Association of Independent Museums

Helping Heritage Organisations Prosper

Success Guides

SUCCESSFULLY MANAGING PRIVACY AND DATA REGULATIONS IN SMALL MUSEUMS

Written by Helen Shone, 2017
Revised by Faye Clews, 2019
Development Partners

CONTENTS

WHO IS THIS GUIDE FOR?

This guide is intended for museums and other cultural organisations wanting to understand how they should be responding to current data protection regulation.

The General Data Protection Regulation (GDPR) is an EU-wide regulation which came into effect on 25 May 2018. The GDPR gives individuals more rights and protection in how their personal information (their data) is used by organisations.

There are two other pieces of legislation controlling the use of personal information, which work alongside the GDPR:

- The Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulation 2003 (PECR)

This guide focuses on the combined effect of the GDPR and these two pieces of legislation, and covers the most important areas for action now. The GDPR applies to the whole UK, so this guide is suitable for all AIM members across the UK.

The GDPR applies to the whole UK, so this guide is suitable for all AIM members across the UK.

Data protection regulations are far more wide reaching than discussed here and we recommend reviewing the guidance and the regular updates provided by the Information Commissioner's Office (ICO) and the Fundraising Regulator as well as other organisations listed in the further reading section.

www.ico.org.uk

www.fundraisingregulator.org.uk

This guide is for trustees, senior teams, members of staff and volunteers involved in fundraising or marketing. However, it would be useful to share the key points with all staff and volunteers since so many of them will come into contact with data collection and processing in the course of their working week. Remember that data protection is not just a fundraising issue, it relates to any data that the organisation collects and uses, from admissions and gift aid declarations to mailing lists and volunteer information.

This guide will outline the main data protection issues to help you carry out an audit of your current position and draw up an action plan. It aims to be a practical guide that will put you on the right path for data protection compliance.

What about our collections and archives?

Many heritage organisations will hold personal data in their collection and archives. As before, although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception in the GDPR if you are keeping it for these archiving, research or statistical purposes.

This exemption applies if your organisation can say that the processing of personal data is necessary for archiving purposes in the public interest or necessary for historical research purposes.

You must have appropriate safeguards in place to protect the rights of individuals whose personal data is being processed. In practice this means:

- Good security measures both in terms of physical security and IT security
- Good policy and procedures
- Only processing what the organisation really needs (data minimisation)

Moving forward, as your organisation acquires new objects or make new loans etc., you should make sure your privacy policy is shared unless this is deemed impossible or disproportionate, and carry out and document a data protection impact assessment regarding the information collected. The Collections Trust and the National Archives provides more guidance:

https://collectionstrust.org.uk/resource/data-protection-guidance-sheet/

https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

WHY ARE YOU COLLECTING DATA?

In the past many organisations have collected data simply because they have had the opportunity, and not because they knew how they would use it. A simple piece of advice is to be mindful and strategic about the data that is collected - be clear why it is that you are collecting data and what you plan to do with it. Document your decisions: the GDPR's new accountability principle requires organisations to be able to show how they comply with data protection regulation, meaning that a record of your decision-making must be kept.

Document your decisions: the GDPR's accountability principle requires organisations to be able to show how they comply with data protection regulation

You may wish to collect personal data for a wide range of purposes, with some of the most common being:

- Newsletter mailings?
- Fundraising appeals?
- Volunteer management
- Events?
- Gift Aid

Only collect the information you need

The GDPR says that: 'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).' This means that you should only collect data that is useful and avoid extraneous information that is irrelevant to your purposes. This also creates a smaller workload for data cleaning and management.

Sensitive personal data (known as 'special category data' under the GDPR) requires more protection under the new regulations. This relates to information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, genetic and biometric data, physical or mental health, sex life or sexual orientation, or details of criminal offences. There are ten specific conditions for processing special category data under Article 9 of the GDPR and you must determine and document which condition you are using before you begin to hold and process this information.

Remember that everyone has the right to request access to the data that you hold

Remember that everyone has the right to request access to the data that you hold, so keep it objective and don't record anything that could jeopardise your reputation. It can be helpful to imagine the data subject standing behind you when entering their information on the database.

Only keep data for as long as you need it

Don't allow personal data to sit around indefinitely. It is tempting to keep hold of the data 'just in case' it is useful, but as the information gets older it becomes less of an asset and more of a liability.

As time passes, it becomes more difficult to ensure that information is accurate; increasing the risk that outdated information will be used in error. Holding on to old data also increases the data burden: it must still be kept securely despite the fact that it is not useful, and the organisation must respond to subject access requests, even though you haven't been using it.

Although no absolute time-scale is given by the GDPR, it states that personal data shall be kept 'no longer than is necessary'. You need to set your own internal rules about how long this should be but there is probably little point in sitting on data that has been dormant for many years.

Be aware that there may be information that is needed for a long period for statutory or reporting reasons; Gift Aid records, for example, must be kept for six years after the relevant accounting period. You can also keep anonymised data for as long as you want. So where appropriate, it is perfectly acceptable to create a skeleton record which keeps certain data fields active for a longer period than other superfluous details.

Having set your internal rules, this should be documented in a simple data retention policy, and a system set up to ensure it is implemented and periodically reviewed. It may be a challenge initially to identify and delete old data (which may be sitting in paper files as well as spreadsheets and databases), but a one-off effort to get the organisation to a sensible data retention position will pay off in the longer term.

HOW ARE YOU COLLECTING AND STORING DATA?

The next step in your data audit is to consider how you are collecting your data and how you are storing it.

Where are your collection points?

Most organisations collect data from a number of different sources. These touch points could be:

- Visitor reception
- Online donations
- Friends group
- Newsletter sign up
- Gift Aid data
- Events
- Commercial hire
- Retail
- Volunteer management systems

Organisations need to be consistent in their approach to gaining consent wherever it is collected. This is important for your supporters' experience, but even more so for back office systems that support your activities - it is very difficult to keep good records on consent if you are asking different questions in different places. Think through the different places that you collect data and consider whether the approach to gaining consent is streamlined.

It doesn't matter if the systems are paper-based in one area of the site and electronic in another, but the main consent statement and options need to be aligned. More information on consent is provided in the sections below.

How do you store your data?

There are two main data protection issues when it comes to data storage:

1. Data security

Storing data securely has always been a requirement under the DPA. However the GDPR goes further by providing specifics about the security of your processing and how you should assess your information risk; these are now legal requirements.

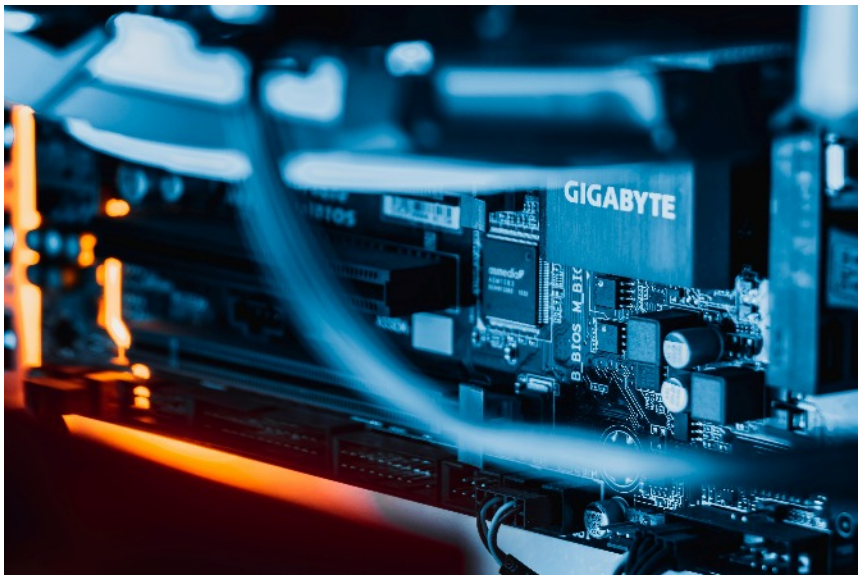
The GDPR's security principle states that personal data shall be:

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

Databases tend to be more secure than paper-based systems and spreadsheets. They are independent of a computer network's main shared documents and require passwords to log in.

Typically, access is limited to those who need it. Risk areas include (though are not limited to) a large number of people having access to the database, lack of suitable data back up process, and data reports downloaded onto the main computer shared drive where anyone can access them. Security should be reviewed periodically to ensure that you are reducing the risk of any data breach.

It is not a requirement to have a database to manage your data - a paper-based or spreadsheet system is fine if this is proportionate to the amount of data you hold and process. But security of these systems must also be reviewed on a regular basis, and procedures put in place to mitigate any security risk. You must document your decision-making and actions.



As part of your data security audit, you should look at the journey that your data takes.

As part of your data security audit, you should look at the journey that your data takes. If you input straight onto a database, then it is a very short one, but not all systems are this high-tech. An example scenario at a small museum could be as follows:

Visitors fill in a paper form at reception on arrival. The form is passed on to an administrative member of staff or volunteer who puts the data onto a spreadsheet.

Risk points could be:

- The form is left unsupervised on the visitor reception desk.
- The form is not shredded or appropriately filed away after the information is put onto the data spreadsheet.
- The data spreadsheet can be accessed by all staff and volunteers who have access to the shared computer network.

All of the above outcomes could lead to information getting into the hands of people inside or outside the organisation who have no right to access it. Mitigation of these risks could be:

- A lockable drawer at reception to ?keep forms in when the desk is unsupervised.
- A system of shredding or redacting personal data is put in place for forms that have been processed.
- The data spreadsheet or the relevant area of the computer network is password protected, with only appropriate people given access.

2. Storing consent data

Organisations need to be consistent in their approach to gaining consent wherever it is collected.

The GDPR require organisations to gather and record more information relating to consent than under the previous system. It states that consent cannot be assumed to last forever, and so organisations are required to record the date that consent was given. And if a supporter subsequently 'opts out' it will be necessary to record the date of this too. The rules also require organisations to offer supporters the option to opt in or out of different communication channels, such as post, email, phone and SMS.

As you can imagine, the combination of these requirements necessitates a large number of new fields in your databases or columns in the spreadsheets. Older databases may not be configured to support these new requirements and so a 'work around' has to be found, using fields that you can 'query' or search as needed.

WHEN DO YOU NEED CONSENT?

Data processing refers not just to the communications that you send out, but also to the range of ways that you may use personal data, from analysis of visitor statistics to prospect research. Some of these activities are considered more 'intrusive' (to use the ICO's description) and therefore may require consent to carry them out. Others can be carried out on the basis of 'legitimate interest' described below. The ICO advises "Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative."

CAN YOU RELY ON 'LEGITIMATE INTEREST'?

There are six different legal bases for processing data, but Consent and Legitimate Interest are the most relevant to fundraising and marketing. If you are going to rely on Legitimate Interest you must balance your organisation's interests to process personal data to meet its objectives against the rights of the individual. The outcome of this balancing test determines whether personal data can be processed without needing consent.

You can rely on legitimate interest for marketing activities (specifically communicating by post or phone) if you can show that how you use personal data is proportionate, has minimal privacy impact, and people would not be surprised or likely to object.

However the exception is electronic marketing (email and SMS) and automated phone calls, which requires explicit consent from the individual (under the Privacy and Electronic Communications Regulations 2003).

The GDPR requires organisations to consider the 'reasonable expectations' of individuals based on their relationship with you. If the individuals in question do not have a relationship with you and would be surprised to receive a mailing, then it is likely that the balancing act would not be in your favour. In addition, you should consider the frequency of the mailings you are sending - for instance, the individuals concerned may feel that monthly mailings are unreasonable, but may be happy to receive an annual update. The ICO provide Legitimate Interest guidance and a helpful Legitimate Interest Assessment template on their website.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/

When you are relying on legitimate interest as your basis for a mailing, you must always provide a prominent and easy step for opting out of future direct mail. And remember that once someone has opted out, the legitimate interest rule cannot be used, so you must find a way to exclude them from your future mailings.

Under GDPR, public bodies (including local authority museums) will no longer be able to rely on legitimate interest as a legal basis for data processing without consent. Instead, they will need to be able to show that 'the processing is necessary for the performance of a task carried out in the public interest' or 'for the performance of a contract with the data subject'.

DATA PROCESSING ACTIVITIES: CONSENT VERSUS LEGITIMATE INTEREST

Performance of a contract / service communications

When someone buys event tickets or orders something from your online shop, they expect to receive confirmation in the same way that they made the transaction - i.e. by email if sent by email or submitted online, or by post if sent by post. This type of confirmation is not designated a direct marketing activity and **can take place without consent.**

The Privacy and Electronic Communications Regulations (PECR) make an exemption in terms of email consent for further follow up communications to this type of commercial activity. You may send information that is directly relevant to the first communication without opt in consent. So someone who buys an event ticket and provides an email address for the processing can be sent information about other events, and someone who buys something in the online shop can be sent emails about other products - but in both cases you cannot add them to a general mailing list. You must always provide an opportunity to opt out of these emails.

Aggregate data

Analysis of aggregate data is considered unobtrusive, as you are not looking at one individual's behaviour, but at the group as a whole. **Consent is not needed.**

Direct marketing

Any mailings which further the aims and objectives of an organisation are considered direct marketing. This includes bespoke letters and individual phone calls, which can be surprising as we tend to think of direct marketing as something sent to large numbers of people. It means that almost all types of communication with supporters need to be covered **either by consent or the legitimate interests rule.**

Prospect research

Prospect research involves the gathering and analysis of biographical, financial, corporate and philanthropic information from a wide variety of sources (both publically available and those unique to your organisation such as your database). Major donor fundraisers use research to ensure that prospects are approached about an area of interest that is most appropriate and in the way most suited to them. Indeed, many philanthropists and high net worth individuals have come to expect this level of research and preparation as part of the process.

There has been much discussion and debate in recent years around how the DPA and now the GDPR apply to charities when carrying out research into existing and new potential major donors.

To comply with data protection legislation, when you are 'processing' someone's data (i.e. doing anything with it, including obtaining, recording, holding or using it for any purpose) you need to do it fairly, lawfully and transparently. So this means that people need to know what you are doing with their data. It also has to be kept securely, accurately, and for no longer than is necessary.

In December 2016 and April 2017, the ICO fined a total of 13 charities under the existing Data Protection Act for offences that included wealth-screening, a form of profiling (often outsourced to specialist agencies) that assesses how much money someone has and how likely they are to donate.

The connecting factor in all of these ICO cases was the issue of consent. The ICO stated that the activities themselves were not illegal; the problem was that they had not informed people that they planned to do these things with their data, and so people did not have the opportunity to object. In all cases, the organisations had consent statements and privacy notices in place, but the ICO ruled that they had not been sufficiently clear in these about how they would be using their supporters' data.

Consent may feel like the 'safest' basis to use for prospect research (and other direct marketing activity) but it is not always practical or appropriate. For example you cannot ask a new potential prospect for their consent to process their data, before you have worked out who they are and whether they are relevant to approach.

The Institute of Fundraising advises that legitimate interest can be a lawful basis for prospect research, providing that the organisation has:

- identified their legitimate interest and showed that the processing is necessary to achieve it;
- concluded that the activity is not unduly intrusive, balancing their legitimate interest against the individual's' interests, rights and freedoms;

- ensured that the individual is made aware of how the organisation might process personal data (by sharing their privacy policy with the individual as soon as possible), and giving them the chance to prevent their data being used in that way.

In summary, **both consent and legitimate interest can be valid bases for prospect research**, providing the organisation has complied with data protection legislation as summarised above and set out in the GDPR. We advise all organisations to review the guidance from the ICO on consent and legitimate interest.

Giving your data to another charity for their own use is to be avoided

Data sharing

Consent is needed for sharing data externally - this may be with a mailing house, agency, consultancy or another organisation. The types of sharing should be spelt out clearly in the privacy policy. Data sharing should always be carried out with a contract in place as you retain responsibility for what the third party organisation does with the data. You need to check their data protection credentials and ensure that they are up to scratch before sharing.

Giving your data to another charity for their own use is to be avoided - an example could be a local organisation wanting to use your mailing list to send information about their activities directly to your supporters. If this activity is something that you cannot avoid, then the sharing activity must be explicitly and unambiguously spelt out in the privacy policy, ideally with the recipient organisation named. But where possible, just avoid this altogether.

Employee and volunteer records

This data can be processed under the legitimate interests rule. The ICO has specific guidance for employee data, which is also relevant for volunteers. It is available here:

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Membership / Friends

When people sign up to membership or a Friends scheme, they automatically provide their contact details. If their data has only been captured purely for the membership scheme, then you are restricting your data processing activities for which you have consent to those compatible with membership. However, since these people are clearly engaged with the museum, you may be able to **use the legitimate interest grounds** for non-membership communications by post. It is advisable to at least add an 'opt in' to email consent statement to the registration form which includes other communications from the museum, and a link to the privacy policy.

One of the stated benefits of a membership or Friends scheme is usually a magazine or newsletter, and this falls into the **'performance of a contract'** category. This may be sent by email (if they have given you their email address as part of the membership sign up) or post. However, what is a grey area is the content of this newsletter. Would the recipient reasonably expect this to include fundraising appeals? If members opted in to a broad consent statement and a link to the privacy policy, then this is unlikely to be a concern.

If your Friends scheme is run by a separate charity, they cannot automatically share data with the parent museum. They would need to consider the legal basis on which this is appropriate - consent or legitimate interest. This separate charity will need to abide by data protection regulations and have their own privacy policy. You may wish to support the Friends' trustees in their own process to becoming compliant as the reputation of the parent museum will be harmed by any data breach.

**This refers to emails owned by individuals. Legitimate Interest can be a lawful condition for sending emails to email addresses owned by corporate bodies, but this can be hard to identify. If in doubt, assume you need consent.*
***As covered above both consent and legitimate interest can be valid bases for prospect research, providing the organisation has complied with data protection legislation*

GDPR AND CONSENT – THE 'OPT IN' APPROACH

Under the GDPR, the standard for what counts as consent is raised from what was previously required under the Data Protection Act 1998.

The new requirement is that consent must be freely given, specific, informed and unambiguous. Individuals must show a proactive choice; consent cannot be assumed from pre-ticked boxes or inactivity. Information about data processing must be explained in a way that people can easily understand, and not hidden in jargon or ambiguity. Individuals should have the opportunity to opt in to different channels of communication (SMS, email etc), rather than be expected to sign up for all of them in one.

The ICO has published a helpful consent checklist:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

At which point should you gather consent?

The ICO and Fundraising Regulator recommend that consent to hold and process data is gained when data is first collected. This is normally achieved through the combination of a consent statement (which gives the main points) and a privacy notice (which gives the detail). Held together, these two should cover all of your data processing activities.

When it is not possible to gain consent at the point of data collection, then it should be at the first available opportunity, such as the first time you make contact with them. It is considered unacceptable to sit on names and addresses without consent just because you are not using them.

What should a consent statement look like?

The consent statement needs to tell people the basics about what you will be doing with their data, and link to the more detailed privacy policy. It should be short enough that people will read and understand it, but long enough for it to be meaningful. Don't use more formal language than usual - it is much better to adopt the same kind of tone that you use in your other communications. And since you are asking people to pro-actively opt in, aim to be engaging so that they want to sign up. Try to think of something inspiring and unique to you. It is good practice to remind people that they can subsequently opt out at any time.

- Use house style
- Be interesting, engaging
- Offer different communication channels, not just a single YES / NO choice
- Be consistent across all data collection locations and ?mediums
- Ensure your statement is not ambiguous
- Remind people they can subsequently opt out
- Provide a link to your privacy policy

Consent doesn't have to be given through a tick box or a written statement. It can be oral or via another act which demonstrates an individual's wish to opt in - for example a business card dropped into a box when it is made very clear what the card will be used for. But where consent is not written, it is best practice to confirm in writing and provide a link to the privacy policy.

WHAT IS A PRIVACY POLICY?

The privacy policy (sometimes called a privacy notice or fair processing information) is probably your most important document relating to data protection. It should be a clear explanation of who you are and what it is that you will do with an individual's data. It should cover all of your current data processing activities and attempt to future- proof against your future data processing needs, otherwise there is a risk that you will find yourselves unable to do something important at a future date.

Some examples of clear privacy policies include:

National Museums of Scotland - www.nms.ac.uk/privacy-notice

Cancer Research - www.cancerresearchuk.org/privacy-statement

It is acceptable to update privacy policies as long as they are readily accessible, but if there is a major change it will be necessary to actively bring this to the attention of your supporters.

What should a privacy policy cover?

In a way, this should be a summary of everything we discussed in this document. Remember that you must be specific, clear and unambiguous in describing your data processing activities. It must be easy for non-specialist audiences to understand what it is that you will be doing with their data. It is accepted practice to write in long-hand where needed, using a whole paragraph to explain one area of data processing if this is the best way to avoid ambiguity. You can also have a list of bullet points if this seems the best way to get your information across, but remember that clarity is prized more highly than brevity. Headings to include, where relevant, are:

- Who you are, including your charity number and address
- What personal data you collect
- What you will do with the data, examples include -
    - ❑ Mailings relating to news and events
    - ❑ Fundraising appeals
    - ❑ Research (be specific ?about the type of research you will carry out)
    - ❑ Wealth screening (explain what this is and how you will do it)
    - ❑ Aggregate data analysis, which could include monitoring visitor
    - ❑ statistics or the effectiveness of communications, including email
    - ❑ Tracking
    - ❑ Data sharing - who you will share it with and for what purposes
- Cookies on your website
- How you will store the data and keep it secure
- How people can submit a ‘Subject Access Request'
- A statement regarding updates to your privacy policy, 'We regularly review our privacy policy and may make changes from time to time.'
- The date of the latest update to the privacy policy
- How to get in touch

The Subject Access Request is a legal requirement that all organisations must fulfill if requested. This refers to an individual's right to see a copy of the information an organisation holds on them. This includes an entitlement to be:

- told whether any personal data is being processed
- given a description of the data, the reasons it is processed and whether it will be shared
- given the source of the data

Under GDPR you may no longer charge a fee unless the request is 'manifestly unfounded or excessive' or if the individual makes multiple requests.

Don't just write a privacy policy and leave it to gather dust on your desk. You need to share it with your supporters and make it easy to find.

Publicising the privacy policy

Don't just write a privacy policy and leave it to gather dust on your desk. You need to share it with your supporters and make it easy to find.
It is usual to have a web page dedicated to the privacy policy. Links to it can then be situated as a footer on your website (so that you can link to it from any page) and as a footer in your emails.

If you are producing a privacy policy for the first time, you should inform supporters, perhaps through your newsletter, magazine or other regular mailing.?It may not feel like the most interesting thing in the world to be promoting, but it is important for you to be able to demonstrate that you have made efforts to share this information.

Be prepared to manage people opting out of different elements of your privacy policy. They may say that they are happy to receive newsletters, but don't want to receive appeal mailings, for instance.

WHAT DOES THIS MEAN FOR YOUR HISTORICAL DATA?

GDPR applies to historical data, not just data that has been collected after GDPR came into force. Many organisations will have data that complied with the old system of 'opt out' i.e. "we are holding your data until you tell us not to"; others may have historical consent from individuals, but whether those consents meet the higher requirements of GDPR are questionable.

Between 2016 and 2018 organisations had a two-year transition period to get their houses in order, aligning their data processing operations to GDPR requirements. For many this involved repermissioning campaigns that saw huge reductions in the size of databases. However the situation since the 25 May 2018, when GDPR came into effect, is that if the past grounds for processing do not satisfy the new GDPR requirements, then the processing of historical data is unlawful.

So if you are relying on consent as the lawful basis for processing, you will need to assess whether the historical data you hold meets the GDPR standards. For example did individuals actively opt-in; were they given genuine choice and was it clear and specific what they were consenting to; were they provide with an opportunity to opt out; and can you date when consent was given?

If you are relying on legitimate interest as the lawful basis for processing, and you only intend to contact individuals by mail, then it is likely that you can continue to process this historical data (subject to a legitimate interest assessment).

But remember that you should only keep data as long as you need it to fulfill the purposes you collected it for in the first place. GDPR also includes a new 'right to be forgotten'; if you can't identify why you still need it, then this is an opportunity to cleanse that database.

ACTION CHECKLIST

All of your data protection decision-making should be documented through the minutes of trustee or internal meetings or in policy documents. This is so that you can show what actions you have taken to ensure you comply with regulations if complaints are made or you are audited by the ICO.

- **Assess your data collection needs against the data you are collecting. Are you collecting more than is necessary? Can you get rid of data that is not needed? How long do you need to keep your data? Create a data retention policy and implement it.**
- **Where and how are you collecting data? Are you consistent?**
- **Security: Are your data collection and storage systems secure?**
- **What changes do you need to make to your database or other systems to record consent dates?**
- **What data processing activities are you carrying out?**
- **What consent do you have to carry these out?**
- **Will you rely on the legitimate interest rule for some activities? If so, document why you consider this reasonable.**
- **How will you update your consent statement?**
- **Do you have a privacy policy? If not, create one. If you do, review it carefully.**
- **Newly created privacy policies should be publicised - how will you do this?**
- **What are your plans for your historical data?**

FURTHER INFORMATION

Arts Council England: A practical guide to lawful fundraising for arts and cultural organisations
https://www.artscouncil.org.uk/publication/practical-guide-lawful-fundraising

Collections Trust: Data Protection Guidance
https://collectionstrust.org.uk/resource/data-protection-guidance-sheet/

Fundraising Regulator: The Code of Fundraising Practice specifically Section 3: Processing personal data (information)
https://www.fundraisingregulator.org.uk/code/all-fundraising/processing-personal-data

Information Commissioner's Office: Guide to data protection
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office: Lawful basis for processing: Legitimate Interests guidance
https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf

Information Commissioner's Office: Guide to Privacy and Electronic Communications Regulations
https://ico.org.uk/for-organisations/guide-to-pecr/

Institute of Fundraising: GDPR: The Essentials for Fundraising Organisations
http://www.institute-of- fundraising.org.uk/guidance/research/gdpressentials/

Institute of Fundraising: Connecting people to good causes: A practical guide to fundraising research
https://www.institute-of-fundraising.org.uk/library/iof-connecting-people-to-causes/

National Archives: Guide to archiving personal data
https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

IMAGE CREDITS

Cover photo by Arif Riyanto on Unsplash
Page 4 photo by Curtis MacNewton on Unsplash
Page 6 photo by Stephen Dawson on Unsplash
Page 8 photo by Florian Krumm on Unsplash
Page 9 photo by Christina @ wocintechchat.com on Unsplash
Page 12 photo by Bill Oxford on Unsplash
Page 17 photo by Mari Helin on Unsplash

Supported using public funding by
ARTS COUNCIL ENGLAND

development partners

About Development Partners

Development Partners is a fundraising and business development consultancy to museums, heritage and cultural organisations. We work across the UK with organisations of all shapes and sizes from major museums to small volunteer-run heritage sites. Together we assess and capitalise on the unique opportunities of each organisation to build a stronger future.

www.development-partners.co.uk

Association of Independent Museums
Helping Heritage Organisations Prosper

The AIM Hallmarks
Visitor Focus

AIM Association of Independent Museums
AIM Postal PO Box 181 Ludlow SY8 9DR
Registered in England No. 1350939 | Charity No. 1082215