Cobseo
The Confederation of Service Charities

Data Protection Aide Memoire

Effective from: 12 February 2019
Last updated: 13 February 2019

This Cobseo Aide Memoire has been produced at the request of Members to inform the Cobseo Membership of the minimum expectations required of ***every organisation*** under the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

Please note, this is a living document that will be amended if or when the law or guidance on it changes. The most up-to-date version of this document will always be found on the Cobseo governance hub at cobseo.org.uk/governance. Feedback from document users is welcomed in order to improve the usefulness of the advice presented here. It should also be noted that this document is not a substitute for legal advice. This document is intended to assist Members to understand how to comply with data protection requirements and gives an indication of the measures Members should be achieving or aspiring to achieve to maintain a good standard of data protection within their organisations.

Similar to other Cobseo Aide Memoires, this document provides a digest of the information on data protection currently available, including regulatory advice. It lists the necessary measures organisations should have in place and seeks to communicate them in an easily understandable manner. This Aide Memoire also signposts readers to other guides, checklists and templates that can provide further details on the measures described.

This Aide Memoire deals with data protection under three main headings: lawfulness, accountability, and security. This structure has been designed to be consistent with the Information Commissioner's Office (ICO) data protection guidelines:

- An Introduction to Data Protection – the General Data Protection Regulation and Data Protection Act and why they are important to implement
- The data protection expectations:

    Lawfulness, Fairness and Transparency – the grounds on which organisations collect and use personal data and how to be fair, open and honest in data use

    Accountability and Governance – the measures that will ensure organisations are able to demonstrate compliance with the principles of data protection law

    Security – the procedures to ensure the integrity and confidentiality of personal data is upheld at an organisation and protected appropriately

- Advice, Assistance and Training – a list of the resources available to Members to help ensure good data protection standards are maintained
- Data Protection and Beyond – what changes or additions to data protection law Members can expect to see in years to come
- Contributors
- A Glossary – for explanation of the terms used within this Aide Memoire

Introduction

After a two-year transition, the General Data Protection Regulation (GDPR) came into European Union law on 25 May 2018. The 'Regulation' replaced the previous Data Protection Directive (1995) and was supplemented in the United Kingdom by a new statute, the Data Protection Act (DPA) 2018.

GDPR vs. DPA

Put simply, the DPA allows for the continued application of the GDPR legislation within the UK now and after the UK has left the European Union. The DPA also provides detail on the derogations within this legislation – the matters where the GDPR allows individual countries to decide details (e.g. setting the age for children's consent) or expand on the GDPR (e.g. on matters relating to national security or law enforcement.)

In summary, the GPDR and the DPA are a set of rules on data protection and privacy that 1; should read alongside each other, and 2; are laws that all UK organisations need to comply with.

PECR

The Privacy and Electronic Communications Regulations sits alongside the GDPR and DPA, giving individuals specific privacy rights in relation to electronic communications. This legislation will be replaced in the next year or so by a new ePrivacy Regulation (ePR).

ICO

Data protection in the UK is regulated by an independent body, the Information Commissioner's Office (ICO). The ICO can take action against any organisation that does not meet data protection standards. Read more on the types of action the ICO can take here. The ICO also provides advice to organisations, including charities, on data protection and compliance – for more, see the section on Advice, Assistance and Training in this Aide Memoire.

Data Protection

Interpretation of data protection law and guidance on it are constantly evolving. Organisations need to remain abreast of these advancements and make time to continually demonstrate data protection compliance; an undertaking that permeates all levels of an organisations.

The Principles

The GDPR defines a set of principles to adhere to in order to maintain compliance with data protection. Each principle should be considered when processing personal data. The principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation

3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Lawfulness, Fairness & Transparency

This principle sets out the grounds on which an organisation collects and uses personal data. This is known as an organisation's lawful basis. At least one of these must apply whenever you process personal data.

Lawful Bases

1. **Consent** – this offers individuals control over how their personal data is processed. Put simply, it means asking whether an individual wants an organisation to hold data on them, and if and how they want it to be used by that organisation and relevant third parties. It is important to note that consent requires a positive opt-in from an individual i.e. a pre-ticked box on a website pop out is **not** a positive opt-in. It also should be clear on how an individual can opt-out. This means that the individuals giving consent are fully informed and consent is freely given and specific. See ICO's guide on consent for more information.

2. **Contract** – if an organisation is fulfilling a contractual obligation with an individual, an organisation can use this basis for processing someone's data. However, generally, this lawful basis is not applicable to charities other than when trading.

3. **Legal Obligation –** this lawful basis is used if an organisation needs to process data to comply with the law. The organisation should be able to identify the specific legal provision that justifies their obligation to process data e.g. a charity would need to process personal data to report a serious incident report to the Charity Commission.

4. **Vital Interests** – an organisation can rely on this lawful basis if they need to process data to protect someone's life. This is likely to be relevant for emergency medical care when an individual is not capable of giving consent to their data being processed.

5. **Public Task (commonly used by public authorities) –** organisations can use public tasks as a reason for processing data if an organisation is addressing a public

interest, function or power that is set out in law. Charities are generally not eligible for this lawful basis.

6. **Legitimate Interests –** this lawful basis involves using someone's data for reasons they would expect, when balanced against the rights and freedoms of that individual. When using this as a basis, organisations should have a compelling justification for using personal data and use as little personal data as possible. An example of this would be a charity processing personal data on an individual to provide information on a service that an individual has requested.

   For more on lawful basis, click here.

Sensitive Data

There are types of data that data protection law deems more sensitive than others. Organisations should protect these data types with even greater care.

Special Category Data

This includes information on a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

As well as needing a lawful basis for processing this type of data, organisations will need to comply with Article 9 of the GDPR and the specific conditions and safeguards set out in the DPA. Organisations who process this type of data can read more here.

Criminal Offence Data

This includes personal data about criminal convictions or offences.

As well as a lawful basis for processing this type of data, organisations will need to comply with the conditions set out in the DPA. Organisations who process this type of data can read more here.

Purpose Limitation

While a lawful basis is an organisation's grounds for processing data, purpose limitation involves an organisation only using personal data for a specific purpose. This purpose must be made clear to individuals when the data is collected.

For example; if an organisation collects a beneficiary's phone number to contact them about an appointment (on the grounds of the legitimate interests of providing the service that the individual is seeking), that organisation cannot use that number any further to, for instance, promote other services provided by the charity.

Data Minimisation

Organisations must ensure that personal data being processed is adequate, relevant and limited to what is necessary. This is so that it fulfils the purpose for which it is needed. Organisations **must** not hold any more data than is necessary.

Individual Rights

The GDPR and DPA legislation gives more control to individuals. Part of this is achieved through the following eight individual rights:

Right to be Informed* – this gives individuals the right to know how their personal data is being used. This should be shared with the individual at the time of data collection in a privacy policy (more on this later).

Right of Access* – this is sometimes referred to as a subject access request. It is a right that allows individuals to be given the personal data an organisation holds on them. This is subject to certain conditions. Read more here.

Right to Rectification* – to have inaccurate personal data rectified or completed if it is incomplete.

Right to Erasure* – also known as the right to be forgotten where an individual can ask for their personal data to be removed from an organisation's records. This right is also subject to certain conditions. Read more here.

Right to Restrict Processing* – this is the right to restrict an organisation processing personal data in certain circumstances. Read more here.

Right to Data Portability* – this allows individuals to transport personal data, they have submitted, from one IT system to another in a safe way that will not affect usability. This only relates to data that can be automatically read and processed by a computer.

Right to Object* – this is the right for an individual to ask organisations to stop processing their personal data including for direct marketing.

Rights Related to Automated Decision Making, including Profiling – this relates to Article 22 of the GDPR, and profiling, in the charity sector, often involves the automated processing of personal data to evaluate certain things about a charity's donor, for example. Read more here.

*These requests can be made verbally or in writing to any part of your organisation (including through social media channels). Organisations have one month to respond to these requests.

In all cases, organisations should explain these rights in privacy notices to individuals.

Privacy Notices

A privacy notice (or statement) is a public document that explains how an individual's data is collected and used. An organisation's privacy notice should be made available to the individuals who the organisation is collecting data from and made specific to the needs of the organisation. It must be provided upon collection of data and before any consent is sought. A privacy notice should be written clearly and in a concise way. For what to include within a privacy notice, see here for ICO's privacy notice checklist. Alternatively, University College London have further guidance on how to write a privacy notice with a free, downloadable example.

Children

Organisations should consider what lawful basis they have for processing data on children. If organisations are dealing with children under 13, they need to obtain consent from the child's parent or legal guardian unless the service that organisation is providing is a preventive or counselling service to children.

It should also be made clear to children how and why organisations are collecting their data. Organisations should consider how this may be communicated in a privacy policy – the language of a privacy notice addressed to adults will be notably different from one that is communicated to the under 13 age group. Organisations might find the National Society for the Prevention of Cruelty to Children's (NSPCC) privacy policy useful in determining what content, and how it is written/presented, should be included within a privacy notice by an organisation that processes data from children.

Organisations who process data on behalf of children under 13 should consider what happens when a child reaches the age of 13 in terms of consent. Individuals who are 13 years old and over have the same data protection rights as an adult, including individual rights. How this is communicated in a privacy notice should be considered.

Direct Marketing

Direct marketing is the communication of advertising material directly to individuals through a variety of different media, for example, through email, text or even online advert.

For charities, direct marketing is commonly used as a fundraising method. Both the ICO and the Fundraising Regulator have various advice and support for organisations on using direct marketing relating to fundraising – for this guidance, see the Advice, Assistance and Training section.

The Fundraising Preference Service gives individuals control over what direct marketing they receive from registered fundraising organisations and allows individuals to withdraw their consent from having their personal data processed. The Fundraising Regulator will process an individual's request and give the relevant charity 21 days (from 1 March 2019) to remove the individual from its direct marketing lists. Failure to comply with a request is a breach of

the Fundraising Code and might see the Fundraising Regulator inform the Charity Commission and/or ICO of a charity's failure to comply.

As mentioned, the Privacy and Electronic Communications Regulations, also known as PECR, will be replaced by an ePrivacy Regulation (ePR) in 2019 or 2020. In the meantime, charities should continue to apply the electronic communication regulations as listed in PECR. ePR will impact how charities, particularly those who fundraise, use direct marketing.

Accountability & Governance

The previous section addressed how organisations should collect and use data appropriately. This part of the Aide Memoire explains how organisations are accountable for these methods and how these should be upheld within an organisation's activities.

Data Protection Officers (DPO)

A data protection officer (DPO) advises on data protection at an organisation and the appropriate measures required. DPOs report directly to a charity's board and will be the main contact for colleagues and the ICO when it comes to data protection. Therefore, DPOs should be experts in the field and, when appointing a DPO, organisations must ensure that whoever they recruit into this role has no conflicts of interests. A sample job description for a DPO can be found here.

Although not all organisations are required by law to appoint a DPO, every organisation should have someone working for them that is responsible for the organisation's data protection. This person should be in a position of authority and have an understanding of the organisation's processes. This person will be main contact for colleagues and the ICO when it comes to data protection.

Find out if an organisation requires a DPO by taking the ICO's 5-minute quiz.

Note: if an organisation does not need a DPO but hires one to further demonstrate their compliance, that DPO **will** be required to undertake the same responsibilities of a DPO at an organisation where appointing a DPO is mandatory.

Data Protection by Design and Default

Data protection by design and default is essentially a risk-based approach to data protection. Organisations need to prioritise data protection and think about the potential risks for both the organisation and individuals when processing data. Organisations need to consider the necessary measures to reduce risk at the design stage of their activities and practices. This enables organisations to build-in data protection into all aspects of their operations.

This type of approach is explained within Kingston Smith's article on data protection by design.

An example of a risk-based approach to data protection would be considering how to cope with subject access or deletion requests *before* setting up a new a database.

A data protection impact assessment (DPIA) should be completed when embarking on any new project or process considered high-risk to individuals. This is now a legal requirement of organisations. More on DPIAs can be found here and a sample DPIA template can be found here.

Documentation

Under Article 30 of the GDPR, the ICO can request records on an organisation's data processing activities. To stay compliant, organisations should keep electronic and up to date records of the following:

- The name and contact details of the organisation (and where applicable, of other controllers, the representative and the data protection officer) – see definitions of these roles on the next page.
- The purposes of processing data.
- A description of the categories of individuals and categories of personal data processed.
- The categories of recipients of personal data.
- Details of transfers to third countries including documenting the transfer safeguards mechanisms in place.
- Retention schedules.
- A description of technical and organisational security measures.

For more information on this requirement, including templates to help organisation's document their processing activities, click here.

Accuracy

Organisations should be clear on how they ensure that the personal data they hold is not misleading or incorrect in any way. Any personal data held by an organisation should be kept up to date, and if a piece of data is either misleading or incorrect, an organisation should be clear on how they plan to correct it or erase it.

As outlined above, these steps should be recorded within an organisation's documentation.

Storage Limitation and Data Retention

These terms are used interchangeably to refer to the time frame in which an organisation stores personal data. The requirement of organisations is simply to be able to justify that period in their documentation.

As mentioned previously in this document, personal data should only be retained for the original stated purpose.

Data Controller vs. Data Processor

> **Data controller** – is usually an organisation that determines the purpose for how personal data is processed and is legally responsible for compliance with data protection law.
>
> **Data processor** – is likely to be a member of staff, within or external to a charitable organisation, that processes the data on behalf of the data controller.
>
> A contract with between the data controller and the data processor is a legal requirement designed to ensure compliance with data protection law.

For more on the responsibilities of data controllers and/or data processors, click here.

Trustee Accountability

While the DPO (or relevant person) handles the routine data protection, Trustees are ultimately responsible for a charity's compliance with the law. The Charity Commission recommends charities have a dedicated Trustee to take accountability of their data protection compliance. This Trustee should have no conflicts of interests i.e. they should not partake in the day to day management of data processing activities.

Security

This section considers the necessary measures to ensure the personal data stored or processed at an organisation is done so securely and guarantees the safety of that data.

Implementation of Data Protection

Implementation of data protection should also cover the physical IT infrastructures and operational processes at an organisation. This should be backed up by regular data protection training of staff to ensure that the culture of data protection permeates an organisation from Trustees to volunteers.

Passwords

Organisations are expected to process data through appropriate technical measures e.g. password systems and, perhaps, a supporting two-factor authentication. The latter usually includes a password and a one-time token generator.

Advice on password storage and what makes a good password can be found here.

Encryption

Encryption is the process of turning a file into coded data, so that if that data file is discovered by someone that should not have access to it, the file is unintelligible to read. This process is usually paired with an encryption key (put simply, a password) which then unscrambles the coded data to make it legible to an authorised body. It is usually an effective method to use when transferring data, but only when within the UK. Different measures should be in place for international transfers of data – see more below.

Encryption is another technical measure used to protect personal data, however this element refers to Article 32 of the GDPR and requires an organisation to produce an encryption policy to govern how and why it will be used. This policy should be made available to staff through training. For more on encryption, click here.

Cyber Security

Cyber security within data protection consists of technologies, processes and/or controls that are designed to protect data being hacked, damaged or destroyed – also known as a cyber attack.

To ensure basic technical controls, organisations can use established frameworks like the government scheme, Cyber Essentials to guard stored data against common cyber threats.

Please note, the technical controls required at an organisation will depend on its processing activities – see the Cyber Essentials scheme for more.

Additionally, the National Cyber Security Centre has useful guidance, particularly for smaller charities, on Cyber Security.

International Transfers

The GDPR upholds a standard of data protection inside the European Union and European Economic Area. Transferring and processing data outside these areas is sometimes known as a restricted transfer. The security of personal data should be considered by organisations when it is transferred internationally. The ICO have produced a list of considerations for organisations who are required to make such a transfer.

Personal Data Breaches

Personal data breaches should, in certain circumstances, be reported by organisations to the ICO within 72 hours of the organisation becoming aware of a breach. This is a legal obligation. Any individuals whose personal data held at an organisation that might be adversely affected by this breach should also be informed. A personal data breach report form can be found here.

A record of breaches and a strategy of how to detect and alert the ICO and individuals affected about a breach should be kept.

Advice, Assistance & Training

The following information provides a list of guidance and courses on data protection that is specific to the third sector and provided by reputable sources known to Cobseo.

Regulatory guidance and training

The ICO hold the GDPR and the DPA guidance on their website. They also have a useful self-assessment tool on data protection available for all organisations. For charities, see the ICO's FAQs for charities. The ICO also have a variety of training videos available that help digest the code and guidance on the GDPR and DPA.

ICO's guidance on direct marketing is available here. A condensed version of this guidance can be found in the ICO's direct marketing checklist, for organisations who wish to self-assess how compliant they are with data protection standards of direct marketing.

As mentioned, the ICO's guide to Privacy and Electronic Communications Regulations (PECR) is being revised but is still relevant for organisations today.

For those organisations who fundraise as an active part of their activity, see the Fundraising Regulator's resource library on data protection.

Free resources

See also the NCVO website for data protection support and their blogs on how to prepare data protection at an organisation.

Knowhow Nonprofit also have a variety of free online guidance on data protection that might be of some use to organisations.

Regional guidance

The Northern Ireland Council for Voluntary Action's (NICVA) data protection toolkit was based on the NICVA's experience in delivering training and answering enquiries from small charitable organisations in Northern Ireland.

The Wales Council for Voluntary Action (WCVA) also have a wide range of advice and guidance on the GDPR and data protection. See also their resources produced for third sector organisations in Wales that include information sheets and short films.

Legal guidance for the charity sector

Kingston Smith have written an informative article into the positives of data protection for not for profit organisations.

Data Protection & Beyond

While the GDPR and DPA may have increased the governance work required of organisations when it comes to data protection, these laws have also shed light into how to protect personal data in order to help build public trust.

It should be noted that advancements to data protection law are coming, and it is important to stay abreast of the Privacy and Electronic Communications Regulations (PECR); replacement legislation is expected in 2020. Protecture provides a useful summary of what ePrivacy law will mean to organisations in years to come.

Contributors

The Cobseo Governance Support team would like to thank all the people and organisations who have contributed to the production and review of the Cobseo Data Protection Aide Memoire to date. These include:

- ABF The Soldiers' Charity
- Greenwoods GRM LLP
- Officers' Association
- Protecture

Glossary

The following list define some of the terms listed in this Aide Memoire.

1. **Cookies** - data sent from an organisation's website to a user's computer to track the user's visits and activity on the organisation's webpages
2. **Cyber Security** – a set of controls designed to protect data from being hacked (from a cyber attack)
3. **Data Controller** – determines the purpose for which and how personal data is processed and is legally responsible for compliance with data protection law
4. **Data Processor** – someone who processes data on behalf of the data controller
5. **Data Protection Impact Assessment (DPIA)** – a way to identify potential risks to personal data when embarking upon a new process or project

6. **Data Protection Officer (DPO)** – someone who is the main point of contact for the organisation's and ICO's data protection queries and advises on an organisation's compliance with data protection
7. **Direct Marketing** – the communication of advertising material directly to individuals through a variety of different media, for example, through email, text or even online advert
8. **Lawful basis** – an organisation's grounds for collecting and storing personal data
9. **Purpose limitation** – an organisation can only use personal data for a specific purpose and this purpose must be made clear to individuals before their data is collected
10. **Personal data** – information used to identify a living individual
11. **Privacy notice** – a notice, or statement, that is publicly available which states an organisation's reasoning for collecting and using personal data, and how it is stored i.e. for what time frame and how it is safeguarded
12. **Processing (personal data)** – is how personal data is stored, updated, destroyed and/or used by an organisation
13. **Restricted transfer** – the transfer to and process of data outside the European Union and European Economic Area

Cobseo – The Confederation of Service Charities
2nd Floor
Mountbarrow House
6-20 Elizabeth Street
London SW1W 9RB

0207 811 3225
enquiries@cobseo.org.uk
www.cobseo.org.uk