AMNESTY INTERNATIONAL UK SECTION

DATA PROTECTION GUIDANCE FOR GROUPS

INTRODUCTION

We have a collective responsibility, as part of the Amnesty movement, for our reputation. When anyone trusts us with their personal information, it is our responsibility to ensure we treat this information in a way that lives up to their expectations, gives them confidence in us, and complies with all our legal obligations.

The Data Protection Act 1998 (the Act) sets out rules which must be followed when handling personal information.

Amnesty UK has introduced new data protection policies and procedures, and provided training to staff and volunteers to help us comply with the Act. We have a shared responsibility to follow the data protection rules.

It could cause damage and distress to our supporters if we do not treat their personal information properly. A breach of the Act could result in criminal prosecution and a fine of up to £500,000 – money which could otherwise be spent on human rights work.

There have been many high-profile data protection breaches recently within the charity and membership sector. For example, in 2016 the Information Commissioner's Office (ICO) which enforces the Act, fined The Alzheimer's Society £80,000, The British Heart Foundation £18,000 and the RSPCA £25,000. If we were to be fined or even just investigated for a potential breach, our reputation with the general public and our supporters would be seriously damaged.

Please take time to read these pages. They cover important points that you should remember when you are handling personal information.

Generally, a useful way of thinking about data protection is to treat people's personal information in the same way that you would expect your own information to be treated.

The 1998 Act will be replaced by new legislation in May 2018. We will revise this guidance before the new legislation comes into force.

THIS GUIDE CONTAINS:

- Key roles and definitions
- The Data Protection Act principles (in brief)
- The Data Protection Act principles with guidance on their purpose and how they might apply to you

Associated documents

- A data protection quick checklist
- Fair Processing Notice guidance

KEY ROLES AND DEFINITIONS

Personal data is information, held electronically or in manual records (eg paper, photographs), which identifies a living person. For example:
• Name • Address • Date of birth • Contact details
• Bank account details • Interests • Photographs
Please note, personal data includes facts and opinions about a person if it identifies them. For example, notes on how you think someone has behaved, performed or appears.

Sensitive personal data is the same as personal data but is about a person's:
• health • religion • political opinion • trade union membership
• racial or ethnic origin • sex life • criminal activity

The Act has **8 Principles** which must be followed when processing personal and / or sensitive personal data. 'Processing' has a wide definition under the Act and it is difficult to think of anything an organisation might do with data that will not be considered processing.

The **Information Commissioner's Office** is the organisation responsible for enforcing the Act.

A **data controller** is the person, group or organisation that collects and decides how personal information will be used. They must register with the Information Commissioner and declare what personal information will be stored and how it will be used.

A **data subject** is the living person whose personal information is being processed.

THE EIGHT PRINCIPLES OF THE DATA PROTECTION ACT

THE DATA PROTECTION PRINCIPLES
The Data Protection Act 1998 was developed to protect people's personal information, provide rules to be followed when processing personal information, and give data subject certain rights.

In brief, the Eight Principles of Data Protection are that personal data must be:
1. collected and processed fairly and lawfully
2. held and used only for specified purposes
3. adequate, relevant and not excessive
4. kept accurate and up to date
5. not kept longer than is needed
6. used in line with the data subjects' rights
7. kept safe and secure
8. not transferred outside of the European Economic Area (the EU plus Iceland, Norway and Liechtenstein) unless that country has a suitable data protection law in place.

Organisations and their staff and volunteers that collect, store and use personal information have to follow the eight data protection principles.

PRINCIPLE 1:

PERSONAL DATA MUST BE PROCESSED FAIRLY AND LAWFULLY

This means that you must be clear and transparent with people when collecting their personal information about how it will be used. You must not mislead people or disguise how personal information will be used. When collecting someone's personal information in an electronic or paper form, or verbally, they should be informed:

1. of the purpose for which their personal information will be used. For example, for a petition, to sign up for an event or to be added to a mailing list.
2. if their personal information will be shared with any other groups or organisations. For example, with an Amnesty International UK office.

This is done by including a **Fair Processing Notice** (FPN) at every point that personal information is collected. You need to create a FPN for electronic and paper forms, for example petitions, competitions, events and membership forms, and on your website.

A FPN is sometimes known as a **data protection statement** or privacy notice. It describes who will be holding the personal information (the name of your group), why it is being collected, and the name or type of any other organisation that it might be shared with.

Failing to have a FPN is not only a breach of the Act but it can also hamper our work. If groups gather names in support of an action and send these to the London office, we would not be able to progress with the action if the FPN stating the information would be shared with us was not included when the personal information was collected.

You must obtain the **explicit consent** of a person if you are using their sensitive personal data. Explicit consent is a direct statement, provided verbally or in writing, and giving permission for sensitive personal data to be used for a specific purpose. **Please note** that someone may give you sensitive personal data without you asking for it. **For example,** someone speaking to you at a Pride stall may mention their sexuality in passing, or you may discover someone is a trade union member through campaigning on workers rights. If you are going to use that information at all, even just record it, you must get the person's explicit consent to do so, and it is a good idea to obtain this explicit consent as part of the FPN. You must keep a record that explicit consent has been obtained and the date that it was obtained.

The correct wording for a FPN is very important. An inadequate FPN could mean that we cannot legally use the personal information provided to us.

See here for information on Amnesty UK's Fair Processing Notice guidance.

PRINCIPLE 2:

Personal information should be used only for lawful and specified purposes

You can only use the personal information that is collected for the purpose(s) described in the FPN. If personal information is collected for a petition and only this purpose is included in the FPN, then you can only use the information for the petition; you cannot use it for any other purpose(s), for example you cannot send it to an Amnesty International UK office.

PRINCIPLE 3:

Personal information must be adequate, relevant and not excessive

This means that your group should only collect just the right amount of information for the purpose required and described in the FPN – no more, no less.

Even if a person gives you more information that you need to know, for example in an email or phone conversation, only the relevant information should be recorded. The Act does not allow for personal information to be kept because 'it might become useful'.

PRINCIPLE 4:

Personal information must be accurate and up to date

Personal data must be accurate at all times. You must check that your files and records containing personal information are accurate and up to date. It is a good idea to remind people when communicating with them to notify you of any changes in their personal information. If someone informs you of a change (phone number or address, for example) you must amend all records as soon as possible.

PRINCIPLE 5:

Personal information should be kept only as long as is necessary

Your group should decide and document how long it needs to keep different types and records of personal information. For example, you will keep financial information for six years. You must have a valid reason for keeping personal information. Once the information is no longer required it must be disposed of securely, for example shredded or via a confidential waste system.

PRINCIPLE 6:

Processed in line with data subject's rights

The Act provides certain rights for people. The two most relevant to us are the right to subject access and the right to prevent processing for direct marketing purposes.

Subject Access

People have the right to see the personal information held about them. Anyone who believes that your group or Amnesty International UK is holding personal information about them (paper or electronically) can apply for a copy of this by making a Subject Access Request (SAR).

If it is clear that a person is asking for their own personal information, then the request should be treated as a SAR, even if they do not explicitly use that term or mention the Data Protection Act.

You must assume that anything you record about a person could be seen by that person. So you must not record any unfair or untrue comment that you would be unable to defend if challenged.

If anyone makes a SAR to your group, please send their contact details to Amnesty International UK's Data Protection Officer immediately at dataprotection@amnesty.org.uk

We are required to respond within 40 calendar days of receiving the initial request so please inform us immediately. Our Data Protection Officer will work with you to ensure that we supply the information in accordance with the law.

Direct Marketing

People have the absolute right to prevent their personal information being processed for direct marketing purposes.

The definition of 'direct marketing' in the Act includes an organisation communicating its aims and objectives by email, e-newsletter, telephone, text message or post. This includes information about our campaigns, petitions, events and fundraising activities.

You must only contact individuals with direct marketing messages by electronic means (email, text message) if they have already opted in to receiving these communications by email and / or text message.

Every direct marketing message you send by email and text message must include an unsubscribe function so that the recipient has a choice to opt out of further communications from the group. Supporters must not be contacted again if they unsubscribe or request not to receive further direct marketing messages.

If someone contacts you to say that they no longer wish to receive direct marketing messages by post or phone call, you must remove their name from or suppress it in your group mailing list. Supporters must not be contacted again if they have requested not to receive further direct marketing messages.

Mailing lists must be updated immediately when someone unsubscribes. To include someone who has unsubscribed in another mailing would be a breach of the Act.

If you receive a request from a contact or supporter to stop receiving communications from Amnesty UK, please forward the details to the Supporter Communications Team immediately (sct@amnesty.org.uk), as we may need to update our mailing lists too.

PRINCIPLE 7:

Personal information must be kept securely

The Act requires that appropriate measures are taken to protect personal information from accidental loss, damage, destruction and theft.

There are some simple measures that should be taken by groups to protect the personal information that you process; all group members need to be aware of them:
Anyone who handles your group's personal information must be aware of their data protection compliance responsibility and understand how to comply with the Act's Eight Principles.

Access to personal information should be limited to those on a strict need to know basis.

Do not leave confidential papers or screens containing personal information visible to others – for example, in meetings, on trains, even in your own home.

Lock desks and cupboards used to store personal information. Keep the keys secure.

Use a shredder to dispose of personal information recorded on paper (including printouts of electronic records and hand-written notes) when it is no longer needed.

Use Royal Mail registered post or a courier to send large volumes of paper containing personal information or sensitive personal data. This also applies to transferring mobile devices such as memory sticks, CDs, DVDs, which must also be encrypted and password protected.

Protect all electronic devices used to process and store personal information with encryption and strong passwords. This includes computers, laptops, tablets and smart phones. Special care should be taken when travelling with these devices.

If it is necessary to email an electronic file or document containing personal information, protect it with encryption and a strong password. Encryption is the scrambling of text or data for security purposes. 7 Zip can be used for encryption.

Emails containing personal information may need to be encrypted or password protected if the information is sensitive or confidential. Do not include any personal information in the subject line of an email.

Double check that you have attached the correct file(s) before sending an email.

Always use the bcc field (not the cc field) when sending an email to more than one person so that the recipients' email addresses are not visible to each other (unless consent to share email addresses has previously been obtained).

Sharing personal information

Amnesty's policy is never to share personal information with any other organisation unless we are legally required to do so, or if another organisation processes data on our behalf. For example, we may use a mailing company to post information for us.

We never pass on personal information to other organisations to use for their own purpose.

A person's personal information must not be disclosed or shared with another person or organisation without their prior consent. This includes contact details and email addresses.

Amnesty UK offices can only share personal information with groups if permission to do so has been obtained.

Groups can only share personal information with Amnesty International UK offices if the FPN states that this information will be shared with us.

Data privacy when storing information online

If you're collecting and storing personal information in a shared system online (in the cloud), be aware that this is not completely secure. Check that your cloud provider offers an appropriate level of protection in line with the Act. Ensure your account is password protected and regularly change it. Limit access to the account to those who need it. Regularly review and update who has access. Avoid storing sensitive personal data in the account. Consider zipping and encrypting files with a password before storing them to minimize the risk of them getting into the wrong hands.

PRINCIPLE 8:

Personal information shall not be transferred to countries outside the European Economic Area (EEA) without adequate protection

Personal data must not be transferred to a country outside the EEA unless explicit consent has been obtained from the person; the data has been completely anonymised; that country ensures an adequate level of data protection. Please contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk for further advice on this if you need to transfer personal information outside of the EEA.