Data Protection Policy

Definitions

- Action21 means Action 21 (2010) Ltd, Registered Charity number 1136450.
- UK GDPR means the UK General Data Protection Regulation.
- Responsible Person means the nominated member of staff or Trustee acting as the Data Protection Officer.
- Register of Systems means a register of all systems or contexts in which personal data is processed by Action21.

General Provisions

- This policy applies to all personal data processed by Action21.
- The Responsible Person shall take responsibility for Action21's ongoing compliance with this policy.
- This policy shall be reviewed at least every 2 years.

Data Protection Principles

The security and privacy of data is taken seriously by us but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. Action 21 is a 'data controller' for the purposes of personal data. We are committed to complying with our all the Data Protection legal obligations regarding how we obtain, handle, process or store personal data.

This policy applies to current and former employees, workers, volunteers, interns, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services), our Privacy Notice and any other notice we issue to you from time to time in relation to your data. Any breach of this policy may result in disciplinary action being taken up to and including dismissal.

Action 21 has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be found on Action 21's website.

Action 21 has taken steps to protect the security of data within the organisation and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

This policy explains how Action 21 will hold and process information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, Action 21.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by Action 21 at any time.

As a not-for-profit body Action21 is not registered with the Information Commissioner's Office as an organisation that processes personal data under the permitted exemptions, however Action21 is committed to processing data in accordance with its responsibilities under the UK GDPR.
Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

What is Personal Data?

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. Personal data includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

Special Categories of Personal Data

Special Categories of Personal Data include the Data Subjects:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data;
- health;
- sex life and sexual orientation; and
- any criminal convictions and offences.

How you should Process Personal Data for Action 21

Everyone who works for, or on behalf of, Action 21 has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of, Action 21 and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained and follow the following principles:

- Do not share personal data informally; keep it secure and don't share it with unauthorised people.
- Regularly review and update personal data which you have to deal with. Update us if your own contact details change.
- Do not make unnecessary copies or keep personal data. Dispose of any copies securely.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not transfer personal data out of the European Economic Area except in compliance with the law and with authorisation of the person responsible for data in Action 21.
- Lock drawers and filing cabinets. Do not leave papers with personal data lying about.
- Do not take personal data away from Company premises without authorisation.
- Ask for help from the person responsible for data in Action 21 if you are unsure about data protection, or if you notice any areas we can improve upon.

Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, Action21 shall maintain a Register of Systems.
- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to Action21 shall be dealt with in a timely manner.

Lawful purposes

- All data processed by Action21 must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- Action21 shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Action21's systems.

Data minimisation

Action21 shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- Action21 shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / removal

- To ensure that personal data is kept for no longer than necessary, Action21 shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

How long will employee and volunteer records be held?

- Action 21 will hold employee records for 6 years.
- Action 21 will hold volunteer records for 3 years, unless holding the data for longer can be justified.
- Action 21 will hold volunteer applications for up to 6 months.

Security

- Action21 shall ensure that personal data held in electronic form is stored securely using modern software that is kept-up-to-date.
- Action21 shall ensure that personal data held in paper form is stored securely.
- Access to personal data shall be limited to staff and volunteers who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- It is the responsibility of the staff and the Responsible Person to ensure that volunteers dealing with personal data have been instructed in their obligations under GDPR.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

How to Deal with Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, please inform Data Protection Officer immediately and keep any evidence you have in relation to the breach. We will take the appropriate action.

Employee's Data

How and why we process your data

'Processing' the data that we hold includes collection, recording, organisation, structuring or storage, adapting, retrieving, disseminating, aligning and also removing or erasing it.

Action 21 will process your personal data if it is needed to perform the contract of employment (or services) between us or to comply with any legal obligation, or if it is necessary for our legitimate interests (or for the legitimate interests of someone else). The Privacy Notice covers the reasons for collecting and processing your data, and when and who we share it with. We can process your personal data for these purposes without your knowledge or consent. However, we will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it. We will only process special categories of your personal data in certain situations in accordance with the law. We do not take automated decisions about you using your personal data or use profiling in relation to you.

Subject Access Request (SAR)

Data subjects can make a 'Subject Access Request' ('SAR') to find out the information we hold about them. If you would like to make a SAR in relation to your own personal data, you should make this in writing to the person responsible for data in Action 21. We will comply with all legal requirements. If you receive a SAR, please pass it on to the person responsible for data and ensure that you keep any information regarding it.

Your Data Subject Rights

The law provides clear rights with regard to your data protection; a full list can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations, and also on the route for you to make a complaint. The following are the key, but not exhaustive, list of rights:

- The right to information about what personal data we process: how and on what basis.
- The right to access your own personal data via a SAR.
- The right to correct any inaccuracies in your personal data, by contacting the person responsible for data in Action 21.
- The right to request that we erase your personal data where we were not entitled under the law to process it – or where it is no longer necessary to process it for the purpose it was collected – and have access temporarily restricted. To do this, you should contact the person responsible for data in Action 21.
- The right to object to data processing where we are relying on a 'legitimate interest' to do so and you think that your rights and interests outweigh our own and you wish us to stop; or for use in direct marketing.
- The right to receive a copy of your personal data and to transfer your personal data to another data controller.
- The right to be notified of a data security breach concerning your personal data.
- The right not to give your consent for processing of personal data, or to withdraw this later by contacting the person responsible for data in Action 21.

January 2024