Telesis Ltd Data Protection Statement

Telesis Limited and all its associated companies are compliant with the data protection regulations and Data Protection Act. We continually monitor and update our processes where required, particularly in the face of future changes to data protection legislation that will be in force from 25th May 2018. As part of the various services and products we offer our customers, and this includes system maintenance, we may hold or have access to data that can identify individuals in order to be able to provide our customers with the services, products and support that is agreed through our contracts. In all instances, access to such data is controlled and limited to specific individuals.

Processing Information

Scope and purpose or processing

Personal data is held for the purposes of the provision of telecommunication services and related products. The personal data held is obtained in support of contractual arrangements and is necessary under the 'legitimate interests' pursued by the controller (Telesis Limited) as defined in article 6.1 of the GDPR. The facility to opt out of marketing communications remains but excludes operational or pricing communications.

Nature of processing

Telesis Limited does not undertake any automated decision making as defined by article 22 of the GDPR. Data will be processed internally by the marketing department for the purposes of objective and permission-based marketing.

Duration of processing

Telesis Limited will maintain personal data for the duration of contracts during the provision of telecommunication services and products. Thereafter, the data will be held for a 'reasonable' period, depending on the nature of the relationship with the customer. The data will be deleted when the retention of that data can no longer be justified under the provisions of the Data Protection Act and is not overruled by competing legislation or regulations.

Types of Personal Data

The personal data held will include: Name, Position, Telephone Number(s), email address.

No 'sensitive data' (as defined by the Data Protection Act) or 'special categories of personal data' (as defined by the GDPR) are held against any existing or former customers.

Categories of Data Subject

The data subjects whose data may be held by Telesis Limited is restricted to that of existing, former or prospective (wholesale only) customers and associated contacts. These data fall under the category of 'personal data' and do not include any 'sensitive data' (as defined by the Data Protection Act) or 'special categories of personal data' (as defined by the GDPR).

Data sharing

There is no routine data sharing of person identifiable data. Where exceptions exist, these concern the management of systems where providers require sample data for the purposes of de-bugging systems or processes. In these circumstances we would implement a formal data sharing agreement to ensure the transaction is handled for the purposes of the 'system fix' and to obtain a legal platform to ensure that access, security and disposal of the data adheres to our requirements in terms of current and future ISO accreditation and Data Protection legislation.

In terms of transactional data (non-person identifiable data), for example direct debit data, there is a robust data sharing agreement and corresponding process for exchanging data with all suppliers. No person identifiable data is exchanged or transferred routinely.

Data hosting

The majority our data is hosted in secure cloud/data centre environments accessible only through VPN, and or in the case of our CRM, a two-factor authentication process, to which we intend to add a fixed IP as an additional protocol. Our data is held within the EU, and where practicable these data will be held in a UK based environment. Some data is held in secure local servers with the relevant backup and security protocols. Access to all systems is managed through robust permission structures based on the requirement of the individual's role, and these are regularly reviewed.

Out of hours access

There are a number of specific roles within our organisation that require that 'specified individuals' have access to data outside of operational hours. For example, to manage and react to incidents of exceptional call reporting (fraudulent calls) and to access systems remotely or on site for the purposes of maintenance or in managing system failures or errors. In these circumstances access is either on our premises or is governed by the same security measures outlined in data hosting.

Access to customer's data for the provision of maintenance and support services

Where Telesis Limited has installed a phone system, we will retain a copy of the installation records and this will include the Programme Requirement Document that contains the user's information for the system being installed. The data we hold as part of the installation records will not be updated where the data in the customer's phone system is changed and updated.

As part of an ongoing maintenance contract, Telesis Ltd Limited will provide designated Telesis Ltd staff with remote access to the customer's telephone system by agreement with the customer. In these instances, and for the provision of the maintenance and support functions, Telesis Limited will access the root system, and this will provide access to information that may identify an individual, including:

- **User Name**
- **User email**
- **User Direct Dial Number**

As a 'Data Processor' in the context of the Data Protection Act, these data will only be accessed where necessary and for the purposes of maintenance and service provision. Telesis Limited is, at the request of the customer able to access, alter and or remove these data, and where required, reset user's passwords. Telesis Limited is not able to view or access user's passwords. It remains the responsibility of users to change and update their passwords in line with the customer's security policies.

ISO review

- **Telesis Limited retains 9001 accreditation and is currently running an implementation programme with BSI to attain 27001 accreditation.**
- **There have been no significant security incidents in the last 12 months.**
- **The organisational risk register contains all risks identified to date and these are managed as determined by our internal processes, reporting to the organisational risk management group.**