

Avco Systems Ltd – EU General Data Protection Regulation Compliance

(v1, Feb 2018)

The EU General Data Protection Regulation (GDPR) will enter into full effect on 25 May, 2018 and will strengthen and unify data protection for all individuals within the European Union (EU).

The main aim of the GDPR is to strengthen and increase the level of control and security of the information stored and processed by an organization. Furthermore, the regulation will ensure that the data controllers and processors are safe custodians of the data.

Avco Systems Ltd takes its obligations under the GDPR very seriously and believes itself already compliant with the legislation through its certification, since 2014, to the ISO/IEC 27001 information security standard. The company is committed to safeguarding its information, and that of its interested parties, from a wide range of threats, in order to ensure business continuity, minimize business risk and to comply with all contractual, legal and regulatory requirements.

The company has a strategy to mitigate information security risks as far as reasonably practicable. This is supported by a formal methodology whereby risks are identified and either accepted according to documented criteria, or reduced through the use of control measures. Action taken will be adequate and proportionate to the expected impact that the loss of confidentiality, integrity or availability may have on systems and their data.

The company has policies to ensure that events or weaknesses that might compromise information security are communicated in a way that ensures timely corrective action. Formal event notification and escalation procedures are supported by an Incident Response Plan and Disaster Recovery Plan, for use should a data breach occur; both are tested annually.

Data Privacy

Avco Systems Ltd is registered with the Information Commissioner's Office, registration Z5850276. The company has undertaken an internal impact assessment to identify and control its data and that of its interested parties: what data is held; the type of data and whether the company acts as controller or processor. There are formal processes for the protection of data throughout its lifecycle.

A Data Protection Officer has been appointed to ensure that the data is processed in line with the principles of the GDPR: lawful processing, individuals' rights, accountability and governance, and transfer of data. The company's Data Privacy Policy details processes whereby accountability and compliance are achieved.

