1.

AMNESTY INTERNATIONAL

DATA PROTECTION GUIDANCE FOR UK GROUPS AND ACTIVISTS

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.

In May 2018 the **General Data Protection Regulation (GDPR)** comes into force in the UK, replacing the Data Protection Act (1998), and in doing so strengthens the rights of individuals, giving people more power over how organisations use their data. The law requires organisations to demonstrate that they are complying and be more transparent about how they use personal data.

We have a shared responsibility to both follow the data protection rules and demonstrate how we comply with them.

It could cause damage and distress to our supporters if we do not treat their personal information properly. A serious breach of data protection law could result in criminal prosecution and a maximum fine of up to €20 million, or 4% of an organisation's annual turnover. While not all infringements of data protection law will lead to serious penalties, any fine is money which could otherwise be spent on human rights work. 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 this guidance. Throughout we highlight key points for you to consider, and attempt to provide practical suggestions where relevant.

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

1. **Data protection guidance:** www.amnesty.org.uk/dpguidegroups
2. **Privacy notice:** www.amnesty.org.uk/privacynoticeguide
3. **Data protection checklist:** www.amnesty.org.uk/dpchecklist
4. **Consent checklist:** www.amnesty.org.uk/consentchecklist

THIS GUIDE CONTAINS:

- Key roles and definitions
- An overview of the data protection principles with guidance on their purpose and how they might apply to you
- An overview of the rights granted to individuals under the GDPR, with guidance on their implications

Associated documents

- A data protection quick checklist
- Privacy Notice guidance
- A checklist on obtaining, documenting and managing consent

KEY ROLES AND DEFINITIONS

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

A **data controller** is the person, group or organisation that collects and decides how personal information will be used.

Personal data is information held electronically or in manual records (e.g. 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 about a person's
• health • religion • political opinion • trade union membership • racial or ethnic origin • sex life

Data protection law refers to the laws (including the GDPR and the Privacy and Electronic Communication Regulations) that control how organisations use personal data, and that are enforceable in the UK.

Data protection principles are rules which must be followed when processing personal and / or sensitive personal data.

'Processing' has a wide definition under data protection law 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 data protection law in the UK.

March 2018

If you have any questions about data protection, contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk **or** activism@amnesty.org.uk
For more detailed guidance about data protection, see www.ico.org.uk

AMNESTY INTERNATIONAL

THE DATA PROTECTION PRINCIPLES

The principles, which provide rules to be followed when processing personal information, are similar under the GDPR to those in the Data Protection Act. In brief, the principles of Data Protection are that **personal data must be:**

1. collected and processed lawfully, fairly and transparently
2. held and used only for specified, explicit and legitimate purposes
3. adequate, relevant and limited to only what is necessary
4. kept accurate and up to date, and corrected or deleted if there are mistakes
5. not kept longer than is needed
6. kept safe and secure, to protect the data from being used inappropriately

And finally:

7. data controllers must be able to show how they comply with the principles above

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

PRINCIPLE 1:

Personal data must be processed lawfully, fairly and transparently

KEY POINTS

✔Wherever possible, you should obtain consent before acquiring, holding or using personal information.

✔Be clear and transparent about how you use data by including a Privacy Notice at every point that personal information is collected.

✔If you're unsure how to go about doing any of the above, please contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk for more advice.

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 told:

1. who will be handling their personal information.
2. the purpose for which their personal information will be used (eg a petition or to sign up for an event).
3. if their personal information will be shared with any other groups or organisations (eg an Amnesty International UK office).

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

A Privacy Notice is sometimes known as a **data protection statement** or **Fair Processing Notice** (FPN). It is a written declaration that must be presented in clear and plain language, and in an accessible format.

Being honest and open about who you are and what you are going to do with the personal data you collect in a Privacy Notice, is only one element of fairness. Fairness also includes:

1. using information in a way that people would reasonably expect.
2. thinking about the impact of your processing - will it have negative effects on the individuals whose personal information you're using?

Failing to have a Privacy Notice is not only a breach of data protection law 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 Privacy Notice stating the information would be shared with us was not included when the personal information was collected.

Remember, 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, in passing, mention their sexuality. 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 Privacy Notice. You must keep a record that explicit consent has been obtained and the date that it was obtained.

The correct wording for a Privacy Notice is very important. An inadequate Privacy Notice could mean that we cannot legally use the personal information given to us. See here for information on Amnesty UK's Privacy Notice guidance.

PRINCIPLE 2:

Personal information should be used only for specified, explicit, and legitimate purposes

You can only use the personal information that is collected for the specified, explicit and legitimate purpose(s) described in the Privacy Notice. If personal information is collected for a petition and only this purpose is included in the Privacy Notice, 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 limited to only what is necessary to achieve the purpose for which it was collected

This means that your group should only collect just the right amount of information for the purpose required and described in the Privacy Notice – no more, no less. Even if a person gives you more information than you need to know, for example in an email or phone conversation, only the relevant information should be recorded. Data protection law does not allow for personal information to be kept just because 'it might become useful'.

PRINCIPLE 4:

Personal information must be accurate and up to date, with errors corrected or deleted as soon as possible

KEY POINTS

✔ **Regularly check** that the information you hold is accurate. At least **once a year** you should remove any records that are no longer needed.

Personal data must be accurate at all times and especially before sending any communications to a mailing list. If there is any doubt about the accuracy of personal data then it should not be used. 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 (eg phone number or address) you must amend (or where relevant, delete) 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:

Personal information must be kept safely and securely in a way that protects it from falling into the wrong hands

KEY POINTS

✔ Data protection law requires **that appropriate measures** are taken to protect personal information from accidental loss, damage, destruction, theft and unauthorised use.

✔ **All group members** need to be aware of **simple measures** that should be taken to **protect** the personal information that you process.

Our tips for keeping data safe

- Anyone who handles your group's personal information must be aware of their data protection compliance responsibility and understand how to comply with the data protection principles.
- Access to personal information should be limited 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. Take special care 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. Most software programmes used to create zip files will offer encryption options.
- 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).

March 2018

If you have any questions about data protection, contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk **or** activism@amnesty.org.uk
For more detailed guidance about data protection, see www.ico.org.uk

AMNESTY INTERNATIONAL

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

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 International UK offices can only share personal information with groups if permission to do so has been obtained. Don't pass on personal information to other organisations to use for their own purpose unless you have consent to do this or it is needed to prevent serious harm to an individual, or for the prevention or detection of a crime.

Groups can only share personal information with Amnesty International UK offices if the Privacy Notice 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 might not be completely secure.

Check that your cloud provider offers an appropriate level of protection in line with data protection law. Ensure your account is password protected and regularly change your password. 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 7:

Data controllers must be able to show how they comply with the principles above

KEY POINTS
✔Have a plan in place to **identify and report any breaches or 'near misses'** of data protection law to the Data Protection Officer at Amnesty International UK at dataprotection@ amnesty.org.uk **as soon as you discover** them.
✔Ensure you **keep written records** of how you use personal information and that this information is kept up to date.
✔Data protection law requires you to consider privacy at the start of any project. This is also known as **'privacy by design'**.

Accountability has always been a feature in data protection law, but now anyone handling personal information must be able to demonstrate and provide evidence of how they comply with data protection principles.

Personal data breaches
A data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal information.

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; or if someone accesses the personal information or passes it on without the permission of the data subject. This includes breaches that are the result of both accidental and deliberate causes.

It can also include:
- sending personal information to an incorrect recipient
- electronic devices containing personal information being lost or stolen
- altering the personal information of someone without their permission

A breach can have a range of negative effects on the individuals concerned, including emotional distress, and a breakdown in trust. More severe breaches can significantly affect the lives of individuals.

Data protection law makes clear that when a security incident takes place, we have to act quickly. If you come across something that you think is a data protection breach or there has been a near miss, please let the Data Protection Officer at Amnesty International UK know immediately. If a breach has occurred, we will need to report it to the Information Commissioner's Office within 72 hours.

Record keeping
Data protection law requires you to keep written records explaining how you process personal information, ensure that these records remain accurate and are updated when things change. If we were ever audited by the Information Commissioner's Office, groups should be able to provide documentation that outlines:

- the types of personal information you collect (eg email addresses, phone numbers) and who you collect this from (eg group members)
- the information you provide in your Privacy Notice
- records of consent
- the location where you store personal information
- records of personal data breaches
- any third parties who will receive this personal information (for example, Amnesty International UK Section)

Once a year check your records and remove the details of anyone who is no longer involved. Paper records must be disposed of carefully, for example using a shredder. As with paper records, you must check your electronic records once a year and delete files or details of anyone who is no longer involved.

Privacy by design
Privacy by design is about putting in place appropriate measures to respect people's right to privacy, from the very beginning.

For example, if you are organising an event, it would be about ensuring you have thought through any privacy implications early in the planning stages - and discussed them with Amnesty International UK's Data Protection Officer if necessary.

March 2018

If you have any questions about data protection, contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk **or** activism@amnesty.org.uk
For more detailed guidance about data protection, see www.ico.org.uk

AMNESTY INTERNATIONAL

DATA SUBJECT RIGHTS

The General Data Protection Regulation provides the following specific rights for all individuals.

- **The right to be informed** – your obligation to be transparent and provide the appropriate information when collecting personal information
- **The right of access** – an individual's right to access the personal information that you hold about them
- **The right to rectification** – your obligation to correct any personal information that is found to be inaccurate or incomplete
- **The right to data portability** – an individual has the right to move, copy or transfer your personal information easily and safely from one IT environment to another
- **The right to restrict processing** – an individual has a right to 'block' or suppress processing of personal data.
- **The right to object** – an individual's right to object to any processing of their personal information
- **The right to erasure** – also known as the right to be 'forgotten', an individual's right to have any personal information held about them deleted or removed
- **Rights related to automated decision making including profiling**

HOW TO RESPOND TO REQUESTS

Groups are most likely to receive requests that relate to the following rights.

The right of access (subject access requests)
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 (on 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 data protection law.

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 let Amnesty International UK's Data Protection Officer know immediately at: dataprotection@amnesty.org.uk

We are required to respond within one month of receiving the initial request, so our Data Protection Officer will work with you to ensure that we supply the information in accordance with the law.

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

The definition of 'direct marketing' by the Information Commissioner's Office 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 can 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. Individuals must not be contacted again if they unsubscribe, or if they 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. Individuals must not be contacted again if they have requested not to receive further direct marketing messages.
If you receive a request from an individual to stop receiving communications from Amnesty International UK, please forward the details to the Supporter Communications Team immediately (sct@amnesty.org.uk), as we may also need to update our mailing lists.

The right to erasure
The right to erasure is also known as 'the right to be forgotten'. People have the right to request that their personal information is deleted or removed where there is no compelling reason for its continued processing.

If you have disclosed an individual's personal information to others, you must contact each recipient of that information and ask them to erase the personal data in question. If requested, you should also inform the individual affected about the other recipients of their personal information. If you have published personal information online, for example on social networks, forums or websites, you should also erase the personal information from online platforms. If you receive a right to erasure request and you're unsure how to handle it, please get in touch with Amnesty International UK's Data Protection Officer.

March 2018

If you have any questions about data protection, contact Amnesty International UK's Data Protection Officer at dataprotection@amnesty.org.uk or activism@amnesty.org.uk
For more detailed guidance about data protection, see www.ico.org.uk

AMNESTY INTERNATIONAL