DATA PROTECTION POLICY

Axis Group Integrated Services Limited
361-373 City Road
London
EC1V 1LR
Incorporating:
Axis Security Services Ltd
Acuity
Axis Cleaning & Support Services Ltd
Axis Academy

June 2018

DATA PROTECTION POLICY

There may be occasions when the Company needs to collect, store and use personal data about people including past, present and prospective consignees and sub-contractors in order to continue with its business and effectively meet its customers' requirements.

The proper and lawful processing of personal data is very important to maintaining our customers' faith and confidence in our operation and ability to meet their expectations.

Everyone at the Company has an important role to play in ensuring that personal data is processed lawfully and fairly. For the avoidance of doubt, processing includes the storing and retention of personal information.

Personal data means any information relating to a living individual who can be identified (in other words - not companies) directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

We hold personal information about all sorts of people we deal with including employees and sub-contractors.

All personal information must be dealt with correctly and appropriately no matter how it is collected, recorded and used – no matter whether on paper, in a computer / electronically or on other material. This must be in accordance with the provisions of the European Union General Data Protection Regulation ('GDPR').

Every employee has a duty to be aware of the regulations' principles in order to ensure that the Company effectively complies with the law on data protection.

Any personal data which we collect, record or use in any way, whether it is held on paper, on computer or other media, will have appropriate safeguards applied to it to ensure that we comply with GDPR.

We fully endorse and adhere to the principles of data protection contained within GDPR.

The eight principles are as follows:

1. Personal data shall be processed fairly and lawfully with the Data Subject's consent. Additional, specific conditions may be required for processing to be undertaken, especially in relation to special categories of data and children.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act (see further details below).
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data 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 freedom of data subjects in relation to the processing of personal data.

To ensure that the requirements of the principles are adhered to, the Company will:

1. Ensure that the policy and guidelines on the collection and processing of personal data are lawful and undertaken for legitimate purposes, published, clear and up to date

2. Ensure all employees and clients, whose personal data the Company collects, have given their consent and this is recorded and stored.

3. Ensure all employees and clients have the ability to rectify their own personal data as well as ensuring that there is a clear and easy process for individuals to withdraw their consent, request the right of erasure or object to the processing of their personal data.

4. Ensure that all employees managing and handling personal information are trained appropriately, including the updating and issuing of all Privacy Notices.

5. Ensure that everyone in the Company managing and handling personal information is supervised appropriately.

6. Produce a framework detailing the holding period for types of personal data and ensure that this is enacted in the business.

7. Ensure that anyone in the Company who does not normally handle personal information knows what to do if the occasion arises.

8. Work with clients to assess that it is clearly understood and documented who is responsible for all aspects of personal data compliance that may be created and/or managed at a client site.

9. Work with clients to assess where an impact assessment is necessary where there is potential for high risk to a data subjects rights.

10. Ensure that subject access requests and queries about personal information are dealt with within one month where the request and task is reasonable.

11. Ensure that incidents involving breaches of this policy are recorded, analysed, and disciplinary action taken as appropriate. This will also involve notifying the Data Subject affected and considering whether a notification to the UK Information Commissioners Office is required. All efforts will be made to ensure data breaches are informed to the relevant parties within 72 hours.

12. Provide a clear route for ensuring that all staff know how to identify and notify Management of a Data Subject Request.

13. Track all data requests so that, where possible, they can be responded to within a one month timeframe.

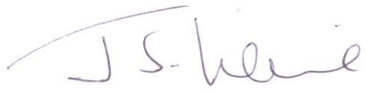
14. Review where and how data is stored by all data processors working on behalf of the Company involving personal data being processed to ensure compliance with GDPR.

15. Integrate this policy with other corporate policies associated with data protection.

16. Review this policy regularly and updated when necessary.

Where we collect any special categories of personal data, we will take appropriate steps to ensure that we have explicit consent to hold, use and retain the information. This may include data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

The Company follows an ethical marketing practice and does not give details of customers, suppliers or sub-contractors without their explicit consent.



Jonathan Levine
Axis Group Integrated Services Ltd

Dated: **June 2018**
Review Date: **November 2019**