Accelerate People

Data Protection Policy

Accelerate People

Document History

To ensure quality control and to quickly identify any changes made version control must be listed below. Including the latest version number, date of the amendment and changes made.

Document Details	
Document Name	Data Protection Policy
Purpose of Document	This policy describes how this personal data must be collected, handled and stored to meet Accelerate People's data protection standards and comply with the law.
Document Version Number	V1.0
Document Status	Live
Document Owner	Head of Compliance

Version History		
Version Number	Date Amended	Changes Made
V1.0	06/07/2021	Document created

This policy will be reviewed on an annual basis and, where appropriate, updated in response to input from consumers, results from internal and external monitoring arrangements, amendments in internal procedures, IfATE, ESFA and EQA actions or where developments in legislation occur.

INDEX

1. Terminology

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data controller means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing.

Data processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Processing means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

Data Subject means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

2. Introduction

Accelerate People needs to gather and use certain information about individuals.

These can include customers/users, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet Accelerate People's data protection standards and comply with the law.

3. Why this policy exists

This data protection policy ensures Accelerate People:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Provide training and support for staff who handle personal data, so that they can act confidently and consistently

4. Data Protection Law

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. These state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

The Data Protection Officer is responsible/accountable for demonstrating compliance for the above principles.

5. Policy Scope

The policy applies to all Accelerate People office spaces, all staff of Accelerate People and all contractors, suppliers and other people working on behalf of Accelerate People

It applies to all personal data, meaning any information relating to an identified or identifiable natural person ('data subject'), that Accelerate People controls, stores or processes. This can include:

- Name
- An identification number/ULN
- Location data
- An online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

6. Data Protection Risks

This policy helps to protect Accelerate People from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately
- A laptop or mobile device being stolen
- A data protection impact assessment not being carried out when introducing new technology
- Not locking away documents containing personal data (at home or work) when left unattended
- Deliberately accessing or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to Accelerate People's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

All staff have an obligation to report a security incident as soon as they are aware that it has occurred by emailing one of the Directors of Accelerate People immediately. All security incidents in Accelerate People are investigated by the Directors.

The investigation will ensure action is taken to minimise any impact, recover the information and that appropriate action is taken to prevent similar occurrences. Our company has an obligation to document and report incidents to the Information Commissioner's Office (ICO) - the UK Data Protection Regulator.

7. Responsibilities

Everyone who works for or with Accelerate People has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy, our privacy notices and data protection principles.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible/accountable for ensuring that Accelerate People meets its legal obligations
- Where appropriate, the Data Protection Officer is responsible for:
    - Keeping the board updated about the data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule
    - Arrange data protection training and advice for the people covered by this policy
    - Dealing with Subject Access requests from individuals to see the data Accelerate People holds about them
    - Checking and approving any contracts or agreements with third parties that may handle Accelerate People's sensitive data
- The Directors are responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standard
    - Evaluating any third-party services the company is considering using to store or process data
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Approving any protection statements attached to communications such as emails and letters
    - Addressing any data protection queries from journalists or media outlets like newspapers
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

8. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should note be shared informally. When access to confidential information is required, employees can request it from their line managers

- Accelerate People will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within Accelerate People or externally
- Data should be regularly review and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should request help from the designated security officer if they are unsure about any aspect of data protection.

9. Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for example on a printer.
- Data printouts should be shredded or disposed of using the confidential waste.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, it must be encrypted and stored securely.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud storage service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with Accelerate People's standard backup procedures.
- Data should never be saved directly to un-encrypted laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

10. Data Use

When working with personal data:

- Employees should ensure the screens of computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, unless the contents of the data has been encrypted.
- Data must be encrypted before being transmitted electronically. The designated security officer can explain how to send data to authorised external contact.
- Personal data should never be transferred outside of the geographically areas defined under the GDPR, if you need to transfer data outside the European Economic Area, please check with the designated security officer.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

11. Lawfulness, Fairness & Transparency

Personal data shall be processed fairly and lawfully, Accelerate People will define these through our privacy policies/notices.

To ensure our processing of Personal data is lawful, data shall not be processed unless:

- Data subject gives consent for one or more specific purposes
- Processing is necessary to meet contractual obligations entered into by the data subject
- Processing is necessary to comply with legal obligations of the controller
- Processing is necessary to protect the vital interests of the data subject
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller
- Purposes of the legitimate interests pursued by the controller

12. Purpose Limitation

Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. These need to be defined within Accelerate People's privacy notices and if these change we would need to gain the data subject's consent before we start the data processing.

13. Adequacy

The storage and processing of personal data must be adequate, relevant and limited to what is necessary related to Accelerate People's specified purpose. Data processing should only use as much data as is required to successfully accomplish a given task. Additionally, data collected for one purpose cannot be repurposed without further consent. When collecting data, remember to ask yourself several questions for each point of data you are planning to collect:

- Does the individual know I am collecting the data?
- How am I planning to use this data?

- Does the individual know why I am collecting the data?
- Is there a way of achieving this purpose without having to collect the data?
- How long will I need the data for to achieve the purpose?

14. Data Retention

Accelerate People may retain data for differing periods of time for different purposes as required by statute or best practices, individual departments incorporate these retention times into the processes and manuals. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data. Accelerate People disposal procedures must be followed when appropriate, if you have any questions regarding the disposal of data, please contact the Data Protection Officer.

15. Subject Access Requests

All verified individuals who are the subject of the personal data held by Accelerate People are entitled to:

- Understand how and why we will use their data
- Request and receive the data we hold on them
- Update data if it's incorrect or incomplete
- Have the data deleted if the processing is no longer necessary in relation to the purpose, the data subject has withdrawn consent, the data subject objects to the processing, the processing is unlawful or it must be erased to comply with a legal obligation
- Restrict the processing of their data when they:
    - Contest the data accuracy
    - Have objected to the processing, but haven't been verified
    - Oppose the deletion of the data due to unlawful processing, but requests the restriction
    - Required the data to be held to form a legal defence
    - Transfer the personal data to a different data controller
    - Object to the data being processed if the processing is
- The processing is based on legitimate interests or the performance of a task in the public interest/exercise of an official authority (including profiling)
    - Not to be subject to a decision based solely on automated processing, including profiling, which significantly affects the data subject
    - For purposes of scientific/historical research and statistics
    - Direct Marketing (including profiling)

If an individual contacts the company requesting this information, this is called a subject access request. All subject access requests must be logged and the Data Protection Officer must be informed as soon as possible.

Subject access requests must be done in writing by email to the Data Protection Officer as outlined below, as per our privacy notices and a data subject will need to be verified before any data is released.

Data subject access requests are free of charge, we may be able to charge 'reasonable fee if there are requests for further information and any fee must be based on the administrative cost of providing the information. Information requested must be provided within 1 month of receipt of a request.

Data Protection Officer, Sam Sawyer Sam@accelerate-people.co.uk