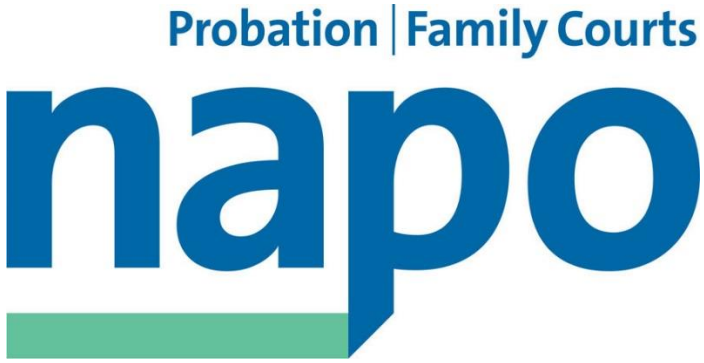

Data Protection Guide

Version Control

Version	Date	Review Date	Reviewed By
1.0	June 2018	June 2019	Office Manager

Foreword

Data protection law in the UK and Europe is being strengthened through the Data Protection Act 2018 / General Data Protection Regulation (GDPR). This makes it even more important, for Napo and our members, that privacy is integrated into our day to day work. The increasing profile of the importance of protecting personal data means that the public at large, and so also our current and potential members, are more conscious of it. We cannot afford data protection to be an afterthought.

This guide is intended for use by

- Napo staff
- National Officers
- Branches
- Committees
- Local Representatives
- National Representatives

As such, this guide has been designed to give everyone an appreciation of the legal requirements that Napo must abide by to ensure that they comply with all UK and European Data Protection Regulations.

The content of this handbook is correct at the time that it was issued and will be updated from time to time as privacy legislation changes or internal processes are updated.

1. Introduction to Data Protection

1.1 Data Protection Laws

At the time of writing Napo must comply with:

- Data Protection Act 2018
- General Data Protection Regulation
- Privacy and Electronic Communication Regulations 2003 (PECR)

This guide aims to take the key points from each law and put them into a Napo context.

For clarity, in this document, the terms “GDPR”, “Data Protection” and “Data Protection Regulations” will be used. These terms should be taken to include all of the above regulations that are applicable.

1.2 Data Protection Basics

All organisations in the UK must comply with the current Data Protection Regulations.

Data protection is enforced in the UK by the Information Commissioner’s Office (ICO). The ICO has a number of powers, including the ability to fine organisations up to €20,000,000 or 4% of annual turnover (whichever is the greater) per data protection breach and the ability to publicise information about data protection breaches.

Data protection applies to the “processing” of “personal data” by “data controllers” and “data processors” about “data subjects”.

1.2.1 Personal data

is any information about a living individual which enables them to be identified. If data is “obviously about” a person, then it is personal data. Examples of personal data potentially processed by Napo are:

- Membership number
- Date of birth
- National insurance number
- Bank details
- Email address
- Home address
- Case files
- IP address

Records of opinions about an individual, or intentions towards them, are also classed as personal data.

Personal data can be held in any form. This could be on electronic media (such as USB sticks, CDs, computer drives and cloud computing) or hard copy files.

The majority of data Napo holds on members is personal data

1.2.2 Processing
includes:

- Obtaining and retrieving information.
- Holding and storing information, including in the membership system, and on paper.
- Making information available to others, within or outside an organisation.
- Printing, sorting, matching, comparing, altering and destroying information.

Everything Napo does with personal data is considered to be "processing"

A **Data Controller** determines how personal data will be used.

Napo is the data controller for all personal data that we have

A **Data Processor** is a body which processes information on behalf of a data controller.

For example, Sage Publishing who distribute the Probation Journal, are data processors

1.2.3 Data subjects are the individuals whose personal data we hold. They include:

- Members
- Lapsed members
- Prospective members
- Employees
- Previous employees
- Prospective employees
- Agency staff
- Contractors
- Suppliers

All of the membership related work which is carried out by Napo must be done in line with GDPR

Data Protection is about striking a balance between the rights of individuals to know about and control what's happening to their personal data and the sometimes competing interests of those with legitimate reasons for using their personal data.

2. The Six Principles of Data Protection

GDPR focuses on six principles which stipulate that:

1. Personal data shall be processed fairly and lawfully and in a transparent manner.

2. Personal data shall be collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with that purpose.

3. Personal data shall be adequate, relevant and not excessive for the purpose of the processing.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data shall not be kept for longer than is necessary for the purposes of the data processing.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.

2.1 Principle 1
Personal data shall be processed fairly and lawfully and in a transparent manner

There are six “fair processing” conditions for using individuals’ personal data, and Napo needs to comply with at least one of them to ensure that data is being fairly and lawfully processed. The key conditions which Napo relies on are:

- The individual has given their consent for their personal data to be used by the organisation.
- The processing is necessary to pursue Napo’s legitimate interests as a trade union (in a way that will not cause unwarranted damage or distress to the individual).

To ensure transparency, Napo must communicate to members how we will process their personal data. This involves:

- Publishing a privacy statement that explains how Napo processes personal data. This is available from the home page of the Napo website.
- Explaining to members what we will use their personal data for whenever we collect it. This could be explaining that we need to update their address details to send them a ballot paper, or explaining that the information they provide on a case form will be used to represent them.

“Special categories” of personal data and further conditions for processing

Some personal data is classed as “special category” or “sensitive” under GDPR. This data includes information relating to an individual’s:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual orientation

To be able to use special category personal data there are further conditions (additional to those highlighted above) which Napo must meet. The most common are:

- The person involved has given explicit consent for the data to be used.
- Data is processed in the course of Napo's legitimate activities, with appropriate safeguards, for trade union aims.
- The data is used to obtain legal advice or defend legal rights.
- Data on race, religion or health is used for equalities purposes.

The misuse of special category data, including information about trade union membership, can cause damage and distress for the individuals concerned. Extra care must therefore be taken when handling these categories of data.

2.2 Principle 2

Personal data shall be collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with that purpose

To legally process personal data, Napo must be listed on the publicly available register which is maintained by the ICO. The process of registering is known as "notification".

Under GDPR, branches are covered by Napo's registration and so **do not need to notify separately**.

Notifications identify several "purposes" for processing data, and these are the only activities that Napo is legally allowed to collect and use data for. Napo's registered purposes include:

- Processing membership data
- Processing potential membership data
- Processing staff data

2.3 Principle 3

Personal data shall be adequate, relevant and not excessive for the purpose of the processing

This principle is about making sure that Napo does not collect more information than we need to.

Never ask a member for information that Napo does not need.

2.4 Principle 4
Personal data shall be accurate and where necessary, kept up to date

This principle requires Napo to keep personal data up to date and accurate.

Please note – the details here are will be subject to further change.

The key to accuracy is the use of one single membership system (currently Sodalitas). This is because membership data updates can be done from different parts of Napo, for example:

- Member updates their own details via their profile on the Napo website.
- Member updates their details over the phone to Napo Membership.
- Postal mailings to the member are returned to Napo Membership.

We therefore all need to use the same membership system and not rely on separate lists.

Napo should not keep membership data on any system other than Sodalitas, or use separate lists of data

2.5 Principle 5
Personal data shall not be kept for longer than is necessary for the purposes of the data processing

GDPR stipulates that personal data should not be kept longer than is necessary for the purpose it was collected. The ICO expects organisations like Napo to have a data retention schedule which identifies the different types of information in use and how long that information should be kept.

GDPR does not set specific times for which data should be kept; -organisations are expected to consider their own retention needs. However, there are some legal retention periods e.g. case files should be kept for at least 6 years. Other documents like membership forms only need to be kept for a year after all the relevant data has been entered onto Sodalitas.

Napo's retention schedule is as follows:

- Employees
    - 6 years from termination of employment.
- Job applicants
    - Data of unsuccessful job applicants is kept for 12 months
- Contractors and volunteers
    - for as long as the contractor or volunteer is currently contracted
- Members, officials and activists
    - All information (updated as appropriate) will be kept throughout an individual's time as a member and for such reasonable period (and to the extent necessary) after membership as may be needed to enable the member to access any post-membership benefits. Typically this would be 10 years from the date of retirement. This is to ensure that the

members information is available should a pension dispute arise after retirement - the time limit on this being 10 years from the date of retirement. When membership of Napo ceases membership will no longer be active and not available for access unless there is a specific written request from the member.

.

2.6 Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data

Data Protection requires organisations to keep personal data (whether it be in hard copy or electronic form) secure against accidental loss, damage or destruction.

For **electronic data** e.g. that held on computers, cloud computing or removable media, (USB pens, CDs, etc) the ICO would expect to see:

- Password protection
- Encryption
- Virus protection
- Use of firewalls
- Data backup processes

For **hard copy data** examples of good data security practices are:

- Door security and restricted access to branch offices
- Lockable filing cabinets
- Secure storage areas
- Clear desk policies

Secure use of email

Some branches use their employer's email system, whereas some use email providers such as Hotmail and Gmail. Whatever email system you use, ensure it is as secure as possible by doing the following:

- Have a strong password.
- Lock your screen when away from your desk (Shortcut - Windows key +L).
- Always sign out of your email account when finished if you are using a shared device.
- Ensure that no one else has access to your emails. Never use a family or shared email account for Napo business.
- If emailing more than one person, use the Bcc field rather than the To or Cc field (NB using Sodalitas bulk email does this automatically).

Secure archiving

Napo is responsible for the security of any archived files. Any branches, local or national representatives that hold files locally must also ensure that the archived files are secure. For advice on how to check your archive is secure, please contact Napo HQ.

3. Rights of the Data Subject

Individuals have several rights under GDPR. The following are most relevant to Napo branches:

3.1 Right of access

Individuals have the right to be provided with a copy of their own personal data held by Napo. These requests are called subject access requests (SARs). They cover information held in paper form and electronically.

Never write down anything about an individual that you would not want them to see

Napo can apply exemptions to withhold certain data. For example, legally privileged information between Napo and its legal advisors does not need to be disclosed. Exemptions are applied on a case by case basis.

If an individual makes a subject access request, please contact Napo HQ immediately. We must reply within one month, so time is of the essence!

3.2 Right to restrict processing

Anyone can request that a data controller, such as Napo, stops processing their personal data. In practice, we may just stop doing whatever the person is specifically objecting to (e.g. sending mailings).

If a member asks Napo to stop processing their personal data completely, that person would no longer be able to be a member, and if a potential member requests this, then they could not go on to become a member of Napo.

If a member asks you to stop processing their personal data, please contact Napo HQ immediately.

3.3 Right to erasure

An individual has the right to ask Napo to delete their data, if there is no compelling reason for us to keep it. There are circumstances in which we can refuse to delete data (e.g. an ongoing legal case), and we also need to consider our data retention requirements (see section 2.5).

If a member asks you for their personal data to be deleted or destroyed, please contact Napo HQ immediately. Do not start deleting anything until you have heard back from us.

3.4 Right to rectification

An individual can ask Napo to rectify their data if it is inaccurate or incomplete.

If a member asks you to do this, contact Napo HQ or advise them to update their own details online via their Profile on the Napo website, or to email membership@napo.org.uk.

3.5 Right to data portability

GDPR allows individuals to obtain and reuse their personal data for their own purposes across different services. For Napo this is likely to take the form of a request for an individual's details to be passed to another union that they wish to join.

If a member asks you for this data, please contact Napo HQ immediately.

3.6 Right to object to processing

a) Right to opt out of direct marketing
These requests must be acted upon immediately and no further direct marketing material sent to the individual. The ICO defines "direct marketing" broadly – it includes the promotion of an organisation's aims, values and policies. This presents some challenges when we want to contact members with regard to campaigning issues.

If a member asks to stop receiving marketing, you should contact Napo HQ immediately.

b) Right to object to other types of processing
An individual can object to any processing where Napo's lawful basis is legitimate interest (this covers most of our processing). If a member does this, please contact Napo HQ immediately.

3.7 The right to complain to the regulator (the ICO)

If someone believes their personal data has not been processed in accordance with GDPR, they can ask the ICO to make an assessment.

If GDPR is found to have been breached and the matter cannot be settled informally, the ICO could take action against Napo which could be a fine of up to €20,000,000 or 4% of annual turnover (whichever is the greater).

3.8 The right to compensation

An individual can claim compensation from a data controller for damage and distress caused by a breach of GDPR. Compensation for damage (i.e. financial loss) is regularly awarded by the courts. Compensation for distress only is less common, but has been awarded in certain circumstances.

4. International Data Transfers

4.1 Transferring data outside of the European Union

Data Protection Regulation states that data is not allowed to be transferred outside of the European Union ("EU") unless that country is designated as having "an adequate level of protection", or other safeguards are in place.

Napo does not transfer data outside of the UK.

5. Privacy and Electronic Communications Regulations 2003 (PECR)

The Privacy and Electronic Communications Regulations 2003 ("PECR") are specifically about electronic direct marketing communications.

Examples of "electronic communications" are: email, direct messages on social media, text message, fax and automated telephone calls.

"Direct marketing" is defined very broadly and includes the promotion of an organisation's aims, values and policies. A large proportion of Napo's electronic communications are therefore direct marketing, even though we are not trying to sell a product.

The key requirement of the PECR is that individuals contacted electronically must have given their prior consent for this communication, other than in very limited circumstances.

PECR does not consider that contacting people as a default unless they have opted out is satisfactory. They look for evidence that individuals have given their explicit consent before any communications take place. This can make contacting potential members and members tricky when it comes to information which is about educational and campaigning matters.

Opt-out consent is only acceptable when **all** of the following three criteria are met:

1. The contact details were obtained from the individual during a sale of a product or service. For Napo this will usually be when a person is becoming a member, or we are contacting an existing member; and

2. The communication relates to similar products or services. For Napo this will usually be a communication about a campaign; and

3. The option to opt out (or "unsubscribe") was provided when the data was collected and is included on each and every subsequent communication. For Napo this means always ensuring there is an unsubscribe option on all electronic communications.

The conditions are very specific and so cannot be relied upon in many situations.

It is therefore very important to know why the personal data that you have was collected in the first place.

6. Freedom of Information Act 2000

Napo, although a trade union for public service workers, is not itself a public body. The Freedom of Information Act 2000 ("FOI Act") only applies to public bodies. Any FOI requests should be directed to Napo HQ for review and response – the standard response is that the FOI Act does not apply to Napo and therefore the information will not be provided.

Subject access requests (SARs) often incorrectly refer to the Freedom of Information Act. SARs must be responded to by Napo within short deadlines or face large penalties. It is therefore important to recognise and respond to them quickly.

7. Napo Activities

7.1 Data processing

All of the tasks below are data processing and must follow GDPR:

- Receiving and inputting membership forms
- Amending or deleting membership details
- Running reports
- Sending bulk emails

When completing any of these activities:

- Do use Sodalitas for all of these tasks, as it is the easiest and most secure way.
- Do update member records as soon as possible.
- Do lock your computer screen when you are away from your desk.
- Do shred any membership information when it is no longer required.
- Don't let someone else use your login.
- Don't leave paper copies of membership details on your desk.

Sodalitas significantly reduces the risk of data protection breaches occurring and should be used whenever possible. It is a secure system, accessible only by authorised persons. It also records all changes made to membership data, maintaining the accuracy of the information.

7.2 Collecting potential member information

Potential members' personal data can be collected as long as the people are aware their data is being recorded and retained, and they must be allowed to opt out of this data collection exercise. It is imperative that the data collected about potential members is not excessive – avoid collecting more information than is needed – and that it is stored securely and not shared with anyone who has no need to see it.

A retention period should be set for this information and, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer or shredded or placed in a confidential waste bin or bag if it is in paper form.

7.3 Data cleansing

This is a crucial branch activity, especially in the run up to a ballot. If a member requests that their personal details are updated, this should be done via Napo HQ as soon as possible.

It is important to ensure that in the process of collecting updated member data, this data is not inadvertently shared with others. This would breach GDPR and could give cause for members to complain to the ICO. It is important to ensure that any method of data collection always maintains everyone's confidentiality. For example, do not openly circulate a spreadsheet which contains a line of information for each member; instead, send individual update sheets to individual members. Similarly, do not send out a blanket email to members without using the "blind carbon copy" (Bcc) field – some members wish to keep their membership confidential.

7.4 Storing data securely

7.4.1 Hard copies, file notes, incoming and outgoing letter correspondence

Napo has a duty to ensure that data is held securely. Provisions that must be considered putting in place include:

- Lockable filing cabinets
- Security keypad on the door of the office
- A file logging out and in procedure
- A clear desk policy
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin, for example.

7.4.2 Electronic data

The same requirement applies to electronically held data. Provisions that must be considered putting in place include:

- A logging process for laptop removal from the office.
- Using storage on a network, rather than laptop or desktop computer, if possible
- Encryption of all removable media (USB pens, CDs etc). If you use employer-provided computers it is likely that these will have some form of encryption installed.
- Password protection on all files containing member data.
- Use of Sodalitas for processing member data (encrypted and password protected).
- Up to date antivirus and malware systems.
- Adequate firewalls.
- Secure destruction.

It is important that when a computer is no longer required, that any data is removed in such a way that it is not recoverable. There are several organisations that will forensically clean a computer hard drive and provide a data destruction certificate to prove that it has been done.

7.5 Sharing information

Personal data should not be shared with third parties unless cleared by Napo HQ.

7.6 Using an external print/processing house

When data is passed to third parties for processing, the ICO requires organisations to choose a third party which will provide sufficient security guarantees for both its use and storage. It doesn't matter whether the information is electronic or hard copy. Examples of third party processors are:

- Mailing houses
- Website hosting
- Napo staff payroll providers

It is essential that a formal agreement is in place with third party processing organisations. The agreement should ensure that there is a contractual obligation on the processor to:

- Implement specific security measures.
- Use the data only for the original purpose they received it.
- Have trained personnel.
- Disallow further subcontracting.
- Grant rights of access for audit and subject access purposes.
- Delete data within an agreed retention schedule or when a subject has requested Napo delete their data.

7.7 Extracts from the membership system

If any data extracts are taken from Sodalitas, it is essential that appropriate permissions and security are in place. We need to ensure that the information is:

- Passed to the receiver securely (for example using encryption, password protection or secure FTP which encrypts the file for you).
- Not circulated widely.
- Given only to those individuals who have a need to see the data.
- Only used for the specific purpose for which it was extracted.
- Held securely.
- Securely destroyed after use.

The importance of thinking before sending extracts from Sodalitas (or any other personal data to a third party) cannot be overstated. Consider what you are doing it for and check that doing it will not breach data protection law.

Below is a table of 'dos and don'ts' which you should bear in mind when extracting information from Sodalitas:

Do
Only extract the information that is needed to complete a task. This makes sure that the data is not excessive.
Only use extracts for one task. A new list should be extracted for each task as the data may have changed.
Keep the information on systems and networks that are recognised as being acceptable for Napo work. These may belong to an employer or to the union.
Take care when taking personal data out of the office. Only take the information if it is necessary, keep it safe and return it as soon as possible.
Update Sodalitas if a member's details are out of date.
Use Sodalitas for all membership data work.

Don't
Extract more information than you need for a task. A lack of time is not a legitimate reason for not producing tailored reports.
Provide information to others not involved in the task for which the data was extracted.
Keep the information that you have got to use for a very similar exercise that you know you're going to do in the future.
Leave personal data that has been taken out of the office unattended.
Put information into a normal bin, use a secure disposal bin or bag instead. Someone else could find it and misuse it. Preferably shred it.
Have a local member list or spreadsheet instead of using Sodalitas.

7.8 Releasing information to prevent or detect crime

The police or other crime prevention / law enforcement agencies (e.g. Benefit Fraud Office and Local Authority functions) sometimes contact data controllers or data processors and request that personal data is disclosed in order to help them prevent or detect a crime. Napo does not have to comply with these requests, but GDPR does allow organisations to release the information if they decide it is appropriate.

Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This includes considering:

- The impact on the privacy of the individual/s concerned.
- Any duty of confidentiality owed to the individual/s.

- Whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender.

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for Napo to release the information.

If such a request is received then please refer the requestor to Napo HQ.

7.9 Communicating with members

As is explained in the PECR section this guide, contacting members by email or text message requires opt-in consent.

7.9.1 Using email and text messaging

As well as the conditions relating to PECR, the ICO has stated that all email addresses are personal data, and as Napo is a trade union, email addresses are sensitive personal data, requiring extra conditions to be met before the data can legally be used. It is therefore essential that when communicating with members using email and text distribution lists that the following provisions are made:

- Individuals who have opted out of mailings (apart from statutory information like ballots information) are not included in mailings or bulk text messages. Sodalitas bulk email will do this for you.
- The blind carbon copy (Bcc) field on the email address line is used. Sodalitas bulk email will do this for you.
- An option to unsubscribe to similar communications is added to the bottom of the email or text message each time a message is sent out.

If a member informs Napo that they no longer wish to be contacted via email or text, their preferences should be updated on Sodalitas. They should also be removed from any distribution lists we have.

It is best to use Sodalitas to send bulk emails as the following security features are included within it:

- Lapsed members not emailed.
- Bulk emails are automatically sent using Bcc.
- Changes to member contact preferences are immediately reflected.
- Communications are recorded to member's communications history.
- Avoids the need for membership extracts or lists.

7.9.2 Sending letters to members

Some members wish their trade union membership to be confidential and request that any union related mailings are sent to their home address, rather than their workplace address. Napo must ensure that these requests are complied with. Inadvertent disclosure of an individual's trade union membership would be a breach of GDPR.

7.10 Representing members

7.10.1 Employment, welfare, and health & safety case files

Any information directly related to a potential or actual case is extremely sensitive and several of the Data Protection principles apply. Provisions that Napo need to make include:

- Secure storage for live and archived case files.
- Limited access to only those officials/staff who need to see the data.
- Collection of data is limited to only that which is relevant to the case in hand.
- Information held in the file is accurate.
- A sign in/out process is in place, if the file needs to be taken out of the office.
- A file retention policy is in place.
- Secure disposal once the file is no longer needed.

It is much safer to keep any case files within the office. If this is not possible, i.e. a file needs to be taken off the premises, considerable care should be taken to ensure that its whereabouts are known, and that it is always kept secure.

In order to preserve the legal privilege that exists between Napo and its legal advisors - Thompsons – for legal advice that is sought regarding a merits assessment for a particular case, the original documentation between Napo and the legal advisors should not be copied in full to the member. This information should be summarised before passing it to the member – this serves to protect Napo's interests in the longer term.

8. Subject Access Request (SAR)

An individual has a right to request access to all the personal data that an organisation holds about them. They also have a right to know the source of the data, the purposes that it is being held for and who it has been shared with. The individual must make the request in writing by letter or email.

Individuals requesting an SAR do not need to provide a processing fee unless the request is "unfounded, excessive or repetitive" or the request is for further copies of information already provided. The individual must provide some form of identification so that we ensure we are providing data to the right person.

By law, Napo must respond to subject access requests within one month.

Data we need to provide can include:

- Details held on Sodalitas, including notes.
- Case files including handwritten notes, emails, letters etc.
- Complaint files

The scope of the search can include Napo HQ, branches, and any other organisation which is processing data on Napo's behalf.

It is important to note that email exchanges between Napo staff, National Officers, branch officials, and representatives with reference to a member may have to be considered for disclosure in response to a SAR. So please:

- Keep any documented information factual.
- Carry out periodic housekeeping on email and other information sources.
- Keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document).
- Only copy into emails those people who “need to know”.
- Do not use abusive or derogatory language in emails or other documents.
- Do not include any personal opinions in email or other documents.
- Do not use email when a telephone call will do.

8.1 What to do if a request for subject access arrives at the branch

If the branch receives an SAR it is important to immediately forward it to the Data Protection Officer at Napo HQ otherwise time could be lost and so fewer days available to complete the response to the request. SARs must be responded to by Napo within short deadlines or face large penalties. It is therefore important to recognise and respond to them quickly.

The branch should be prepared (but not begin) to gather all their relevant documents, including emails, as Napo HQ will soon be in contact asking for it. It is important to provide all the relevant documents, even if some are thought to be contentious.

Napo HQ will review all data before it is passed to the individual, and will either redact, withhold or provide the data in response to the SAR. Flag any documents which you consider to be contentious or sensitive in some way. Please explain why you are concerned about them being released. This will help inform the response to the SAR, but does not necessarily mean that the information will be withheld. Information can only be withheld in response to a SAR in very limited circumstances.

9. Breaches of data protection – Actions to take immediately

9.1 Actions to take immediately

Whenever there is an actual or suspected breach of GDPR, regardless of the level of impact, contact the Data Protection Officer at Napo HQ. Napo HQ must be informed within 24 hours of you becoming aware of the breach.

Give the Data Protection Officer all the information that you can at that point about the breach. For example:

- The nature of the actual or suspected breach.
- The type of data involved and its sensitivity, including a copy of the information that has been compromised if possible.
- How the breach happened.
- When it happened.
- When you become aware of it.

There is a requirement under GDPR to report certain breaches to the ICO. Where necessary, this will be done by the Data Protection Officer. Please do not report anything to the ICO yourself – report it to the Data Protection Officer at Napo HQ.

Once a breach has been managed, it is important that any lessons learned and security improvements are put in place as soon as possible, to avoid any recurrence of the same problem.

9.2 What is a data protection breach and how to report it

In the course of its activities, Napo accrues a large amount of personal data regarding members, staff and activists. Personal data is any information that is about, or can identify, a living person. This includes things such as their name, address, phone number, email address, membership number and IP address.

Under GDPR, a data breach is: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data”. It therefore does not always refer solely to the loss of personal data.

Most breaches are a result of human error or procedures not being followed. They are rarely malicious.

Data protection regulation requires Napo to report certain types of data breach to the ICO within 72 hours from when you discovered it, or risk incurring large penalties for not meeting our obligations. It is therefore important to **report suspected breaches or near misses to the Napo Data Protection Officer on 0207 223 4887 or DPO@napo.org.uk as soon as they are discovered**. If in doubt, call anyway!

The following are examples of data breaches of varying severity:

- Leaving a case form on a bus which is either recovered later or lost.
- A Napo laptop or mobile phone is stolen.
- Documents are left behind or mislaid during an office move.
- Confidential waste is disposed of insecurely.
- Accidental deletion of a member’s case file.
- An employer informs us that a check-off file has been sent to a non-Napo recipient.
- Saving a list of members in a publicly accessible location.
- Sending an email to lapsed members.
- Using the To or Cc field to send a bulk email instead of the Bcc field.
- Sending an email to the incorrect person with the same name as the intended recipient.
- Member data is accessed during a cyber attack.
- A significant disruption to access to the membership system - Sodalitas.

If you have any further questions regarding data breaches, do not hesitate to contact Napo HQ.

Appendix 1 - Resources

Websites:

Napo Privacy Statement - https://www.napo.org.uk/Privacy-Statement

Information Commissioner's Office – https://ico.org.uk/for-organisations/

General Data Protection Regulation (2018) guidance – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Privacy and Electronic Communication (PECR) guidance - https://ico.org.uk/for-organisations/guide-to-pecr/