7. Security Safeguards

Section 2: Compliance Assessment Checklist

This section explains how Data for Change assesses whether its AI voice survey practices are supported by appropriate technical and organizational safeguards to protect personal data from security risks, unauthorized access, third-party misuse, and potential data breaches.

Risk Assessment

We assess risks to personal data by:

☐ Identifying where personal data is stored, processed, and transferred
☐ Mapping possible vulnerabilities, such as data breaches or unauthorized access
☐ Reviewing risks related to AI voice survey data
☐ Other: [specify]

Technical Controls

We implement the following technical controls:

☐ Encryption of sensitive data at rest
☐ Encryption of sensitive data in transit
☐ Secure servers
☐ Firewalls
☐ Access controls, such as passwords or multi-factor authentication
☐ Regular system updates and security patches
☐ Other: [specify]

Organizational Controls

We implement the following organizational controls:

☐ Limit data access to authorized staff only
☐ Apply role-based access control
☐ Train employees on data protection and security practices
☐ Establish internal data protection policies
☐ Other: [specify]

Monitoring and Review

We monitor and review security safeguards through:

☐ Regular security audits
☐ Security testing
☐ Continuous updates based on new risks
☐ Documentation of security measures
☐ Other: [specify]

Third-Party Risk Management

We manage third-party risks by:

☐ Assessing whether partners or processors apply adequate safeguards
☐ Using contracts to enforce data protection obligations
☐ Reviewing third-party access to personal data
☐ Other: [specify]

Data Breach Preparedness

We prepare for potential data breaches by:

☐ Establishing incident response procedures
☐ Assigning responsibility for breach response
☐ Preparing to notify regulators where required
☐ Preparing to notify affected individuals where required
☐ Other: [specify]