Dynamic Access Solutions LTD

DATA PROTECTION POLICY

Introduction

We have a requirement to request, use and retain personal data in order to carry out our business and provide employment to staff to enable us to carry out and supply installations, products and services in order to fulfil our contractual and legal obligations. This personal information must be collected and dealt with appropriately- whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the General Data Protection Register 25 May 2018 (GDPR).

The following list below of definitions of the technical terms we have used and is intended to aid understanding of this policy.

Data Controller - The person who (either alone or with others) decides what personal information Dynamic Access Solutions Ltd will hold and how it will be held or used.

GDPR May 2018 - The European legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer - The person(s) responsible for ensuring that it follows its data protection policy and complies with GDPR.

Data Subject/Service User - The individual whose personal information is being held or processed by Dynamic Access Solutions Ltd (for example: a client, an employee, a supporter)

Explicit consent - is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data.

* See definition

Notification -Notifying the Information Commissioner about the data processing activities Dynamic Access Solutions Ltd as certain activities may be exempt from notification.

Information Commissioner - The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing - means collecting, amending, handling, storing or disclosing personal information.

Personal Information - Information about living individuals that enables them to be identified - e.g. name, address, email address, contact telephone number. This also applies to information collected from customers, employees of organisations, companies and agencies and applies to named persons, such as individual volunteers or employees within Dynamic Access Solutions Ltd.

Sensitive data - means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual orientation
- Criminal record
- Criminal proceedings relating to a data subject's offences

Data Controller:

Dynamic Access Solutions Ltd is the Data Controller under GDPR, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying (if required to do so) the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Disclosure:

Dynamic Access Solutions Ltd may be required under compliance to legal obligations, to share data with other organizations such as HMRC, and Local Authority Departments or Institutions.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Dynamic Access Solutions Ltd to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State.
2. Protecting vital interests of a Data Subject or other person.
3. The Data Subject has already made the information public.
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion.
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Dynamic Access Solutions Ltd regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those we deal with.

Dynamic Access Solutions Ltd intends to ensure that personal information is treated lawfully and correctly. To this end Dynamic Access Solutions Ltd will adhere to the Principles of Data Protection, as detailed in the General Data Protection Register 25 May 2018.

Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under GDPR
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Dynamic Access Solutions Ltd will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil and necessitate its contractual and operational needs or to comply with any legal requirements,
- Ensure the quality of information used,

Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:

- The right to be informed that processing is being undertaken,
- The right of access to one's personal information
- The right to prevent processing in certain circumstances and
- The right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

Data collection:

Dynamic Access Solutions Ltd will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person verbally over the telephone or electronically via email or by completing a form.

When collecting data, Dynamic Access Solutions Ltd will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Data Storage:

Information and records relating to customers, suppliers and employees will be stored securely by Dynamic Access Solutions appointed Data Protection Officer and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is Dynamic Access Solutions Ltd's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy:

All Data Subjects have the right to access the information Dynamic Access Solutions Ltd holds about them. Dynamic Access Solutions Ltd will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, Dynamic Access Solutions Ltd will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with GDPR.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal information is appropriately trained to do so,
- Everyone processing personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows what to do and, in all cases, directs the enquiry to our Data Protection Officer,
- It deals promptly and courteously with any enquiries about handling personal information,
- It describes clearly how it handles personal information,
- It will regularly review and audit the ways it holds, manage and use personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy will lead to disciplinary action being taken against them.

Personal Data Breaches

We have a duty to report certain type of personal data breach to the relevant supervisory authority and this must be done within 72 hours of becoming aware of the breach where feasible.
If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay.
We will keep a record of any personal data breaches, regardless of whether we are required to notify or report.
We consider that a personal data breach can be broadly defined as a security incident that may affect confidentiality, integrity and availability of personal data which could include:

- Access by an unauthorised person
- Deliberate or accidental action by a controller or processor
- Sending personal data to an incorrect recipient

- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Our staff know how to escalate a security incident to the appropriate person and we keep a register of breaches, reportable or not.

Accessing Your Own Personal Data:

1. You have the right to ask for a copy of any of your personal Data held by Dynamic Access Solutions LTD.
2. Upon request and within 30 days of your application, we may provide you with a copy of the personal data which we hold about you (in return for a small fee). Please address requests to : datacomplianceofficer@eloqsecurity.com and insert "Personal Data Access" as the subject heading, or alternatively write to us – The Data Compliance Officer, Dynamic Access Solutions Limited, 6 Whisby Way, Lincoln, LN6 3LQ.
3. If you do not receive a response to your enquiry - or if you feel your enquiry has not been satisfactorily addressed, you can contact ICO directly:

The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 01625 545700
Fax: 01625 524510
Website: www.dataprotection.gov.uk
Email: mail@dataprotection.gov.uk

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR 25 May 2018
In case of any queries or questions in relation to this policy please contact the Dynamic Access Solutions Ltd.

Data Protection Officer:
Jason Healy
Managing Director
Data Protection Officer