2. Security & Compliance

Why it matters:

We handle sensitive user and club data, so we need to protect it, follow the law, and make sure we're ready for problems before they happen. This avoids legal trouble, builds user trust, and reduces downtime.

What we should do:

- **Run regular security audits** to catch issues early and stay on top of any risks.
- **Use encryption** for data in transit and at rest, so data is protected at all stages.
- **Follow GDPR and legal requirements**, especially around data handling, user consent, and retention.
- **Manage secrets properly**, such as API keys, credentials, and tokens—using secure storage and limited access.
- **Plan for disaster recovery**, with strategies in place to restore service quickly in case of major failures.
- **Set up failover options** where needed, so services can stay online even if something breaks.

What we should take care of:

- **Security audits** Use tools like Microsoft Security Code Analysis in Azure DevOps or CodeQL to scan the code regularly, especially during CI/CD pipelines.
- **Encryption** Enforce HTTPS for all endpoints via Azure App Service or Azure Front Door. Store sensitive data using Azure SQL with Transparent Data Encryption (TDE) and optionally use Always Encrypted for highly sensitive fields. Key management via **Azure Key Vault**.
- **Secret and credential management** Store connection strings, API keys, and other secrets in **Azure Key Vault**. Access should be limited through **Azure Managed Identities**, so code doesn't store any credentials directly.
- **Compliance and GDPR** Azure provides built-in tooling for GDPR compliance (e.g. **Microsoft Purview** for data mapping and tracking). User data access and deletion endpoints should be built into our own services, following .NET naming and structure conventions.
- **Disaster recovery** Use **Azure Backup** for snapshots and long-term storage. Test recovery procedures regularly. For business-critical services, leverage **Azure Site Recovery** to keep downtime to a minimum.
- **Failover and high availability** Services can be hosted in Azure App Service Plans with **multi-region deployment**, backed by Azure Traffic Manager or Front Door for smart routing. Use **Azure SQL with Geo-Replication** or **Cosmos DB with multi-region write support** where applicable.