Dated:11.01.2024

Data Protection Policy (2023)

Goal of the data protection policy

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018 but also to provide proof of compliance.

Preamble

Adults Move Lincolnshire CIC needs to gather and use certain information about individuals. These can include customers, 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 the organisation's data protection standards — and to comply with the law.

Purpose

The principles underlying this data protection policy ensures DHSC: • Complies with Data Protection legislation and follows good practice • Protects the rights of staff, customers and partners • Is open about how it stores and processes individuals' data • Protects itself from the risks of a data breach or cyber-attack on its systems

Scope

This policy applies to all personal data and special categories of personal data (previously known as sensitive data) processed by Adults Move Lincolnshire CIC and as defined under the General Data Protection Regulation (GDPR), including structured sets of personal data held in electronic or other filing systems that are accessible according to specified criteria.

'Personal Data' means any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to: (a) an identifier such as a name, an identification number, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. This can include:

• names of individuals;

• postal addresses;

• email addresses;

• telephone numbers;

• any other information relating to individuals.

For personal data to be processed lawfully, one or more of the following legal grounds must apply:

• the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

• processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

• processing is necessary for compliance with a legal/statutory obligation to which the controller is subject to

• processing is necessary in order to protect the vital interests of the data subject or of another natural person;

• processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

• processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (although 'legitimate interest cannot generally be used by public bodies as a before processing, it is included here in the interest of completeness).

Special categories of personal data (sensitive data)

These are personal data deemed to be more sensitive by law, and so need additional protection. They cannot be processed unless at least one further condition for processing special category data is fulfilled. These conditions are:

• the data subject has given explicit consent;

• the processing is necessary in the context of employment law, or laws relating to social security and social protection;

• the processing is necessary to protect vital interests of the data subject or of another natural person;

• the processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes;

• the processing relates to personal data which have been manifestly made public by the data subject;

• the processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity; • the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects;

• the processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and service

• the processing is necessary for reasons of public interest in the area of public health (e.g. ensuring the safety of medicinal products);

• the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing. Special categories of data consist of information which relates to:

• the racial or ethnic origin of the data subject; • their political opinions;

• their religious beliefs or other beliefs of a similar or philosophical nature;

• whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); • their physical or mental health;

• their sexual life or orientation;

• genetic/biometric data (where processed to uniquely identify an individual).

The Policy

Dated:11.01.2024

This policy sets out Adults Move Lincolnshire CIC's commitment to: protecting personal data; how this commitment is implemented with regard to the collection and use of personal data; and ensuring the rights of individuals whose data is held (the Data Subject) can be exercised as prescribed by the General Data Protection Regulation. Adults Move Lincolnshire CIC is committed to ensuring that it complies with the underpinning six data protection principles, as listed below.

The 6 Data Protection principles

The 6 Data Protection principles:

• personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
• personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; • personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
• personal data shall be accurate and, where necessary, kept up to date
• personal data shall be 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 shall be 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.

These principles will be adhered to with the following ambitions:

• meeting our legal obligations as laid down by the GDPR;
• ensuring that data is collected and used fairly, lawfully and transparently (excepting the provisions of the Law Enforcement Directive);
• processing personal data where an appropriate legal basis to do so exists and only in order to meet our operational needs or fulfil legal requirements
• taking steps to ensure that personal data is up to date and accurate
• establishing appropriate retention periods for personal data; • ensuring that data subjects' rights can be appropriately exercise
• ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues, i.e. Data Protection Officer;
• ensuring that all staff are made aware of good practice in data protection;
• providing adequate training for all staff responsible for personal data;
• ensuring that everyone handling personal data knows where to find further guidance; • ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;
• sharing information where required by law and where approved information sharing agreements are in place and when agreed processes have been followed;
• regularly reviewing data protection procedures and guidelines within the organisation; • adopting local and national data protection best practice, including incorporation of appropriate learning from any published ICO data protection and/or European Data Protection Board (EDPB) guidance;
• publishing and promoting this policy and the rights of data subjects including how to make a right of access request;
• registering with the Information Commissioner as an organisation which handles data; • establishing procedures for reporting data protection breaches to relevant authorities for investigation, including self-referral mechanisms;
• being clear with individuals whose data we process as to how we store it, what we do with it and why;

• responding to any valid subject access requests promptly and in any event within one month of receiving them (unless limited exceptions apply)

Data Protection Risks

This policy helps to protect Adults Move Lincolnshire CIC from some very real data security risks, including:
• breach of confidentiality and public trust; for instance, information being shared inappropriately;
• failing to offer choice; for instance, all individuals should be free to choose how the organisation uses data relating to them when the processing is by consent;
• failing to observe the enhanced rights that citizens have under the GDPR - for example, right of access, right to rectification, etc;
• reputational damage; for instance, Adults Move Lincolnshire could suffer if hackers were to successfully corrupt, gain access to or steal sensitive data.

Roles and Responsibilities

Adults Move Lincolnshire CIC's responsibilities:
• Adults Move Lincolnshire CIC is the data controller under Data Protection Legislation for the personal data it processes for its own purposes. It is also a joint data controller for business undertaken through its Executive Agencies - the Medicines and Healthcare Products Regulatory Agency and Public Health England. (The term 'joint data controller' is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing);
• the Accounting Officer has overall responsibilities for compliance with data Protection legislation;
• the Data Protection Officer (DPO) is responsible for monitoring progress and advising the organisation on implementation of this policy; acting as primary contact on any data protection queries; and approving responses to Right of Access requests (generally described in this document as 'Subject Access Requests');
• the DPO is also responsible for monitoring the completion of all mandatory training for all staff (with special emphasis on staff handling personal data on daily basis) and to ensure access to further guidance and support;
• Adults Move Lincolnshire CIC provides clear lines of reporting and an appropriate separation of duties to allow the DPO to supervise compliance with GDPR, reporting to the directors
• the DPO will conduct regular assurance activity to monitor and assess new processing of personal data;
• the DPO will monitor and report on all data processor requirements e.g. Roles & Responsibilities, notification, data subject access requests;
• the DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (employees, customers etc.).

Employee responsibilities

All employees have individual responsibility for complying with this policy and following accompanying guidance.

All employees will undertake relevant data protection training, including the Civil Service Learning 'Responsible for Information' training, and any other training that shall be deemed as mandatory.
Employees will:
• observe all forms of guidance, codes of practice and procedures about the collection, sharing, handling and use of personal information;

• develop a comprehensive understanding of the purpose for whichAdults Move Lincolnshire CIC uses personal information;
• collect and process information in accordance with the purpose for which it is required to be used by Adults Move Lincolnshire CIC to meet its statutory requirements and business needs;
• ensure the information is destroyed when no longer required in line with our information management guidance.
• upon receipt of a request by or on behalf of an individual for information held about them (Subject Access Request), staff will refer requests to the Information and Security Compliance Team as quickly as possible so that the request can be acted on quickly and legal advice sought if required.
• understand that breaches of this policy may result in scrutiny by the Information Commissioner's Office (ICO) with the potential for fines to be levied and accompanying reputational damage. There is also the potential for misconduct action.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be carried out if a project or the introduction of a new service or policy is likely to result in a high risk to the privacy of individuals. A DPIA is a process that helps identify privacy risks and ensure lawful practice when a new project is designed, or changes are made to an existing service or policy.

The purpose of the DPIA is to ensure that privacy risks are mitigated including promptly addressing any identified issue while allowing the aims of the project or policy to be met whenever possible.

According to the Information Commissioner's Office, a DPIA is required when an organisation plans to:
• embark on a new project involving the use of personal data;
• introduce new IT systems for storing and accessing personal information;
• participate in a new data-sharing initiative with other organisations;
• use profiling or special category data to decide on access to services;
• initiate actions based on a policy of identifying particular demographics;
• use existing data for a new and unexpected or more intrusive purpose;
• match data or combine datasets from different sources;
• collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
• profile children or target services at them; or
• process data that might endanger the individual's physical health or safety in the event of a security breach;
• continue to utilise long standing databases where the DPIA may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues. \

Data Protection by Design and Default

In compliance with data protection by design principle, we will ensure data protection risks are taken into account throughout the process of designing a new process, product, policy or services, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processing complies with the law and protects the rights of the data subjects.

To comply with data protection by design and by default principles, we will ensure mechanisms are in place within the organisation to ensure that, by default, only personal data which are necessary for each specific purpose are

processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

Breach Notification and Reporting

We must report any losses or suspected breaches of personal data to the Information Commissioner within 72 hours of becoming aware of the breach.
When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we are required by law to notify the affected individuals without undue delay.
If you discover or suspect a breach of data protection rule, loss or compromising of personal data, you must report it immediately to Rebecca Loveridge adultsmove@gmail.com. The data breach reporting form is included as an annex at the end of this policy document.

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work.
Personal data should not be shared without adherence to relevant guidance. When access to confidential information is required, employees can request it from their line managers.
Adults Move Lincolnshire CIC 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.
Strong passwords must be used, and they should never be shared.
Personal data should, under no circumstances, be disclosed to unauthorised individuals, either within the department or externally.
Data should be regularly reviewed 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 Data Protection Officer -Rebeca Loveridge- 07833606051- if they are unsure about any aspect of Data Protection.

Data Storage

This policy document describes how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see/access it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
• when not required, sensitive paper or files should be kept in a locked drawer or filing cabinet;
• employees should make sure sensitive paper and printouts are not left where unauthorised people could see them, for example on a printer or unattended on a desktop:
• sensitive data printouts should be shredded and disposed of securely when no longer required;
• all Adults Move Lincolnshire CICI's information should be handled in line with the acceptable use of ICT Policy
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.
• if data is stored on removable media (e.g. CDs or data sticks), these should be kept locked away securely when not being used.
• data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing 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 regularly tested.
• Adults Move Lincolnshire CIC's Data should under no circumstances be saved directly to personal laptops or other mobile devices such as tablets or smart phones.
• all servers and computers containing data should be adequately protected in line with NCSC principles and the Cabinet Office issued Baseline Security Standards.

Data Accuracy

The law requires Adults Move Lincolnshire CIC' to take reasonable steps to ensure data is kept accurate and up to date. It is incumbent upon Adults Move Lincolnshire CIC to ensure personal data held and processed is accurate and to ensure it continues to be accurate. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
Adults Move Lincolnshire CIC will make it easy for data subjects to update the information Adults Move Lincolnshire CIC holds about them.
Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
Where additional data sets are required the Information and Security Compliance Team should be engaged to ensure this is reflected on the Department's Information Asset Register.

Right of Access Request / Subject Access Request

All individuals who are the subject of personal data held by Adults Move Lincolnshire CIC are entitled to:
• ask what information the organisation holds about them, how it is used and why;
• ask how to gain access to it;
• be informed how to keep it up to date;
• be informed how the organisation is meeting its data protection obligations.
A request for access to personal information held by Adutls Move Lincolnshire (known as Right of Access Request or a Subject Access Request) must be responded to within one calendar month.
Providing Information
Adults Move Lincolnshire CIC aims to ensure that individuals are aware that their data is being processed, and that they understand:
• how the data is being used; • who it is shared with;
• how long it is kept for; • how to exercise their rights.

To these ends, Adults Move Lincolnshire CIC has a privacy statement; setting out how data relating to individuals is used by the organisation.

Monitoring, Review and Evaluation

The Directors will monitor the companies approach to data protection and associated rights.This policy will be reconsidered against any legislative changes and reviewed on an annual basis.

Dated:11.01.2024

References, legislation and guidance

- The General Data Protection Regulation (2016)
- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Adults Move Lincolnshire CIC's Privacy Statement (below)

Adults Move Lincolnshire CIC Privacy Statement

Adults Move Lincolnshire takes the security of your personal information very seriously. Our online services (www.adultsmovelincolnshire.com) is powered by Wix, who have their own GDPR which is approved and adopted by the EU. The information you provide us may include your name, email address, phone number, address, medical conditions and payment details. With this information, Adults Move Lincolnshire will only contact you about the service you have purchased and other activities we provide. You have a right to access the personal information you have provided us with and you may ask us to delete it at any time. This can be done via email adultsmove@gmail.com.

Dated:11.01.2024

ADULTS MOVE LINCOLNSHIRE

General Data Protection Regulation (GDPR) Incident Report Form

Time and Date breach was identified	
Description of the Data Breach	
Who is reporting the breach: Name/Post/School	
Contact details: Telephone/Email	
Classification of data breached (in accordance with Trusts Security Policy) i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	

Email form to the DPO and advise that a Data Security Breach report form is being sent.

Received by:	
Date/Time:	