The GDPR and Barnstaple u3a

The GDPR is the European Union's comprehensive data protection law that governs how personal data of individuals in the EU is collected, processed, and stored, ensuring privacy and security rights. Currently this still applies to us in the UK, despite Brexit.

Overview
The **General Data Protection Regulation (GDPR)**, formally known as Regulation (EU) 2016/679, came into effect on **May 25, 2018** across all EU member states to harmonize data privacy laws and strengthen individual rights regarding personal data. It applies not only to organizations within the EU but also to any entity worldwide that processes or targets data related to EU residents. The regulation replaced the earlier Data Protection Directive 95/46/EC and introduced stricter rules and higher penalties for non-compliance.

Key Principles
GDPR establishes several **core principles** for processing personal data:

- **Lawfulness, fairness, and transparency**: Data must be processed legally and transparently.
- **Purpose limitation**: Data should only be collected for specific, legitimate purposes.
- **Data minimization**: Only the necessary data should be collected.
- **Accuracy**: Personal data must be accurate and up to date.
- **Storage limitation**: Data should not be kept longer than necessary – 6 months after leaving the u3a
- **Integrity and confidentiality**: Data must be securely processed to prevent breaches.
- **Accountability**: Organizations must demonstrate compliance with GDPR principles.
- **Financial Records:** will be professionally shredded after 7 years back from the current April with GDPR certification.

.

Rights of Individuals
Under GDPR, individuals have **enhanced rights** over their personal data, including:

- Right of access: Individuals can request access to their data.
- Right to rectification: Correct inaccurate or incomplete data.
- Right to erasure ("right to be forgotten"): Request deletion of personal data under certain conditions.
- Right to restrict processing: Limit how data is used.
- Right to data portability: Receive data in a structured, machine-readable format.
- Right to object: Object to processing for marketing or other purposes.
- Rights related to automated decision-making and profiling: Safeguards against decisions made solely by automated processes.

.

Obligations for Organizations
Organizations processing personal data must:

- Obtain valid consent where required.
- Implement technical and organizational measures to protect data.
- Maintain records of processing activities.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing.
- Appoint a Data Protection Officer (DPO) if necessary.
- Report data breaches to authorities within 72 hours when feasible.

.

Enforcement and Penalties
GDPR enforcement is carried out by national data protection authorities in each EU member state. Non-compliance can result in substantial fines, up to €20 million or 4% of global annual turnover, whichever is higher. The regulation emphasizes accountability and encourages organizations to adopt privacy by design and by default.

GDPR still applies to publicly available information, which means the person or organisation sharing it needs to comply with data protection laws.

Lawful Bases for Processing Personal Data
Under GDPR, organisations must have a lawful basis for processing (which includes publishing) your personal data. This includes your explicit permission for your name, phone number and email address to be used so that u3a members can access your u3a Group activities.