DATA PROTECTION ACT 2018

As of 25 May 2018, the Data Protection Act 2018 comes into effect. The legislation gives individual citizens more rights in regard to their personal data and organisations will be required to be more accountable about what they do with the information.

Recognising the potential conflict between individuals' rights and the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, special provisions have been made under the EU Law Enforcement Directive (LED).

Key requirements of the new legislation

- The definition of personal data is wider than previous data protection legislation, e.g. an online identifier (such as an IP address) can be personal data
- Individuals gain a number of rights including the 'right to be forgotten' and the right to restrict processing, plus an enhanced right of access to their own data - some of these rights are reduced or negating if the data is being processed for law enforcement purposes.
- There are some extra requirements about how operational data is recorded and shared:
  - **Fact or opinion**: it should be clear to the reader whether recorded information is based on fact or assessment / opinion.
  - **Categories of persons**: *where possible* the 'categories' of individuals should be made clear, e.g. suspect, victim, witness, other persons related to a crime.
  - **Logging**: IT Systems must keep logs of: any alterations to records, access to records, erasure and disclosures/sharing of records.
  - **Data quality**: when sharing data which may be of poor quality, the receiving body must be provided with information to allow them to assess the reliability of the data.

- Organisations must demonstrate how they comply with the legislation, in particular by providing comprehensive, clear and transparent privacy policies and maintaining records of their processing activities in an Information Asset Register (IAR)
- Data Security Breach reporting becomes mandatory and organisations must notify the Information Commissioner's Officer (ICO) within 72 hours of becoming aware of any incidents
- The maximum amount that organisations may be fined by the ICO for non-compliance increased to €20 million (approximately £17 million)
- Individuals can request access to information held about them (Right to Access Request) free of charge and the time organisations have to respond has been shortened from 40 days to one calendar month
- Organisations must obtain informed consent from individuals to process their data unless there is an alternative and appropriate lawful basis for doing so (e.g. law enforcement activity).
- The transfer of personal data outside of the EU (and other listed EU approved counties) will be subject to specific rules and safeguards to protect individuals' privacy.
- Where a decision is made by solely automated means that has a legal or significant effect and where special category data is being processed, it must be with consent or in the significant public interest. Where this involves processing of special category data for law enforcement purposes it may need to be authorised under domestic legislation.
- There must be a written contract between forces and third parties (Data Processors), engaged to use / process personal data on behalf of Sussex Police as they will now

assume some liability for complying with the Data Protection Act – this includes outsourced services, e.g. payroll, custody.

More information on the legislation can be found on the Information Commissioner's Office website:

- GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Law enforcement data processing [https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-bill/]