GDPR Frequently Asked Questions

Active consent.

- **Do we need to contact all clients that we have stored as data on our database?**
  Having active consent is the corner stone of GDPR which does mean that you have to contact everyone on your data base to get their active consent. Without that you cannot continue to contact them. The National Trust for example are contacting all of their members and asking them to respond with their consent otherwise the member will receive nothing further from the National Trust.
- **We use Mailchimp (a US company) to manage our email list/membership database. They say that they intend to support European/GDPR standards of data protection. How do we create a wording for people to actively consent for us to hold data about them (email address and name ONLY) and then to confirm that to us; and at the same time b) confirming that they wish to be a member of our organisation?**
  Problem solved if Mailchimp is going to meet EU standards and will issue a 3rd party agreement with you confirming this.
  Please see attached draft statement for another membership organisation that may be adapted.

Archives.

- **How can we balance GDPR compliance with maintaining and enabling the continuation and access of a historical archive?**
  Archives - Please see attached draft information sheet from Advising Communities

CCTV.

- **How does using CCTV (necessary for insurance purposes e.g. for the prevention of arson) affect our ability to meet GDPR?**
  CCTV - Please see attached draft information sheet from Advising Communities

Converting paper records.

- **GDPR appears to suggest that paper based data/files need to be converted into electronic records. Is this correct? Should this conversion be done for every single client file no matter how historically held?**

  You do not need to convert written records to electronic records but you do need to know what you have and where it is stored in case you have a request to see the data, correct it or delete it.

Data Protection Officer.

- **Do we need a data protection officer?**

  You almost certainly do not require a qualified data protection officer. However it is advised that you have a data protection officer being the point of contact especially for any data subject requesting what information you hold, to correct it or eliminate it. This should be the point of contact for all requests.

Data retention and storage.

- **Is there a clearly defined time period for storing and destroying files?**
- **When we create spreadsheets for projects that have project details including email addresses, do we have to delete them once the project has finished?**

  Data must only be kept for as long as you have consent, as long as it is still needed but there are different rules re employment records, health and safety, HMRC and Charity Commission.
  Health and Safety requires data to be held for 7 years
  HMRC requires financial data to be held for 7 years
  Charity Commission require that trustee declarations re not being disqualified are kept indefinitely. Minutes are kept for 7 years unless business critical and then keep for ever.
- **What constitutes the correct storage of digital data (we use Google (Drive, Docs, email etc.) to store and send data?**

  'Correct storage of digital data' has the same principles as paper data - must be stored in safe, secure way, limited people having access etc. So:

  - Groups should consider creating an updated inventory of personal data that they handle. Google has created some tools to help people identify and classify data.

- Review your current controls, policies, and processes to assess whether they meet the requirements of the GDPR, and build a plan to address any gap e.g. needs to be password protected where possible, access not shared widely, an IT policy in place.
- Data only to be used/accessed by trained and appropriate staff so they shouldn't store everything in open folders i.e. they should ensure the settings on google drive and docs set to private, not public. If they are processing data like membership forms etc., ensure that only a select few people can access it.
- Consider anonymising data if they don't need to know details.
- Ensure that they regularly delete data they don't need.
- Ensure that they know what's in their Google drive, docs etc. so if a person requests to see their data then they know what data they hold.
- Also need to ensure they have taken steps to prevent hacking/data leaks through up to date virus scanners etc. Perhaps consider limiting use on personal computers as this is harder to control?

Google themselves have also suggested:

- Consider how you can leverage the existing data protection features on Google Cloud as part of your own regulatory compliance framework. Conduct a review of G Suite or Google Cloud Platform third-party audit and certification materials to see how they may help with this exercise.
- Review and accept our updated data processing terms via the opt in process described here for the G Suite Data Processing Amendment and here for the GCP Data Processing and Security Terms. The updated terms will apply starting on 25 May 2018 when the GDPR comes into force.
- Monitor updated regulatory guidance as it becomes available, and consult a lawyer to obtain legal advice specifically applicable to your business circumstances.

The data needs to be stored on European servers so the organisation then have to comply with GDPR. You should have a 3rd party written agreement with the other organisation to confirm they are meeting the regulations and I would expect them to issue such an agreement. See google advice above – this looks like their official agreement so needs checking out.

- **What do we do with staff records, past and current?**

  Staff files must be kept for the duration of their employment + 5 years.

  However do ensure that any disciplinary records that should only be kept for 3 or 6 months are shredded once that time is over.

  Staff records have to be accurate and up to date and the employee can ask to see what data you are holding (including references) and ask for it to be corrected if it is not accurate.

  DBS are kept for as long as the person is employed.

  Anything re their pay details must be kept for the duration of their employment + 7 years in case HMRC question them.

- **How do we reconcile our obligation to keep client files/data related to current/previously funded projects until 2023 with GDPR requirements, should a client wish to have all data related to them deleted?**

  GDPR did not exist when the agreement with the funder was agreed.

  GDPR states that data should not be kept for longer than is necessary.

  GDPR over rides a funder's requirement for legal files which have to be kept for 6 years.

  However, you may wish to consider that you could claim that this would meet the legal basis for "legal requirement". You could write to the funder and explain the new requirement and explain what the new legislation requires of them. If they are really insistent then you could contact all the clients involved for their permission – but they don't have to give it and do have the right to be forgotten.

  If a client asks for their information to be changed/deleted, then it is suggested that the organisation keeps a log record that says ' A. Smith requested information be deleted in accordance with GDPR on DATE and this was complied with on DATE'. That way they are ensuring their records are up to date and they can provide evidence to the funder.

Fundraising.

- **How can we promote a giving campaign whilst being GDPR compliant?**

  Fundraising giving pages like JustGiving are updating their websites to be GDPR compliant including asking explicitly for consent (in this case it may be that JustGiving are the Data Processors, and you're the Data Controller so they need to have things in place for their own protection):

https://justgiving-charity-support.zendesk.com/hc/en-us/articles/360001292653-What-GDPR-updates-are-being-made-to-JustGiving-and-when-

The Institute of Fundraising has created a PDF which you can download and which gives advice and tips:
https://www.institute-of-fundraising.org.uk/library/gdpr-the-essentials-for-fundraising-organisations/

This article has just come out from the ICO Office which says 'consent to market to donors is not required if you are using direct mail and relying on legitimate interest':
http://fundraising.co.uk/2018/02/02/ico-gives-charities-new-reason-optimistic-gdpr/#.WtWMTH-YOpo

The charity finance group has also written this guidance:
https://www.civilsociety.co.uk/news/free-gdpr-guide-published.html

Photographs.

- **We have photographs of school children on our website, never with their name. Do I need to block them from being downloaded by our website users?**

  Photographs - Please see attached draft information sheet from Advising Communities
- **Can our use of photographs (both digital, printed and displayed) meet the new [GDPR] regulations?**

  Photographs - Please see attached draft information sheet from Advising Communities
- **how would we search for someone's data in the event of a request, particularly in regard to photographs (which might have been posted to social media years ago)?**

  Photographs - Please see attached draft information sheet from Advising Communities

Version of 01_05_18

Attachments:

1. Draft privacy notice for membership organisations
2. Draft information sheet on archives and GDPR
3. Draft information sheet on CCTV and GDPR
4. Draft information sheet on photographs and GDPR

Attachment 1: GDPR Example of permission re members

(Name of the organisation and contact details)

Privacy Notice for our membership

We need your consent by 24.5.19 to keep in touch with you. Without your consent we will have to remove you from our mailing lists and you will no longer receive information and updates from us.
You can change your mind regarding your preferences and how we contact you, or even ask for details about you to be changed or to be deleted from our mailing lists at any time.

Data Protection
You are probably aware by now that a huge change to the UK's Data Protection Laws will be implemented on the 25th of May 2018 in the form of the General Data Protection Regulation (GDPR).

Although the principles of the GDPR are similar to those under the Data Protection Act 1998, the GDPR introduces penalties and new rights for individuals and as such we need to take steps now to ensure we are compliant when it arrives.

This means we need your active consent by 24.5.18 to stay in touch with you. The consent is valid for one year and we will ask you for your consent again after that time. Without your consent we will have to remove you from our mailing lists and you will no longer receive information and updates from us.

If you consent you must tick the relevant box and let us know your preferences for how you would like to receive information, what information you would like to receive and how often.
You have an absolute right to change your preferences and withdraw your consent at any time

The information you provide in this form will be used solely for dealing with you as a member/supporter of [name of organisation].
[Name of organisation] club has a Data Privacy Policy which can be found at [??? Website perhaps??]. Your data will be stored and used in accordance with this Policy.

If you have any queries, questions or comments please contact (insert contact details of the person you wish them to contact).

Full name……
Address……
Telephone……
E mail……
Date……..

I give my consent to (Name of the organisation) to stay in touch with me for one year so that I can receive information and updates from the organisation.

Please tick the box to confirm consent ( )

I wish to receive this via email. Please tick the box ( )

I wish to receive this via mail. Please tick the box ( )

I am aware of where I can access (Name of the organisation) Data Privacy Policy

I am aware I have an absolute right to change my preferences and withdraw my consent at any time.

Signature …….

Attachment 2: GDPR – Archives

Unfortunately GDPR at this point, doesn't protect/exempt archives - although this may change with the UK Data Protection Bill coming into effect.

GDPR applies to all data held by an organisation whether current or historic. Current data tends to be online and easier to sort through however, historic or archived data can be in paper form, stored in multiple places and less easy to access.

It seems that the biggest issue for historic/archived data for an organisation is if a person exercises their right to see, amend or delete the data being held by an organisation. The GDPR provides 30 days to comply with these requests, or a person has a right to complain to the Information Commissioners Office. If data is stored in multiple places and not sorted it will be difficult for an organisation to a) retrieve the data to comply with any requests and b) be confident that they have located all the relevant data. If an organisation does not respond to a request within 30 days there may be penalties imposed by the ICO.

There are lots of recommendations for organisation to move to a cloud based storage facility for data, or to use third parties to sort/archive/store such information on behalf of the organisation. This can be costly, particularly for smaller community organisations.

We recommend the following actions:

1.Start with mapping out where your data comes from and where it is stored;

2.If your information is stored in multiple places, consider moving it to one secure filing cabinet, using online cloud storage etc;

3.Once your data is in one place, consider sorting through it to find out if the data is:

a) still active ie relating to any contracts, legitimate interests of the organisation or information which you must store for legal purposes such as employee information, gift aid,

tax etc. You'll need to file this information perhaps under categories, to make it easy to locate information

b) Redundant ie is duplicated/stored in different places - you only need one copy of up to date information. If this information applies to children, you'll need to check you have up to date consents.

c) Obsolete ie data which isn't being used/relevant, which is out of date etc and which you don't need to keep any longer.

4. Create a 'chain of custody' meaning an audit trail so that you can answer the 'who, what, where, why and when' questions. You could create this is an excel spreadsheet/hand write in a master copy which is stored securely but will make it easier and quicker to locate information to respond to any requests you might receive, and to respond to any audits/questions the ICO might undertake.

5. Clean up the data - you don't need to keep multiple copies or data which is obsolete. Check before you delete anything! But if you are deleting data you will need to ensure that it is done so securely - don't throw it away for someone else to pick it up.

Remember, if you are using volunteers or employee's to go through the data, do ensure they have read your data protection policy, have signed up to the written agreement from the data controller as a data processor and are trained in how to keep good records, and store data securely ie they can't leave data out on tables, or in public places.

Attachment 3: GDPR and CCTV Information sheet

Yes - GDPR does apply to CCTV

The usage of CCTV (Close Circuit Television) to capture images of data subjects may be for security or health and safety purposes. Identifiable imagery is considered as personal data under the GDPR and therefore, at a data protection level, requires the same level of thought and care that is being paid to other affected areas of the business.

Data protection legislation and CCTV are not new concepts under the GPDR. It was indeed included under the DPA (Data Protection Act), with the ICO (Information Commissioners Office) producing guidelines on the topic.

Data Privacy Impact Assessment

It is recommended to conduct a data privacy impact assessment to ensure you can justify processing and that you are not excessively reducing the privacy of data subjects.

GDPR does not discourage CCTV but encourages a balance

CCTV and surveillance are often emotive issues. On one hand business owners and leaders use CCTV for protection and monitoring among other reasons. On the other hand data subjects view this with an air of suspicion due to an invasion of their privacy. In either case, the GDPR does not discourage the use of CCTV but instead encourages a balance and an air clarity for all parties regarding its usage. While in the past, the concerns of data subjects may have been disregarded in favour of the overriding interests of the controller, this can no longer be the case and may prove to be the undoing of some. Whether it be scary administrative fines or embarrassment and shame, it will always be the small things which make the difference.

GDPR requires the processing of personal data to be lawful

By now, most of us are aware that the GDPR requires the processing of personal data to be lawful, fair and transparent. As CCTV collects personal data in the form of image, it is in no way immune. In almost all cases, business owners can rely on legitimate interests or the need to comply with another legal requirement for the legality of operating CCTV. However, they will be required to justify this against the area of coverage. Data subject's rights and

freedoms cannot be overridden, especially in the case of legitimate interests. Even inside a work premises, employees have a right to privacy.

Data subjects have the right to be informed

Data subjects are entitled to understand when their personal data is being processed, covering the transparency aspect of processing. It is recommended that the use of CCTV is communicated via signage which indicates the areas covered and instructions for further information.

Data retention cannot be indefinite

One of the core principles of the GDPR requires personal data to be processed for only as long as its purpose requires it to be. Each camera and its purpose will need to be assessed to determine how long footage can be retained for. For example, a retail store would not be expected to retain footage for any longer than 6 months as by that time, any reported crimes would have been detected and footage reviewed.

There are no defined acceptable retention times as it is subjective to the purpose, however be aware that years later or until the footage overwrites it, is not a good demonstration towards consideration of the data subjects rights.

Data subjects access requests of CCTV footage

As with any other aspect of personal data, data subjects have a right to access, which could result in you disclosing footage to them. Business owners / CCTV operators will need to ensure that the requester is present in the footage and that by supplying the footage they do not disclose any personal data of another data subject. This may involve blurring parts of the footage such as figures or license plates.

Can I charge an administration fee to anyone who wants to access their data on CCTV

The ICO previously recommended that subject access request of CCTV could carry an administrative fee of up to £10, however this is no longer the case under the GDPR.

Security measures such as encryption are essential

Any act of storage or access is considered processing and it is imperative that business owners or CCTV operators uphold the confidentiality and integrity of any footage. Screens displaying live or recorded footage should only ever be viewed by authorised individuals and not members of the public who stray past a security guard post or CCTV operation room.

Footage should be secured regardless of its format, for example in electronic format it should be encrypted and in physical format be locked away and tracked via a signing process.

Attachment 4: GDPR and photographs – Information Sheet

Active consent is generally required together with information on what will happen to their personal data and what rights they have.

Gaining active consent is the cornerstone of GDPR as is explaining what will happen to their personal data, and what rights they have. However photographs that can be classified a**s** **j**ournalism, literature and art are generally outside **of** GDPR.

Checklist for photos you hold or want to take

Are you aware that just promising to send a copy of a photograph to someone in return for letting you take their photograph is a contract and all the GDPR rules apply?

Before taking a photograph did you make the people present aware they have the absolute right not to be photographed?

Do you have evidence of written permission from the subject? (Active consent)

Do you have evidence of giving them and asking them to agree to your privacy statement?

Do you have evidence that you made them aware what will happen to their personal data and what it will be used for?

Do you have evidence that you made them aware of what rights they have? These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

Do you have evidence that you agreed with them how long their photo would be stored?

If someone asked to see what photos you have of them are you able to track all the photos?

If someone asked to see what photos you have of them are you able to encrypt anyone else in the photo thus respecting their right to privacy?

Be particularly aware of photographing children.

Remember issues that impact on Safeguarding

Further information at

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

One complaint from a child/parent/carer whose child's photo was shared without permission, or you sending an unsolicited email to a former client without their permission, could start an avalanche of penalties.

A child over 13 years can give active consent. For children younger than 13 it is their parents or carers who must give any written active consent.

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.(This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.