMRC's approval for own-design forms, but HMRC Guidance states that HMRC will review proposed designs on request.

Gift Aid declarations may also be given orally (in person or over the phone). However, unless an oral declaration is audio recorded (with the recording kept by the charity) it will not be valid unless and until the charity sends the donor a written record of the declaration. HMRC guidance states that *“the written record of the declaration doesn't have to be recorded on paper. For example, the charity's representative might record the details on a computer, with an electronic copy being emailed to the donor, or a paper copy sent by post. If the charity uses an electronic means of recording the donor's information, it will need to be able to demonstrate at an audit that the electronic recording of the information generates a written record sent to the donor.”*

All charities must **keep a record of all Gift Aid declarations made**. Examples of what HMRC is likely to accept as evidence of declarations include:

- written declaration made by the donor or a ticked box confirmation by the donor that they wish Gift Aid to apply to the donation
- an audio recording of the making of a declaration by the donor or an audio recording of the donor confirming a declaration where the declaration is pre-recorded by the charity
- an emailed copy of a declaration
- a scanned image that's an exact replica of a declaration
- confirmation that a donor has been sent a written record confirming their oral declaration.

Important!

HMRC guidance warns that *“the transcribing of declarations given by donors into a database won’t satisfy the requirements to have an auditable record as such a record doesn’t demonstrate that the donor made the declaration”*.

HMRC requires charities to *“keep adequate records to be able to show a clear link between an individual’s donation and the Gift Aid declaration made by the individual”*. To assist with this, charities may add further information and notes on a Gift Aid declaration form.

HMRC also has no objection to a Gift Aid declaration being included in another document, provided that the statutory requirements for a Gift Aid declaration are met.

GDPR compliance: top tips

When considering your approach and documentation, you must be mindful to ensure that you are both meeting the HMRC requirements and complying with the data protection fundamental principles (outlined in chapter 2 of this guide). When reviewing documentation and scripts, you should ask yourself the following questions.

- Is the personal data collected to be used just for Retail Gift Aid purposes or will it also be used for additional purposes, such as fundraising?
- Are all of the different purposes for which personal data will be used made obvious to the donor?
- Is the donor given the opportunity to control whether or not personal data will be used for purposes other than Retail Gift Aid, e.g. through the use of tick boxes (note that if consent is required in order to use the personal data for a particular purpose, for example, using email addresses for direct marketing, then that consent must be freely given, so pre-ticked consent boxes on a form are not acceptable)?

- Are asterisks used to clearly distinguish between personal data that is required for Retail Gift Aid purposes and personal data that the donor may choose to give for other purposes?
- Is the personal data requested limited to what is actually needed for each purpose?
- Have you considered the legal bases that will apply to each different purpose (e.g. processing for Retail Gift Aid on the basis of legal obligation, processing under the Agency Agreement on the basis of contract, processing for fundraising on the basis of legitimate interest or consent, etc.) and outlined this in your Information Notice?
- Do all documents and scripts contain a statement advising the donor where and how they may access a copy of the charity's full Information Notice?

Updating donor details

If a donor has made a Gift Aid declaration generally in respect of all donations to the charity, then it will remain valid (unless it is invalidated, e.g. because the charity does not maintain an auditable record of the declaration or its records are insufficient to show that the donor made the declaration) until the date specified in the declaration or otherwise until donor notifies the charity that they wish to cancel their declaration.

Gift Aid declarations may be made very generally and indefinitely, e.g. "all donations I make from this date until further notice". This is commonly the approach used by charities in respect of the Retail Gift Aid scheme, which means that the Gift Aid declaration will remain valid until it is cancelled (but, see also the record retention practical tips in chapter 3 of this guide).

If a donor changes their name or address, this does not invalidate a Gift Aid declaration. If the donor notifies you of the change, then you should keep a record of the updated information. This may be kept electronically or as a scanned document. It is not necessary to amend the original Gift Aid declaration, but a record of the change does need to be kept on the relevant database.

The GDPR also requires that personal data is accurate and kept up to date, so ensuring that a tried and tested process is implemented to capture and record any changes will

tick two compliance boxes. To ensure full compliance with the GDPR requirements, **you should consider all records and databases on which an individual's personal data may have been recorded** and how you can ensure that each of them is updated. This can pose particular challenges where older or less sophisticated systems are used or different teams operate independently of each other with no effective channels of communication in place.

Donors are entitled to cancel their declarations at any time. Where a donor cancels their Gift Aid declaration (e.g. by notifying you that they no longer want to participate in Retail Gift Aid scheme), **HMRC guidance states that the charity should keep a record of the cancellation**, including the date on which that donor's Gift Aid declaration was cancelled.

Agency Agreement

All charity shops operating the Retail Gift Aid scheme must ensure that Agency Agreements are entered into with donors who sign up to the scheme. HMRC guidance states that it must be made clear to the donor that this is a legally binding contract and the donor must understand that the charity shop will be selling the goods on their behalf.

HMRC also requires Agency Agreements to be entered into in writing. However, there is flexibility about the format for this, and HMRC guidance states that the agreement "*can be a document signed by the donor, or a leaflet or information sheet given to the donor*". HMRC is relaxed about the form of the agreement, provided that it constitutes a legally binding contract, covers the required information, and the charity keeps a record of each donor's agreement.

NOTE: Detailed guidance on the nature and format of Agency Agreements under the Retail Gift Aid scheme and how to ensure that they are legally binding is outside the remit of this guide. If you require any advice on your own arrangements and documentation, it is recommended that you seek professional advice.

Options for documents

There are a wide range of options for the format of obtaining the necessary personal data, Gift Aid declaration, Agency Agreement and for providing the required explanatory statement to the donor about the personal tax implications of making a Gift Aid declaration.

The options range from combining everything into a single hard copy document that the donor completes and signs to not having any hard copy documents at all, but dealing with everything orally and following up with an email or letter to the donor confirming the Gift Aid declaration and terms of the Agency Agreement. Online sign-ups are also used by some charities.

Letters to donors

The various methods of operating the Retail Gift Aid scheme (i.e. Standard, Method A and Method B) are summarised in chapter 1 of this guide. HMRC requires letters to be sent to donors under all three methods, and there are various template letters available online that set out the compulsory text that must be included.

HMRC guidance states that charity shops may send the letters to donors either by email or by post. However, HMRC recommends that all letters are sent by post and warns that *“if a charity is alerted to an e-mail having been rejected by receiving an ‘undeliverable’ message, they must follow up and send the donor a letter by post too.”*

If you wish to send the required Retail Gift Aid letters by email and therefore collect a donor’s email address specifically and solely for that purpose, you should make it clear on the Gift Aid declaration form and in your Information Notice that the donor’s email address will only be used for that purpose unless express consent is given by the donor for direct marketing by email. See chapter 2 of this guide for more information on Information Notices, and chapter 5 of this guide for more information on direct marketing.

Important!

You should bear in mind the comments earlier in this chapter and in chapter 2 of this guide regarding using personal data for different purposes and resist the temptation to add general fundraising content to Retail Gift Aid communications unless you are absolutely confident that you can do so in a way which complies with the direct marketing rules set out in chapter 5 of this guide.

5. Direct marketing: charity fundraising

As explained in chapter 1 of this guide, there are three methods of operating the Retail Gift Aid scheme: the Standard Method, Method A and Method B. Regardless of which method is adopted, letters have to be sent (by post or email) to donors at specific points in time.

For all three methods there are template letters available from HMRC which contain the compulsory wording that must be included. However, HMRC is happy for charities to add additional information to the letter or alter the opening and closing sections, provided that the compulsory text is included.

Many charities choose to include updates about the charity's activities, or direct requests for further donations, either contained within the text of the letters themselves or as inserts or attachments sent together with the letters. This raises specific issues in respect of data protection compliance.

This chapter provides an overview of the **GDPR requirements regarding direct marketing** by both post and email in the context of the Retail Gift Aid scheme where you wish to include marketing information when you send out the required Gift Aid letters/emails.

Direct marketing: introduction

The direct marketing rules apply to **all communications that contain any fundraising or campaigning elements**, even if this is not the main purpose of the communication.

When we talk about the direct marketing rules in this particular context we refer to the following three points.

1. The **data protection principles**, the detailed rules regarding the use of consent and legitimate interests and the specific right for individuals to stop organisations sending them direct marketing communications found in the GDPR.

2. **The additional rules** that apply to direct marketing communications sent out by email found in the Privacy and Electronic Communications Regulations (PECR).
3. **The additional measures** that charities are required to adhere to above and beyond the core legislative requirements set out in the GDPR and PECR under the Code of Fundraising Practice.

Both the GDPR and PECR are enforced by the Information Commissioner, who has a broad range of enforcement powers at her disposal designed to enable her to investigate and punish any breach of the rules.

The Code of Fundraising Practice is enforced by the Fundraising Regulator, who is able to investigate complaints and, where breaches are identified, can make referrals to both the Information Commissioner and the Charity Commission.

NOTE: The creation and sending of fundraising communications might engage a number of additional pieces of legislation and industry codes, such as those relating to intellectual property rights and malicious communications, all of which are outside the remit of this guide, as are the roles of other bodies, such as the Direct Marketing Association, which might become involved in handling certain complaints regarding marketing content.

Adding direct marketing to letters sent by post or email

As soon as a charity incorporates campaign information or fundraising requests into the body of a letter or provides a separate enclosure containing such information with a letter, that communication becomes a **direct marketing communication**. Data protection law does not prevent charities sending direct marketing communications, but it does require that they operate within the marketing rules when they do so. In practical terms, this means that advance planning is crucial.

Charity shops must ensure that, if they wish to use an individual's personal data to send direct marketing communications, this is conveyed very clearly when collecting

the personal data. Please refer to the comments regarding the content and structure of Retail Gift Aid declarations, Agency Agreements and Information Notices in chapters 2 and 4 of this guide.

The exact wording that it is incorporated into Gift Aid declarations and Agency Agreements and included within Information Notices will depend upon which legal basis the charity shop chooses to rely on to send direct marketing communications.

If communications are sent by post a charity shop is able to rely on legitimate interests, although in practice many elect to use consent, which is generally considered to be the higher standard. Where communications are sent by email, a charity shop may not use legitimate interests for direct marketing; **you must have consent to send campaign and fundraising content by email.**

Legitimate interests: post

If a charity shop wishes to rely on **legitimate interests** to send campaign and fundraising content by post it must...

- **reference the fact** that the details provided will be used to contact the individual for campaigning and fundraising purposes by post in the Retail Gift Aid declaration and Agency Agreement
- state within the **Information Notice** that campaigning and fundraising communications will be sent by post on the basis of legitimate interests and provide details of how the individual can ask to stop receiving such communications
- complete a written **Legitimate Interests Assessment (LIA)** outlining why it considers that it is appropriate for it to rely on legitimate interests for the purpose of sending campaign and fundraising communications by post (the ICO has published a template that can be downloaded from its website and used for the LIA; the Fundraising Regulator advises that charities publish their LIAs in full, although this is not a legal requirement)
- ensure that the personal data is **screened** before the campaign or fundraising communication content is sent out to ensure that it is not sent to anyone who the charity has been notified is deceased or who has previously opted out of receiving such communications by post, either by notifying the charity directly or by registering with the Fundraising Preference Service or the Mail Preference Service

- include a **one-step opt-out** method within every communication to allow the individual to easily change their mind in the future – this might include, for example, providing a phone number to use to update preferences, or a returnable preferences form.

Consent: post or email

If a charity wishes to use **consent** to send campaign and fundraising content by post or by email it must:

- include a **clear consent statement and opt-in tick box** which the individual can complete to indicate that they do wish to receive campaigning and fundraising communications by post and/or email – it must be absolutely clear to the individual that this is what they are agreeing to; **if the statement is not clear, or the individual feels they have no choice but to agree, the consent will not be valid**

Important!

Pre-ticked boxes or opt-outs should **not** be used, as these will not provide valid consent. The consent statement and tick box must be separate from the Retail Gift Aid content but equally as prominent. **Do not be tempted to use a smaller font size** for consent statements as this would be a breach of the Code of Fundraising Practice. Consent can be captured verbally if you do not use written forms, in which case a scripted consent statement should be read out at a defined point when the personal data is being collected.

- state within the **Information Notice** that campaigning and fundraising communications will be sent by post and/or email if the individual has consented, that such consent can be withdrawn at any time, and provide details of how the individual can withdraw their consent
- ensure that campaign and fundraising content is **only sent to those who have consented** – the charity must keep a record of how and when consent was obtained (particular thought is needed as to how this will be done when consent is captured)

verbally) and have a system in place to flag those who withdraw their consent to ensure that no further campaign or fundraising content is sent to them in the future

- include a **one-step opt-out method** within every communication to allow the individual to easily change their mind in the future – in the case of email communications, this should be a ‘click to unsubscribe’ link
- have a system in place to ensure that **consent is renewed periodically** – the data protection legislation states that consent will not last indefinitely but does not set out any concrete rules as to how long it can be relied upon (the Fundraising Regulator has produced more detailed guidance on the issue of consent. Again, no concrete expiry point is set but the Fundraising Regulator does suggest that larger organisations should look at refreshing consent **at least every 24 months**).

All charities are advised to consider duration of consent at the outset and make individuals aware of their practices in this regard. The best way to achieve this is to address the issue specifically in the Information Notice. The factors that the Fundraising Regulator suggests are taken into consideration when determining duration of consent include:

- the size of the organisation or campaign (it is recognised that it might be reasonable for smaller organisations or campaigns to refresh consent less frequently)
- how often the charity is sending the individual campaign and fundraising communications (the more often, the shorter the period of consent)
- how intrusive the means of communication used may be
- whether the particular campaign is time-limited by its nature e.g. emergency or seasonal appeal
- the nature of the relationship with the individual (if an individual regularly responds in a positive manner to communications it will be reasonable to allow longer periods between refreshing consent).

Direct marketing: top tips

- Remember that including **anything** about the charity and its current projects/ campaigns in letters under the Retail Gift Aid scheme, even just an update about what you have been doing, will constitute direct marketing. So, care needs to be taken to ensure that you have a valid legal basis for the inclusion of anything in Retail Gift Aid letters that goes beyond the compulsory text required by HMRC.
- Advance planning is key: if you do not provide the relevant information during the first interaction with the individual (and, if appropriate, capture the relevant consents) this cannot be rectified at a later date. Make sure you have fully thought through your strategy and put all of the necessary elements in place from the outset.
- Respect the fact that people sometimes change their minds. If an individual no longer wishes to hear from you, you must respect their decision and ensure you have proper systems in place to ensure you do not continue to send them campaign or fundraising content. Ignoring a request to cease receiving communications is a common trigger for complaints.
- It is important to note that there are requirements in the Fundraising Code of Practice that go beyond what is required under GDPR, for example the Code of Fundraising Practice requires screening against the Mail Preference Service. Guidance on the requirements under the Code is outside the remit of this guide, but extensive guidance can be found on the Fundraising Regulator's website: www.fundraisingregulator.org.uk/.
- If you have any concerns or need further advice about any aspect of your direct marketing or fundraising activities, whether in connection with the Retail Gift Aid scheme or otherwise, it is recommended that you seek professional advice.

6. Sharing data: trading subsidiaries

Many charities operate their Retail Gift Aid scheme via a trading subsidiary. This is primarily done for tax reasons, but some charities opt to set it up in this way in order to be eligible to make use of Method B, which is only available where the Retail Gift Aid scheme is operated by a trading subsidiary.

NOTE: It is outside the remit of this guide to provide any guidance on the circumstances in which charities should set up a trading subsidiary. However, if you are in any doubt, it is recommended that you seek professional advice, either from your accountants or lawyers.

In this chapter we will discuss the legal requirements that apply when data is shared within a group, in particular in the context of shops where trading subsidiaries operate the Retail Gift Aid scheme, but the charity wishes to be able to send marketing communications.

Introduction

Where the Retail Gift Aid scheme is operated by a trading subsidiary, the legal structure of the scheme means that:

- the donor enters into an Agency Agreement with the trading subsidiary
- the donor makes a Gift Aid declaration to the charity
- the trading subsidiary sells the goods as agent for the donor and then holds the net proceeds of sale as agent for the donor until the point at which those net proceeds of sale may be donated to the charity
- the trading subsidiary must write to the donor in accordance with the requirements of whichever method is being operated (i.e. Standard, Method A or Method B).

The net proceeds of sale **never** belong to the trading subsidiary, and will be gifted to the charity at the appropriate time, which will depend upon the Method being used.

Under the Standard Method, the net proceeds of sale will be gifted by the donor (acting by their agent, the trading subsidiary) to the charity once the 21 day period expires after the compulsory letter is sent to the donor. Under Methods A and B all net proceeds of sale up to the pre-agreed specified amount may be automatically donated to the charity by the trading subsidiary (as agent for the donor); after that a letter must be sent and the trading subsidiary must wait for the 21 day period to expire before making the donation to the charity (as agent for the donor).

Notwithstanding that it is the trading subsidiary and not the charity that writes the letters to the donor, it is common for the letter to be on charity headed paper and to contain marketing information about the charity. Additionally, in order for the charity to process the Gift Aid claim, it is necessary for the personal data of the donor to be provided to the charity if it has been collected by the trading subsidiary; similarly, the trading subsidiary requires the personal data in order to act as agent under the Agency Agreement, so it is necessary for the personal data to be provided to the trading subsidiary if it has been collected by the charity.

Compliance with GDPR

The GDPR does not prevent the sharing of personal data between charities and their trading subsidiaries where this is necessary in connection with the Retail Gift Aid scheme. However, in order to ensure that the processing is fair and transparent, as required under the first data protection principle, **individual donors must be made aware of how their personal data may be shared between the two entities.**

The most effective way to achieve this is to describe the sharing arrangements within your Information Notice. Ideally, the Information Notice should start with a 'who we are' section and this is the ideal place to state that when you use the name of the charity or the terms 'we' or 'us' you mean **both** the charity and the trading subsidiary. Within the body of the Information Notice you can then go into more detail about the specific roles played by each entity.

Do bear in mind that you must also have regard to all of the other data protection principles when it comes to sharing personal data in connection with the Retail Gift Aid scheme. In particular, you should make sure that each entity is only handling the personal data that is actually necessary for its part in the Retail Gift Aid scheme process and is not keeping the personal data for any longer than its contribution necessitates, and that if personal data is being shared between different systems appropriate security measures are in place.

In practice, most charity shops that operate the Retail Gift Aid scheme via a trading subsidiary do so in a way that does not involve very distinct activities between the two entities. The most common approach is for the charity to run the shop, hold the lease of the premises, employ all staff and engage all volunteers. The trading subsidiary is only involved in the sale of bought-in goods and the sale of goods under the Retail Gift Aid scheme (the charity directly sells all donated goods that have not been donated under the Retail Gift Aid scheme). However, all sales of goods are dealt with by the same staff and volunteers (i.e. those employed or engaged by the charity). Therefore, there is usually an agreement between the charity and the trading subsidiary under which the trading subsidiary is charged an appropriate proportion of the charity's overheads for running the charity shop.

Where arrangements similar to those described above are in place, it is likely that staff employed by the charity (and/or volunteers engaged by the charity) will collect and process all personal data relating to the Retail Gift Aid scheme on behalf of **both** the charity and the trading subsidiary in relation to their respective roles under the scheme (which should be explained in the Information Notice), and the data will be held on one central database belonging to the charity. The charity's staff will then process the data as required, and send out the compulsory HMRC letters on behalf of the trading subsidiary. In these circumstances, it is unlikely that any additional steps will be required relating to retention of data by the trading subsidiary or that any additional security measures will be required in relation to the sharing of data between the charity and the trading subsidiary, as the data will not be held on multiple databases and will only be retained on the central database for so long as it is required to be retained by HMRC for compliance with the Retail Gift Aid scheme (see chapter 3 of this guide for more detail on record retention).

7. The right to be forgotten

In this chapter we will explain what the 'right to be forgotten' means, when it is available and when it is not available in relation to the obligation of charities to retain Gift Aid personal data in order to comply with HMRC requirements in relation to the Retail Gift Aid scheme.

Introduction

Individuals are given a number of specific rights under the GDPR designed to ensure that they understand and, in some circumstances, can control, who has their personal data and what it is used for. Particular rights granted to individuals under the GDPR include:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling.

NOTE: Giving a full explanation of each of these rights and the circumstances in which they can be exercised is outside the remit of this guide, but detailed information can be found on the Information Commissioner's Office website (www.ico.org.uk).

In this chapter of the guide, we will focus solely on the right to erasure, or the '**right to be forgotten**' as it is more commonly known.

When does the 'right to be forgotten' apply?

Individuals have the right to have their personal data erased if:

- the personal data is **no longer necessary** for the purpose for which the charity originally collected it
- the charity is **relying on consent** as the lawful basis for holding the data, and the individual **withdraws their consent**
- the charity is **relying on legitimate interests** as the basis for processing, the individual objects to the processing of their data, and there is **no overriding legitimate interest** to continue this processing
- the charity is processing the personal data for **direct marketing** purposes and the individual **objects to that processing**
- the charity has processed the personal data **unlawfully**
- the charity must delete personal data to comply with a legal obligation
- the charity has processed the personal data to offer **information society services to a child**.

Where one of the above reasons applies, an individual may make a request for the personal data you hold about them to be deleted.

Be aware that there is no requirement for the request to be made in writing or to make any reference to data protection law, so it is important that your staff and volunteers are trained to recognise 'right to be forgotten' requests and know to whom within the organisation they should pass them. Unless a request is particularly complex, you must act upon it **within one month** from the data that the request is made.

When does the 'right to be forgotten' not apply?

There are a number of exemptions from the right to be forgotten and you should always consider whether one of these might apply before deleting personal data. If the charity needs to continue processing the personal data for one of the following reasons it will not be required to delete the personal data:

- to exercise the **right of freedom of expression and information**
- to comply with a **legal obligation** (such as retaining Retail Gift Aid records in line with HMRC requirements)
- for the performance of a task carried out in the **public interest** or in the exercise of official authority
- for archiving purposes in the **public interest**, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- for the establishment, exercise or defence of **legal claims**.

Can we refuse to comply with a request for other reasons?

A charity may also refuse to deal with a 'right to be forgotten' request for erasure if it is **obviously unfounded or excessive**.

In these cases, you can require that the individual pay you a reasonable fee to deal with their request (which should be based on your actual administrative costs) or simply refuse to deal with the request. You must let the individual know as soon as possible if you are going to charge a fee or refuse a request.

Practical tips for dealing with 'right to be forgotten' requests

- Make sure all of your staff and volunteers have been trained to recognise 'right to be forgotten' requests, know who they should tell about the request and are aware that time is of the essence.

- Take the time to understand whether you are required to comply – is the individual entitled to make the request and does an exemption apply? Remember that you are not obliged to delete data if you are required to retain the personal data to comply with a legal obligation, for example, the requirement to retain Retail Gift Aid records to comply with HMRC record retention requirements.
- Make sure you know who is making the request – it is good practice to ask for ID.
- Ensure you know how long you have to respond and that you don't miss the deadline. Remember to search all relevant systems and databases where the personal data might have been stored.
- Consider whether you have shared the personal data with others; if so you must let them know that a request has been received.
- Make sure you document the request and how it was handled.

Distinguishing between the 'right to be forgotten' and the 'right to prevent direct marketing'

The 'right to be forgotten' and the 'right to prevent direct marketing' are two totally separate rights under the GDPR. It is important that you understand the difference between them. The 'right to be forgotten' is a right to have personal data records **permanently deleted**. The 'right to prevent marketing' is a right to stop an organisation sending its marketing materials.

The 'right to prevent direct marketing' is best served by the use of **suppression** – keeping a few identifying details of an individual so you can ensure they are not inadvertently added back to your marketing database in the future.

Individuals will not necessarily understand the difference between the two rights or understand that the best way for you prevent direct marketing is actually to keep a record of their details. Therefore, when you receive a 'right to be forgotten' request it is important that you engage with the individual to understand what they are trying to achieve and co-operate with them to identify the most effective way to deal with their request.

8. Using EPoS systems

As mentioned in chapter 4 of this guide, most charity shops collect data electronically, often using third party software such as EPoS systems.

In this chapter, we will cover key issues to be aware of in relation to **contracts with providers of EPoS systems**.

Contracting with data processors

The GDPR makes a distinction between 'data controllers' and 'data processors'. A data controller is the decision maker; it will decide what personal data to collect and what purposes to use it for. A data processor will perform specific processing tasks on the data controller's behalf; it will have access to certain personal data but may only use it in accordance with the data controller's instructions and will have no discretion as to how or why that personal data is used. When a charity uses an EPoS system, the provider of that system is likely to be classified as its data processor.

Before entering into a contract with an EPoS system provider, the charity shop should undertake some due diligence to satisfy itself that the provider has good data protection compliance measures in place and a thorough understanding of the legal requirements under the GDPR. This might include researching whether the provider is reputable and whether it has any history of data breaches, asking for an explanation of the security measures it employs and what policies and procedures it has in place. A reputable provider will not be offended to be asked such questions and might even have a prepared statement to provide to potential customers.

To comply with the GDPR, the charity shop must ensure that it has a written contract in place with the EPoS system provider. The contract must contain certain information regarding the processing activities and a number of mandatory clauses.

- The processing details that must be included in the contract are:
 - the **subject matter** and duration of the processing
 - the **nature and purpose** of the processing

- the **type** of personal data and **categories** of data subject
- the **obligations and rights** of the controller.
- The mandatory clauses that must be included in the contract are:
 - that the processor **must only act on the written instructions** of the controller (unless required by law to act without such instructions)
 - that the processor must ensure that people processing the data are subject to a **duty of confidence**
 - that the processor must have appropriate **security measures** in place
 - that the processor must only engage a **sub-processor** with the prior consent of the data controller and a written contract in place
 - that the processor must **assist the data controller** in providing subject access and allowing data subjects to exercise their rights under the GDPR
 - that the processor must **assist the data controller** in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
 - that the processor must **delete or return** all personal data to the controller as requested at the end of the contract
 - that the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In practice, it is likely that a charity shop will be contracting on the EPoS system provider's standard terms of business. However, you should check those terms of business to ensure that they contain all of the required details and mandatory clauses listed above. It might also be possible for you to negotiate more favourable liability clauses if you are not happy with ones in the provider's standard terms of business.

As a rule it will be easier to negotiate terms successfully with a smaller provider, but it is always worth raising the issue if liability is a concern. Agreeing that the EPoS system provider will accept liability up to the limits of its insurance coverage is a common position.

If an EPoS system provider does not have GDPR compliant clauses in its terms of business, this should be a **significant concern**. Unless the provider is able to offer an acceptable explanation as to why its contract is not compliant, the charity shop would be well advised to consider alternative providers. Ignorance of the law is not a sufficient explanation.

Using an EPoS provider: top tips

- You should ensure that you understand where the personal data processed via the EPoS system will physically be stored. It is easy to overlook this issue, particularly if using a cloud based service. If personal data records will be stored or processed outside of the European Economic Area you will need to ensure that adequate safeguards are in place, such as standard contractual clauses or registration under the Privacy Shield. You should also ensure that you provide details of the transfer and security safeguards that are in place within your own Information Notice.
- You should clarify whether the EPoS system provider uses any sub-processor in providing the services. If so, the provider will need a specific or general authorisation from the charity shop to use sub-processors and must ensure that it has written contracts in place with each of them which mirror the data processing terms agreed between the charity shop and the provider.

9. Staff and volunteers

There are a number of important requirements that must be met when signing donors up to the Retail Gift Aid scheme. Charity shops are required by HMRC to provide adequate training to staff and volunteers working within their charity shops, and must be able to demonstrate that this has been done.

This chapter provides a brief overview of the **HMRC requirements for staff and volunteer training** and some top tips for GDPR compliance in this context.

Staff training: HMRC requirements

HMRC guidance states that *“all shop staff involved in the process must undergo training to understand the importance of following the correct procedures and to correctly explain the scheme to donors. Shop staff need to understand that goods can’t be sold on behalf of individuals who do not pay sufficient UK Income Tax and/or Capital Gains Tax. All staff operating the scheme should be aware that anyone who joins the charity’s scheme and doesn’t pay enough tax may have to pay back to HMRC the tax claimed by the charity.”*

Key requirements on which staff and volunteers must receive training include (this is not an exhaustive list).

- Understanding that the scheme is only available to UK tax payers, and knowing how to check this with donors in a customer-friendly manner.
- Understanding the **nature of the arrangements** under the Retail Gift Aid scheme and being able to explain the arrangements to donors, including the nature of the agency arrangement, how Gift Aid applies, and the consequences for the donor if a Gift Aid declaration is made when insufficient tax has been paid by that donor to cover the claim.
- How to **process goods** under the Retail Gift Aid scheme, including sorting, tagging and processing sales of Gift Aided items.
- How to **use the EPOS system** and any other relevant processes for recording and storing Gift Aid declarations, the Agency Agreement and any other records required to be maintained under the scheme.

Charity shops should **keep records of all staff and volunteer training and guidance** that is provided, so that in an HMRC audit they are able to demonstrate that their staff and volunteers have a good understanding of the requirements and processes involved.

Additionally, there is a prohibition on ‘incentivising’ staff to increase sign-ups for Retail Gift Aid. HMRC guidance states that *“inappropriate schemes, specifically designed to increase Gift Aid income, including targets for Gift Aid take up, publishing league tables of shops, giving bonuses, incentives, or otherwise rewarding increased Gift Aid claims from individual shops might lead to some shop staff not following processes correctly. Charities with inappropriate schemes can’t claim Gift Aid on the proceeds from the sale goods sold on behalf of individuals. Where targets or other schemes are in place, they should only be used for monitoring performance and identifying training needs, rather than to directly reward shop staff.”*

GDPR compliance: top tips

- Make sure your staff and volunteers are given data protection training so that they understand the reasons behind the policies and procedures you have implemented and the potential consequences if they are not followed, and that adequate records are kept regarding who has attended training.
- When you talk to your staff and volunteers about personal data breaches make it relevant to them. Giving examples of breaches that have occurred previously or that are particularly likely in the shop environment will help them to recognise any breaches they come across in the future.
- Ensure that the name and contact details of your data compliance manager or data protection officer are readily available to staff and volunteers.
- Increase awareness and vigilance by putting up some of the ICO’s posters and postcards where your staff and volunteers will see them regularly (there are a range of these that can be downloaded and printed from the ICO’s website for free).
- Be mindful that data protection rules apply to the way you handle your staff and volunteers’ personal data too; remind your staff and volunteers to be respectful of the personal data they might hold about each other and only to use it in ways they would be happy for their own personal data to be used.

10. Promoting other fundraising events and social media issues

We are aware that many charity shops are increasingly involved in other fundraising initiatives within charities. This might include signing people up to participate in 'fun run' or similar events, taking photographs of people donating goods and sharing them on social media, etc.

Whilst these are all great ways of maximising the value of your charity shop, it is important to be aware of the potential implications in relation to personal data in this context.

In this chapter we include some of our 'top tips' regarding things to be aware of in managing these sorts of issues and when to seek further advice.

NOTE: GDPR in relation to social media is a complex topic, and it is beyond the remit of this guide to cover this in any great detail.

Other fundraising activities in shops: top tips

- DO... make things as easy as possible for your staff and volunteers by providing them with well written sign up forms that have been prepared with data protection in mind.
- DO... give staff clear instructions about where information or completed forms should be stored or sent and how this should be done.
- DO... tell staff who to speak to if they have questions or concerns.

- DO... remind staff that they should **never** post a picture of a colleague or customer on social media without obtaining their consent and making a record of how and when it was given.
- DON'T... overcomplicate – avoid complex processes or events requiring multiple forms.
- DON'T... overload – there are only so many different initiatives your staff and volunteers can keep up with at once!

11. Answering your questions

To ensure that this guide addresses the issues that you are most concerned about, the CRA asked its Gift Aid Special Interest Group to consider scenarios where they are unsure what they need to do in order to be compliant with GDPR.

In this chapter, we provide answers to three specific questions raised by the CRA Gift Aid Special Interest Group.

Question 1: We have taken on a new volunteer in a charity shop that runs a Retail Gift Aid scheme. What GDPR training do we need to provide them with, and what is the minimum amount of information they need to know to pass on to new donors signing up to the scheme?

All staff and volunteers should be given some basic data protection training as part of their induction. This may be delivered internally or you may use an external resource, such as a webinar. In addition to the formal training, the volunteer should be made aware of key policies and procedures that the charity has in place in respect of handling personal data and told who to notify in relation to potential data breaches or data subject rights requests.

The induction process should include clear instruction in relation to Retail Gift Aid. As explained in chapter 9 of this guide, this is an HMRC requirement. Provided that the charity has created compliant Gift Aid declarations and Agency Agreements, these should address the data protection issues. However, volunteers should be reminded about how and when they should make Information Notices available when dealing with donors. You might decide to issue these in hard copy as standard alongside paper forms or attach an electronic version to email letters or simply publish the Information Notice on your website. Whichever approach is chosen, the volunteer should be made aware of the approach the charity has decided to take and know what to do if an individual asks for a further copy or for the Information Notice to be made available in a different format.

Question 2: We've had a serious data breach, as a bundle of forms sent up to head office to be scanned in have been lost in the post. What do we do next?

You should have a breach management policy in place outlining the measures that will be taken where an actual or potential breach is identified. This should cover breach identification, internal reporting, containment and recovery, risk assessment, notification and evaluation. All staff and volunteers must be given training to ensure they are able to recognise potential breaches and are familiar with the internal reporting procedure.

Under the GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Examples of personal data breach given in the ICO's guidance on personal data breaches include: access by an unauthorised third party; deliberate or accidental action (or inaction) by a data controller or data processor; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; and loss of availability of personal data.

Once a breach report has been received, the charity will need to investigate to understand the nature of breach, whether the breach can be retained or personal data recovered and what risks might arise for individuals.

If the breach carries a risk to individuals, the charity must report the breach to the ICO **within 72 hours** of becoming aware of it. The charity should follow the guidance on the breach reporting section of the ICO's website, which explains exactly what information should be provided and how.

If the breach is considered to carry a high risk to individuals (e.g. because it involves sensitive or financial data) the charity will also have to notify any affected individuals. Again, the guidance on the ICO website should be followed in this regard, but the charity should focus on ensuring that it notifies in a way which is informative, constructive and helpful to the affected individuals.

The ICO guidance on personal data breaches recognises that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and

material damage. Some personal data breaches will do no more than inconvenience those who need the data to do their job whilst other breaches can significantly affect individuals whose personal data has been compromised. The charity will need to assess this on a case by case basis, looking at all relevant factors.

By way of example, the ICO provides the following illustration: *“The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.”*

With regard to identifying a high risk breach that would be notifiable to the affected individuals, the ICO guidance indicates that both the severity of any potential impact as well as the likelihood of potential consequences arising should be considered. By way of example, a loss of medical records is indicated as a breach that would need to be reported to the individual, whilst a university accidentally deleting records of alumni from its database which could be restored from a back-up is an issue that would not require notification to the individual.

The ICO has a dedicated breach reporting help line which charities should use where necessary. The number is **0303 123113**.

The charity must record details of the breach on its internal breach log, even if it decides that the breach does not need to be reported to the ICO or any individuals.

Finally, after the initial urgency of dealing with the breach has subsided, the charity should always take the time to evaluate and assess. Could future breaches be avoided through implementing different policies or procedures? Did the charity handle the breach as well as it could have?

Case study 3: Someone comes into our shop and asks to see the charity’s privacy statement – what do we need to do?

The charity’s privacy policy should be provided, if requested. All staff and volunteers should know where the charity’s privacy policy is made available. This will generally be on the charity’s website, but it is good practice to hold some paper copies at the shop that can be given out in this situation.

12. Further guidance

HMRC guidance

HMRC guidance on Gift Aid is available here (see section 3.42 for the section specifically relating to the Retail Gift Aid scheme): www.gov.uk/government/publications/charities-detailed-guidance-notes/chapter-3-gift-aid

HMRC Gift Aid declaration form for use in connection with the Retail Gift Aid scheme: [www.gov.uk/government/uploads/system/uploads/attachment_data/file/517693/Charity Gift Aid Declaration - When goods are sold by and the proceeds gifted to charities.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517693/Charity_Gift_Aid_Declaration_-_When_goods_are_sold_by_and_the_proceeds_gifted_to_charities.pdf)

Letters to donors

HMRC template letter (standard method): www.gov.uk/government/publications/gift-aid-claim-template-letter-standard-method

HMRC template in-year letter (Method A): www.gov.uk/government/publications/gift-aid-template-letter-for-sales-above-the-100-limit-method-a

HMRC template end-year letter (Method A): www.gov.uk/government/publications/gift-aid-template-letter-for-the-end-of-year-method-a

HMRC template in-year letter (Method B): www.gov.uk/government/publications/gift-aid-template-letter-for-sales-above-the-1000-limit-method-b

HMRC template end-year letter (Method B): www.gov.uk/government/publications/gift-aid-template-letter-for-the-end-of-year-method-b

GDPR guidance

ICO resources for charities: <https://ico.org.uk/for-organisations/charity/>

Fundraising Regulator's Guidance and information (Data Protection for Small Charities):
[www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/
data-protection-library-general-data-protection-regulation-gdpr/](http://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/data-protection-library-general-data-protection-regulation-gdpr/)

Fundraising Regulator's Code of Fundraising Practice: [www.fundraisingregulator.org.
uk/code-of-fundraising-practice/code-of-fundraising-practice-v1-4-310717-docx/](http://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice-v1-4-310717-docx/)

13. Birketts' Charities and Social Enterprise Team

Our Charities and Social Enterprise Team comprises specialists in charity law and regulation. The team is multi-disciplinary, advising charity clients on matters relating to all aspects of their constitutional, governance and operational needs.

Our team comprises lawyers with a particular commitment to their work in this sector, including senior lawyers with significant experience in advising registered and exempt charities, as well as social enterprises and community-based organisations (including community interest companies and community benefit societies).

Our team's background and experience delivers advice that is not only technically excellent but, above all, practical. Many of our team also advise public bodies, commercial entities and high net worth individuals and, accordingly, are familiar with the contracting, funding, gift and legacy issues that charities commonly encounter.

We offer comprehensive advice to all our charity and social enterprise clients including advice on:

- legal structures / collaborations / mergers and restructuring
- charity set up and incorporation
- contracting arrangements, procurement, trading and subsidiaries
- charity retail and Gift Aid for charity shops
- Tax and VAT
- regulatory compliance, investigations and enforcement
- public law, judicial review, disputes and litigation
- governance, trustee duties and responsibilities
- employment, health and safety, safeguarding
- funding, fundraising, sponsorship
- intellectual property, trade marks, data protection
- legacy administration, contentious legacies, and trusts
- construction, property and planning.

14. Birketts' data protection training

Birketts offers a range of training courses on data protection compliance as part of our Shaping Excellence programme. Our standard courses include:

- practical data protection law – a comprehensive introduction for staff
- practical data protection law – handling subject access requests
- the General Data Protection Regulation – getting to grips with the new law.

Full details can be found on our website at: www.birketts.co.uk/shapingexcellence

For details of bespoke data protection training, please contact Kitty Rosser at kitty-rosser@birketts.co.uk or on 01603 756559.

15. Contacts



Liz Brownsell
Senior Associate
Co-Head of Charities and Social Enterprise
01473 406383
liz-brownsell@birketts.co.uk

Liz is Co-Head of Charities and Social Enterprise at Birketts. Her expertise covers a wide range of matters affecting charities, including set up and incorporation, mergers, structuring, governance, commercial arrangements and contracts, trading and charity retail (in particular Gift Aid for charity shops), fundraising (including arrangements with commercial participators and professional fundraisers), matters involving the Charity Commission, releasing permanent endowment and other restricted funds, and general charity law.

Liz has an active interest in the development of the sector and has been involved in a number of CLA Working Parties, including Lord Hodgson's review of the Charities Act 2006 and the Law Commission's consultation on technical issues in charity law. Most recently she was a member of the Charity Law Association Working Party looking at the proposed new Charity Governance Code.

Liz leads the firm's in-house training offering to our charity clients through Birketts' Shaping Excellence Programme, and regularly delivers seminars on a variety of topics. Liz also writes for sector media and has published a number of articles in publications such as Charities Management Magazine.

**Kitty Rosser****Senior Associate**

01603 756559

kitty-rosser@birketts.co.uk

Kitty joined Birketts in 2014. She is a Senior Associate in our Corporate and Commercial Team.

Kitty is an intellectual property lawyer. She assists clients with the identification, protection and exploitation of their intellectual property rights, including trademarks, patents, copyright, design rights and domain names.

Kitty advises on all aspects of data protection compliance including subject access requests, marketing strategies, handling of data breaches (including responding to complaints by individuals and handling ICO investigation), data transfers, preparation and implementation of policies and procedures. She also provides bespoke data protection training.

In the IT field, Kitty negotiates and drafts IT contracts including development contracts for waterfall and agile methodologies and is experienced in advising on both traditional software licensing and SaaS/PaaS licensing models.

Keep up-to-date

Subscribe to our mailing list for insights, industry information and event invitations.

www.birketts.co.uk/register

Follow us:



@birkettsllp



[linkedin.com/company/birkettsllp](https://www.linkedin.com/company/birkettsllp)



@birkettsllp

Cambridge:

01223 326600

Chelmsford:

01245 211211

Ipswich:

01473 232300

Norwich:

01603 232300

Central fax:

01473 230524

For a full list of office and contact details please visit

www.birketts.co.uk/contact-us

Birketts LLP is a limited liability partnership authorised and regulated by the Solicitors Regulation Authority and registered in England & Wales with registered number OC317545.

A list of members may be inspected at any of our offices. The term 'partner' is used to refer to a member of Birketts LLP.

©Birketts 2018.

