GDPR - Whats new?

- **NEW Increased Territorial Scope:** the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.

- **NEW Penalties:** Under GDPR organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). There is a tiered approach to fines e.g. an organisation can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning data stored within 'clouds' will not be exempt from GDPR enforcement.

- **NEW Consent:** The conditions for consent have been strengthened, the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

- **NEW Data Subject Rights:**

    - **Breach Notification**: breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals" and must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

    - **Right to Access**: the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects

    - **Right to be Forgotten**: the conditions for erasure, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

    - **Data Portability:** the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly used and machine readable format' and have the right to transmit that data to another controller.

    - **Privacy by Design:** At it's core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. 'The controller shall implement appropriate technical and organisational measure

in an effective way to protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

- **NEW Data Protection Officers:** A DPO has formal responsibility for data protection compliance within an organisation. The appointment of a DPO under the EU General Data Protection Regulation (GDPR) is only mandatory in three situations:
  - when the organisation is a public authority or body, or
  - when the organisation's core activities consist of either:
    i. Data processing operations that require regular and systematic monitoring of data subjects on a large scale; or
    ii. Large-scale processing of special categories of data (i.e. sensitive data such as health, religion, race, sexual orientation, etc.) and personal data relating to criminal convictions and offences.
- NPCC IM Lead, Commissioner Ian Dyson, has identified that DPO roles can be shared between organisations such as Police Forces and OPCC's.