General Data Protection Regulation (GDPR) Policy

In exercise of the right granted to Axis International Security Services (Ltd) **ICO certificate number (Z3307235)** applies under the terms of the **General Data Protection Regulation Policy (GDPR)** The ultimate responsibility for Data Control for this company is with the Director, who has powers of delegation to suitably qualified staff to act on his/her behalf for specific matters of Data Protection.

In order to maintain fair and lawful activities within the **Data Protection Regulation Policy (GDPR)**, **Data** is defined as information which:

(a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose?

(b) Is recorded with the intention that it should be processed by means of such equipment,

(c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, **Data Protection Regulation (GDPR)**,

(e) Is recorded information held by a public authority and does not fall within any of paragraphs a, to d,

Paragraphs (a) and (b) make it clear that information that is held on computer, or is intended to be held on computer, is data. So, data is also information recorded on paper if you intend to put it on computer.

Relevant filing system (referred to in paragraph (c) of the definition) is defined in the regulations as:

Set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Accessible records were included in the definition of “data” because pre-existing access rights to information were not restricted to automatically processed records, or records held in non-automated systems falling within the definition of “relevant filing systems”. So, to preserve all these pre-existing access rights, the definition of “data” covers accessible records even if they do not fall in categories (a), (b), or (c).

The Freedom of Information Act 2000 created a new category of data which extended the definition of “data” in the **Data Protection Regulation Policy (GDPR)** to include any information held by a public authority which would not otherwise be caught by the definition. Where information requested under the FOI Act includes information about identifiable individuals, public authorities must consider whether its release would breach the **Data Protection Regulation Policy (GDPR)**.

This category of data (which is often referred to as “category (e) data”) is designed to ensure that before releasing any personal information under the FOI Act, public authorities consider whether this would be fair. Processing category (e) data is exempt from most of the rights and duties created by the **Data Protection Regulation Policy (GDPR)**.

Personal data means data which relate to a living individual who can be identified – (a) From those data, or (b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller officer (DCO) or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.

Example
An organisation holds data on any form of hardrive (memory stick, removable hardrive or fixed to a device, visual photographic, video or otherwise). The hardrive records do not identify individuals by name, but bear unique visual reference or which can be matched to other systems to identify the individuals concerned. The information held on the hardrive is therefore termed records of personal data.

Responsibility under the regulations applies throughout the period when anyone is processing personal data – as do the rights of individuals in respect of that personal data. So all must comply with the regulation from the moment the data is obtained until the time when the data has been returned, deleted or destroyed. Duties extend to the way personal data is disposed of when no longer needed to be kept – data must be disposed of securely and in a way which does not prejudice the interests of the individuals concerned. This disposal needs to be recorded in the event of any Subject Access Request (SAR) being made to this company.

Changes in an organisation circumstances do not reduce an individual’s rights under the regulation. Even if an organisation goes out of business, individuals are still entitled to expect that their personal data will be processed in accordance with the data protection principles. However, responsibility for ensuring this happens may shift, depending on the circumstances.

If any person intends to make an SAR, then within the auspice of the **General Data Protection Regulation (GDPR)**, this company has the following form that will be issued to an individual if making an SAR;