Access Anyone Ltd. Data Protection Policy

Access Anyone Ltd is fully committed to compliance with the requirements of the Data Protection Act 2018. The company will therefore follow procedures which aim to ensure that all employees and directors who have access to any personal data held by or on behalf of the company are fully aware of and abide by their duties under the Data Protection Act 1998 (DPA) and GDPR.

Statement of Policy

The company needs to collect and use information about people with whom it works in order to operate and run the business. These may include current, past and prospective employees, customers and suppliers. In addition, the company may be required by law to collect and use information in order to comply with the requirements or guidance laid out in legislation. This personal information must be handled, used and dealt with properly whether it is on paper, in computer records or recorded by other means.

Access Anyone Ltd regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the company and those with whom it carries out business. The company therefore fully endorses and adheres to the Principles of the DPA and GDPR.

The Principles of Data Protection

Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the DPA, with added detail at certain points and a new accountability requirement. The GDPR requires you to show how you comply with the principles.

GDPR requires that personal data shall be;

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;
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.

In addition, the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as data relating to a living individual who can be identified from:

* That data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual. GDPR’s definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address, email address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA’s definition and could include chronologically ordered sets of manual records containing personal data.

Sensitive personal data is defined as personal data consisting of information as to:

* Racial or ethnic origin
* Political opinion
* Religious or other beliefs
* Trade union membership
* Physical or mental health or condition
* Sexual life
* Criminal proceedings or convictions

Why the Policy exists

This data protection policy ensures Access Anyone Ltd;

* Complies with data protection law and follows good practice
* Protects the rights of staff, customers, suppliers and partners
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of a breach of data

Policy Scope

This policy applies to;

* The Head Office of the Access Anyone Ltd
* All companies under the umbrella of Access Anyone Ltd
* All staff and volunteers of Access Anyone Ltd
* All contractors, suppliers and other people working on the behalf of Access Anyone Ltd

It applies to all data that the company holds relating to identifiable individuals, even if the information technically falls outside the scope of the Data Protection Act 2018. This can include;

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* …plus any other information relating to individuals

Data protection Risk

This policy helps to protect Access Anyone Ltd from data security risks including;

* **Breaches of confidentiality**, i.e. information being given out inappropriately
* **Failing to offer choice**, i.e. all individuals should be free to choose how the company uses data relating to them.
* **Reputational damage**, i.e. the company could suffer if hackers successfully gained access to sensitive data.

Responsibility and Accountability

Everyone who works for or with Access Anyone Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility;

* The **Directors** are ultimately responsible for ensuring that Access Anyone Ltd meets its legal obligations.
* The **Directors** are responsible for;
* Keeping the other Directors update about data protection responsibilities, risks and issues.
* Reviewing all data protection procedures and related polices
* Arranging data protection training and advice for the people covered in this policy.
* Handling data protection questions from staff and anyone else covered in this policy
* Dealing with requests from individuals to see the data Access Anyone Ltd holds about them.
* Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* Reviewing the Data Protection Policy annually or when deemed appropriate to ensure compliance with new legislation and best practice.
* Update the Data Protection Policy when new security measures have been introduced.
* Removal of ex-employee details from Access Anyone Ltd ICT systems that grant access to personal data.
* Overseeing the setting up of new employees with access requirements to personal data.
* Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
* Performing regular checks and scans to ensure security hardware and software is functioning properly.
* The **Finance Team** is responsible for;
* Collecting, filing and safeguarding of personal information on employees.
* Archiving personnel and financial files in accordance will the relevant legislation.
* Ensuring the safe destruction of personnel and financial files in accordance with the legal timeframe.
* Processing employee requests for viewing/copying their personal information.
* Updating employee, customer and supplier information on the accounting and payroll software packages and deleting personal data that is no longer appropriate or required by law.
* Updating and managing the Sage Accounting system when information is no longer appropriate. The GDPR applies the same principles to sole traders and partnerships. Suppliers and customers will be made removed from Sage after the end of seven complete financial years.
* Informing the Head of Finance and HR when new employees start in order that data protection training will be conducted in the induction process.
* To update employee personnel records when employees have completed the data protection training.
* Setting up access rights to systems with access to personal data.

General Staff Guidelines

* The only people able to access data covered in this policy should be those who need it for their work.
* Data should not be shared informally. When access to confidential information is required employees can request it from the Directors.
* Access Anyone Ltd will provide support/training to all employees to help them understand their responsibilities when handling data.
* Employees should keep all data secure, by taking sensible precautions and follow instructions held within this policy.
* Each employee is to ensure their login details are never shared and passwords are strong. A strong password uses letters, upper and lower case, numbers and special characters. Never use names that are widely known to be related to you.
* ANY personal data should not be disclosed to unauthorised people, either within or external to the company.
* Data should be regularly reviewed and updated appropriately. If the data is no longer required by law or deemed useful, it must be destroyed by the appropriate means. If a user is unsure check with a director.

Data Storage

When data is stored on paper, it must be kept in a secure place where unauthorised people cannot see or access it. Data print outs must not be left unattended on a printer or on a desk where unauthorised people can see them. Data stored on paper must be destroyed securely when no longer appropriate or required by law.

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

* Computers that can access data must be protected by strong passwords that can be changed and never shared between employees.
* If data is stored on a removable media device, these should always be locked away securely when not be used. Where possible data encryption should be used.
* Data should only be stored on designated drivers and servers, and should only be uploaded to an approved cloud based service; this being the Company’s Office 365.
* Stored cloud based data that is no longer relevant or required by law must be deleted appropriately.
* Data is backed up daily on to company servers, data stored on removable media is encrypted.
* All servers and computers containing data are protected by approved Anti Virus and Firewalls. These are kept up to data with patches.

Data Usage

Personal data is of no value to Access Anyone Ltd unless the business can make use of it. However, it is when the personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

* When working with personal data, employees should ensure that their computer screen is locked when away from their desk.
* Personal data should not be shared informally.
* Data must be encrypted if transferring electronically.
* Personal data must never be transferred outside the EU.

Marketing Data Usage

Access Anyone Ltd may in the future process data under the following guidelines;

* Data will not be shared with any third party, other than a marketing company under our contract.
* Only specific users will have access to pulled data.
* Data spreadsheets must be password protected.
* Data will only be used for the purpose opted by the customer, e.g. Customers can select to receive marketing material.

Data Accuracy

The law requires Access Anyone Ltd to take reasonable steps to ensure data is kept accurate and up to date. It is the also responsibility of the employees who work with the data to make sure it is accurate and up to date.

* 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 the data is updated. For instance, confirming customer details when contacted.
* Access Anyone Ltd will make it easy for the data subjects to update the information Access Anyone Ltd holds about them. Personal data updates by employees can be made anytime through the Finance Team.
* Data will be updated as and when any inaccuracies are discovered. For instance, if a customer can no longer be contacted on a telephone number or an email bounces back as undelivered. The inaccurate data will be removed from the databases.
* It is the Marketing Managers’ responsibility to ensure the marketing database is checked regularly and updated as appropriate.

Data Legal Requirements

Access Anyone Ltd will not keep data longer than is necessary and will destroy it by an appropriate means.

Access Anyone Ltd is legally bound to keep subject data for certain periods of time. The legal requirements are;

* **Payroll Information** – HMRC recommend that the following records must be kept for a minimum of 3 years;
* What you pay your employees and the deductions you make
* Reports and payments you make to HMRC.
* Employee leave and sickness absences
* Tax code notices
* Taxable expenses and benefits
* Payroll Giving Scheme documents, including the agency contract and employment authorisation forms.

Access Anyone Ltd will keep the paper copies of holiday, sickness and HMRC correspondence in the employees personnel file. This data will fall under the time frame of Personnel Records. Data kept on Sage Payroll will is now combined with the Sage Pension’s module. This means that employee data on Sage Payroll will be deleted 6 years after termination.

* Pension Information – 6 Years. The Pensions regulator stipulates that the following information must be kept for 6 years;
* Pension members name, DOB, NI number, gross earnings, contributions payable and date of contributions.
* Automatic enrolment date, opt in notice and the contribution the member is entitled to.
* The date the employee became an active member in the scheme.
* Joining notice.
* Postponement details including name, NI number, date the employee was sent the postponement notice.
* Opt out notice.
* Personnel Records – ACAS recommends to keep personnel records for a minimum period of 6 years after the termination of an employee. Access Anyone Ltd will destroy appropriately personnel files 6 years from the end of the company’s financial year of all terminated employees.

Individual’s Rights

The GDPR includes the following rights for individuals:

* The right to be informed - encompasses Access Anyone Ltd obligation to provide ‘fair processing information’, through its privacy notice (appendices 1). It emphasises the need for transparency over how Access Anyone Ltd uses personal data.
* The right of access - Under the GDPR, individuals will have the right to obtain:
* confirmation that their data is being processed;
* access to their personal data;
* and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice
* The right to rectification - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Access Anyone Ltd **must respond within one month**. This can be extended by two months where the request for rectification is complex.
* The right to erasure - also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
* The right to restrict processing - when processing is restricted, Access Anyone Ltd is permitted to store the personal data, but not to further process it. Access Anyone Ltd can retain just enough information about the individual to ensure that the restriction is respected in future.
* The right to data portability - allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Access Anyone Ltd must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files.
* The right to object – Individuals have the right to object to:
* processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
* direct marketing (including profiling);
* processing for purposes of scientific/historical research and statistics.

Access Anyone Ltd will stop processing data unless it has a legal obligation to continue.

* The right not to be subject to automated decision-making including profiling - GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Access Anyone Ltd will ensure all electronic data capture in principle is opt-in rather that out-out.

Subject Access Requests

All individuals who are the subject of personal data held by Access Anyone Ltd are entitled to;

* Ask what information the company holds about them and why.
* Ask how to gain access to it.
* Be informed how to keep it up to date.
* Be informed how the company is meeting its data protection obligations.

If an individual contacts Access Anyone Ltd requesting this information, this is called a Subject Access Request.

Subject access requests from individuals should be made by email addressed to the Directors. The data controller can supply a standard request form. Although individuals do not have to use this.

Unless the subject access request is manifestly unfounded or excessive there will be no charge for complying. The data controller will provide the relevant data within one month.

The data controller will verify the identity of anyone making a subject access request before handing over any information. If the requested is refused, the individual must be told why and that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

Disclosing Data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstance, Access Anyone Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Directors and company’s legal advisors where necessary.

Providing Information

Access Anyone Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand;

* How the data is being used
* How to exercise their rights

To this end, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available upon request and a version is also available on the company’s website.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

**What information must a breach notification contain?**

* The nature of the personal data breach including, where possible:
	+ the categories and approximate number of individuals concerned; and
	+ the categories and approximate number of personal data records concerned;
* The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
* A description of the likely consequences of the personal data breach; and
* A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

**How do I notify a breach?**

* A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.
* If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.