## **Q1 – GDPR Compliance**

**Scenario:**  
 A women’s business networking club collects and stores personal data about members, including names, contact details, business information, and event attendance records. It plans to launch an online membership portal and wants to fully comply with GDPR.

### **Band 4 (10–12 marks)**

Implementing full GDPR compliance when launching the online membership portal is likely to benefit the networking club if managed properly. By ensuring clear consent mechanisms, secure storage, and transparent privacy notices, the club reduces the risk of regulatory fines and legal disputes. This legal compliance supports trust — members are more likely to share business and personal details when they feel their data is respected, which in turn helps the club personalise event invitations and networking opportunities. Robust GDPR processes also improve data quality, as inaccurate or outdated records are identified and corrected during compliance audits, enabling more effective communication. However, there are costs in legal advice, system configuration, and ongoing audits, which could be significant for a small club. Time spent on training volunteers and staff may delay the portal launch, and opt-out rights could reduce the marketing database. These drawbacks can be mitigated with phased rollout and by using affordable GDPR-compliant software. Overall, the benefits to trust, reputation, and legal protection outweigh the drawbacks if costs are planned for and staff engagement is high.

### **Band 3 (7–9 marks)**

Full GDPR compliance would protect the club from fines and help it demonstrate that members’ information is handled lawfully. Limiting data collection on the portal to only what is needed, such as names and emails, would help meet the principle of data minimisation. Providing a clear privacy notice would improve transparency and could make members more willing to use the portal. However, writing policies, configuring secure storage, and training volunteers could delay the launch and require budget. Consent rules may also mean fewer members agree to marketing emails, reducing event promotion reach. It is likely to be beneficial, but the club would need to plan the work to avoid excessive delays.

### **Band 2 (4–6 marks)**

Following GDPR would make the portal more secure by collecting only necessary details and telling members how their information will be used. This could help build some trust. But it would take time to set up new processes and train people, which might delay the launch. Fewer people might sign up for marketing, so promoting events could be harder. It should protect data but may slow things down.

### **Band 1 (1–3 marks)**

It keeps members’ data safe and shows them what it’s for. It might take time and cost money.

## **Q2 – Data Breach Response**

**Scenario:**  
 The women’s business networking club had a minor data breach when an email list with member contact details was sent to the wrong recipient. The club is considering stricter data access controls and staff training to prevent future breaches.

### **Band 4 (10–12 marks)**

Introducing stricter data access controls and staff training after a breach would address the club’s immediate GDPR risks. Limiting access to sensitive member data ensures only authorised individuals can handle contact lists, reducing the chance of accidental disclosure. Staff training on secure communication methods, such as using encrypted email and verifying recipient details, directly tackles the cause of the breach. This proactive approach demonstrates accountability to members and the regulator, helping restore trust and potentially preventing reputational harm. However, stricter controls could slow down legitimate event organisation if staff have to request access each time, and training costs may stretch the club’s budget. There’s also the risk of resistance from volunteers who see new controls as inconvenient. These drawbacks can be reduced by using role-based access systems that balance security with operational needs. Overall, the benefits of risk reduction and trust rebuilding outweigh operational delays if the changes are well-implemented and supported by leadership.

### **Band 3 (7–9 marks)**

Restricting who can see member contact lists would make mistakes like the recent breach less likely. Training staff to check recipients and use Bcc would improve security and help meet GDPR’s requirements for protecting personal data. This would reassure members that the club is handling information carefully. The main drawback is that planning events could take longer if staff need to request access, and training costs could be a challenge. Overall, it should improve security and confidence if controls are balanced with practical needs.

### **Band 2 (4–6 marks)**

Giving fewer people access to member lists would make it harder for the same mistake to happen again. Training could remind staff to send emails more carefully. But it might slow down event planning if people have to wait for access. It should help prevent problems but could make things less convenient.

### **Band 1 (1–3 marks)**

Fewer people can see the list so it’s safer. Training takes time.

## **Q3 – Outsourcing Data Management**

**Scenario:**  
 The women’s business networking club is considering outsourcing its member database to a GDPR-compliant cloud service provider to handle growth and ensure compliance.

### **Band 4 (10–12 marks)**

Outsourcing member database management to a GDPR-compliant cloud provider could improve the club’s data security and reduce administrative work. Professional providers typically use advanced security measures such as encryption, multi-factor authentication, and detailed audit logs, which may exceed what the club could achieve in-house. This also supports GDPR compliance by ensuring secure storage and documented processing agreements, freeing the club’s volunteers to focus on events and community building. Scalability means the club can handle membership growth without investing in its own infrastructure. However, outsourcing brings risks: the club loses direct control over data, and if the provider suffers a breach, the reputational impact still falls on the club. Subscription costs and long-term contracts may strain finances, and compliance must be monitored to ensure standards are maintained, especially if data is stored outside the UK. With strong contractual safeguards, regular audits, and a reputable provider, the benefits of efficiency and enhanced security outweigh the risks for the club.

### **Band 3 (7–9 marks)**

A GDPR-compliant cloud service could give the club better security and backups than it could run itself, helping with compliance and freeing time for organising events. A provider with good login security would reduce the risk of unauthorised access. However, there would be subscription costs and less control over where data is stored. If the provider had a problem, the club’s reputation could still be damaged. It would probably be a good choice if the provider is carefully selected.

### **Band 2 (4–6 marks)**

A cloud provider could keep member records safe and backed up so they’re not lost. This would save the club from running its own system. But it costs money and means trusting another company with the data. It could be good if the company is reliable.

### **Band 1 (1–3 marks)**

A cloud company stores the data safely. It costs money.