

# QUICK CHECKLIST

## DATA PROTECTION COMPLIANCE

### DO

- ✓ Ask someone for their consent before sharing their personal data with another organisation
- ✓ Ask one person if you can forward their details to the other (or ask both in advance)
- ✓ Email your group putting everyone in the 'bcc' and then explain in the body text who the email has gone to, eg all your local group members
- ✓ Make it clear in any statement if the personal data is staying with the group or being passed to an Amnesty International UK office
- ✓ Ask everyone in your group who accesses or keeps personal data to read these guidelines and confirm that they have read and understood them
- ✓ Ensure that every device you open or keep personal data on is password-protected with a strong password, and that documents are always filed away or shredded after use
- ✓ Encrypt and password-protect any documents containing personal data and send the password in a different medium, eg in a text message
- ✓ Check that emails have the correct file attachment and recipients before hitting send
- ✓ Dispose of out-of-date personal data securely, eg shred paper forms
- ✓ Regularly review those who can access personal data on a cloud system and remove those who no longer need to access it

1. Data protection guidance: [www.amnesty.org.uk/dpguidegroups](http://www.amnesty.org.uk/dpguidegroups)
2. Privacy notice: [www.amnesty.org.uk/privacynoticeguide](http://www.amnesty.org.uk/privacynoticeguide)
3. Data protection checklist: [www.amnesty.org.uk/dpchecklist](http://www.amnesty.org.uk/dpchecklist)
4. Consent checklist: [www.amnesty.org.uk/consentchecklist](http://www.amnesty.org.uk/consentchecklist)

### DON'T

- ✗ Share someone's personal data with another organisation without explicit consent
- ✗ Copy two people into an email who do not already have each other's email addresses
- ✗ Email your group with email addresses in the 'to' or 'cc' fields
- ✗ Pass personal data to the Amnesty International UK offices without consent
- ✗ Pass personal data to anyone in your group unless they have been trained, or have read and understood these guidelines
- ✗ Allow people to see personal data that they have no right to view, eg while working on a train or in a public area
- ✗ Email personal data in an open document
- ✗ Hit SEND on an email with an attachment without double-checking everything
- ✗ Keep out-of-date paper or electronic records of personal data
- ✗ Store personal data in a cloud system without checking its security, adding a password, and ensuring that only appropriate people can access it

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