GDPR Data Protection Policy

To ensure that Text-Connect shall at all times remain fully compliant with the requirements of the General Data Protection Regulation, also known as "GDPR" and the UK's Data Protection Act 2018. To ensure that Text-Connect is properly undertaking the activities and implementing the controls required by GDPR, and that full and accurate data protection records are created and maintained to demonstrate compliance.

Key GDPR Definitions

Personal Data refers to information about a living individual, which means that they can be identified (a) from that data, or (b) from that data and any other information which is, or could in the future, come into the possession of the data controller. Also see Special Categories of Personal Data.

Special Categories of Personal Data (also known as Sensitive Personal Data) refers to a specific sub-group of Personal Data, which comprises an individual's

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- physical or mental health
- sexual preferences or activities
- biometric or genetic data

Data Controller refers to the person, organisation, public authority, agency or other body who, either alone or with others, determines the purposes for which and the manner in which any personal data is to be processed, and defines the controls required for such Processing.

Data Processor refers to any person or organisation (other than an employee of the Data Controller) who undertakes the Processing of personal data on behalf of the Data Controller.

Processing refers to any operation which is performed upon or applied to personal data, whether undertaken manually or by automated means, including its acquisition, organisation, storage, retrieval, consultation, amendment, availability, disclosure, erasure or destruction.

Data Subject refers to an individual who is the subject of personal data.

Data Subject Consent refers to the Data Subject's approval or agreement for an activity to take place, having given consideration to the benefits and risks of the activity. For consent to be valid, the data subject needs to be informed, have the capacity and knowledge to make a decision, and to have given their consent voluntarily. Specific requirements need to be met in connection with the consent which is given by Children, including validating parental consent and the age of the Child.

Child refers to a data subject who is under 16 years of age, and for those under 13 years of age processing is only lawful if parent or guardian Consent has been obtained.

Supervisory Authority refers to the national data protection authority of each EEA country, responsible for enforcing GDPR within their own nation. The Supervisory Authority is also the reporting point for data breach notifications, for conducting investigations, and for issuing administrative penalties in accordance with the requirements of GDPR. Within the UK, the Supervisory Authority is the Information Commissioner's Office.

Our Scope

This Data Protection Policy shall:

- Apply to all Text-Connect activities which related to the Processing of Personal Data, either as Data Controller, or as Data Processor acting under the lawful instructions of a third party.
- Shall apply to all ways in which Personal Data is acquired, received, processed, stored, amended, disclosed and erased by Text-Connect. This shall include Company data, as well as personal data owned by an external organisation, and entrusted to the Company under a contract which specifically communicates data protection requirements.
- Ensure that the rights of Data Subjects under GDPR are upheld by Text-Connect.
- Be communicated to all employees, contractors, third party user, external Data Processors, and any other organisation or individual with a bona-fide need to access Personal Data held by or entrusted to Text-Connect.

Our Policy Statement

In order to fully comply with GDPR, Text-Connect shall:

- Keep all personal information (including employee information) secure, regardless of its format or category, or the process or activities which use it, so as to prevent accidental or unauthorised loss, theft or breach.
- Maintain a full and accurate inventory of all personal data which is under its control.
- Provide regular data protection training to all personnel and third parties who are engaged in delivering any activity which involves the processing of personal data.
- Provide specific data protection training for those employees with specific GDPR responsibilities, including Senior Management and the organisation's Data Protection Officer.
- Ensure that all data processing activities are subject to full and accurate Privacy Impact Assessments, and promptly acting to remediate the findings of such assessments.
- Ensure that personal data processing activities are afforded suitable protection by conducting risk assessments of the physical, technical and personnel elements of the activity.
- Validate that personal data is afforded the protection which is documented with the Company's Acceptable Use Policy and Access Control Policy.
- Only process personal data for legitimate business purposes, and in accordance with the Privacy Impact Assessment which has been prepared to cover that purpose.

- Ensure that all personal information is properly returned or effectively deleted or destroyed when it is no longer required, in accordance with supporting Privacy Impact Assessments.
- Implement a suitable mechanism and supporting records for recording data subject consent for the processing of their personal data, and using these records as a reference point when deciding how personal data is to be processed.
- Clearly communicate to data subjects how their personal data is to be processed, where it is to be transferred to (if applicable), and their rights as data subjects.
- Maintain clear and concise Privacy Notices, and related information for data subjects.
- Ensure that third parties involved in personal data processing activities understand this Policy and related GDPR documentation, and can evidence their own levels of GDPR compliance.
- Ensure that effective processes, technical controls and competent resources are in place to undertake tasks promptly and diligently related to delivering the rights of data subjects.
- Implement effective processes and monitoring controls to provide protection for personal data, and to detect any loss, theft or data breaches.
- Authorise any off-site or off-shore processing of personal data before being approved, and updating and reissuing the corresponding Privacy Impact Assessment.
- Undertake to promptly report any actual or suspected data breaches to the Supervisory Authority within the required time frames, and to communicate the breach to affected data subjects.
- Willingly and fully co-operate with any investigations into data breaches as may be required by the Supervisory Authority or similar legislative function.

This Text-Connect Data Protection Policy was reviewed and updated on 20th March 2024. You are advised to download or print a copy and retain it for your records.