

	Completed	To Be Completed
Hire a Data Protection Officer (DPO)	External Resource : IT and Legal advisor to company(Article 37 GDPR)	Guidelines Checklists ISO 27001 Templates
Data Privacy Design & Assessment	<ul style="list-style-type: none"> - All data is being captured on a centralized portal which has MFA (Multi Factor Authentication) -The Data is being hosted in AWS using S3 buckets (encrypted) -Internal audits been done by IT team - AWS key management services (AWS KMS) 	Encryption in transit : -AWS CloudHSM (hardware security model)
Data Governance	People - Enterprise Architect Process- Documentation of software with coding standards Technology - Data capture on portals, stored in AWS DynamoDB	Configuration management guide with data flow maps.
Get consent for data collection, retention and erasure	The app is downloaded after agreeing to share data for health and wellness purpose of self	Expiration policy as requested by customer
Compliance, auditing & record keeping	Identity and Access Management policies (IAM) on AWS	AWS cloud watch configuration with metrics defined as per ISO audit
Data breach obligations	AWS policies for data handling with alarms for breach	Policy to notify regulators within 72 hrs and individual

		as per GDPR (Article 30)
Security of personal data	Hosted on server in own country -S3 buckets defined -Data on DynamoDB -IAM policies incorporated	AWS cloud watch services
Compliance enabling services	AWS IAM (Identity and Access Management) policies created	AWS Key Management Service
Compliant DPA (Data processing Addendum)	AWS online service terms	ISO-27001 compliance report yearly
Conformity with a code of conduct	AWS Management Console Configuration	AWS Artifact report post deployment