# Legal obligations

Legal obligations for data protection typically include compliance with various laws and regulations designed to protect personal data.

1. General Data Protection Regulation (GDPR) In the UK, the GDPR is the primary legislation governing data protection. Key obligations under GDPR include:

Lawful Basis for Processing: Personal data must be processed lawfully, fairly, and transparently. Organisations must have a valid legal basis for processing data, such as consent, contractual necessity, or legal obligation1.

Data Subject Rights: Individuals have rights regarding their personal data, including the right to access, rectify, erase, restrict processing, and object to processing1.

Data Protection Principles: Organisations must adhere to principles such as data minimisation, accuracy, storage limitation, integrity, and confidentiality1.

Accountability and Governance: Organisations must implement appropriate technical and organisational measures to ensure compliance with data protection principles1.

2. Data Protection Act 2018 The Data Protection Act 2018 complements the GDPR and includes provisions specific to the UK. It outlines additional requirements and exemptions, such as:

Special Category Data: Additional protections for sensitive data, such as health information, racial or ethnic origin, and political opinions1.

Criminal Offence Data: Specific conditions for processing data related to criminal convictions and offences1.

3. Privacy and Electronic Communications Regulations (PECR) PECR governs electronic communications and includes rules on marketing, cookies, and electronic privacy. Key obligations include:

Consent for Marketing: Organisations must obtain consent before sending marketing communications via electronic means1.

Cookie Compliance: Organisations must inform users about the use of cookies and obtain consent1.

4. Data Breach Notification Organisations are required to notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of a data breach that poses a risk to individuals' rights and freedoms1. Affected individuals must also be informed if the breach is likely to result in a high risk to their rights and freedoms1.

5. Data Protection Impact Assessments (DPIAs) DPIAs are required for processing activities that are likely to result in high risks to individuals' privacy. This includes assessing the impact of data processing and implementing measures to mitigate risks1.

# Legal obligations

6. International Data Transfers When transferring personal data outside the UK, organisations must ensure that the destination country provides adequate protection for the data. This may involve using standard contractual clauses or other approved mechanisms1.

By adhering to these legal obligations, Girvan Bowling Club can ensure compliance with data protection laws and safeguard the privacy of its members and stakeholders.