Data Protection Assurance Statement

Organisation Name:	Computer Talk Ltd
DPO Name:	We have reviewed the requirement and determined that it is not applicable to our organisation. However, we have chosen to appoint a member of staff who can advise and assist Computer Talk Ltd in GDPR compliance: Emily Jamieson
Address:	Computer Talk Ltd, Units 1 & 2 Capricorn Centre, Coppen Road, Dagenham, Essex, RM8 1HJ
Email:	gdpr@computertalk.co.uk
Phone Number:	020 8595 7744

1. Restrictions on Sub-Contracting

Requirements

The GDPR gives Data Controllers a wide degree of control in terms of the ability of the processor to sub-contract. Data Processors require prior written consent. The processor is required to inform the controller of any new sub-processors, giving the controller time to object. If there is an objection, the sub-processing may not continue.

The lead processer in a sub-contracting arrangement is required to reflect the same contractual obligation it has with the controller in a contract with any sub-processors and remains liable to the controller for the actions or inactions of any sub-processor.

Our statement

Computer Talk Ltd will seek prior written consent from the Data Controller prior to appointing any sub-contractors or sub-processors, giving the Data Controller enough time to object. Should the Data Controller object to this arrangement, or request further information, we will request the sub-processing of the information immediately.

Any contract Computer Talk Ltd has in place with the Data Controller will be reflected in any sub-contracting arrangement. We understand that Computer Talk remains liable to the Controller for the actions or inactions of any sub-processor.

2. Controller/Processor contract

a. Requirements

Data Processor activities must be governed by a binding contract. The binding obligations on the Processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Controller. There are a number of specific requirements including that the personal data is processed only on documented instructions from the controller, and requirements to assist the controller in complying with many of its obligations. The Data Processor has an obligation to tell the Controller if it believes an instruction to hand information to the Data Controller breaches the GDPR or any other law.

Our statement

As a Data Processor, Computer Talk Ltd acknowledges that we must only use data that is shared with us as per the documented instructions of the Data Controller. We will use this data in order to perform contracted work, informing the Data Controller if we believe their instruction may breach the GDPR or any other law.

b. Requirements

If there is no contract with the Data Controller, please provide an up to date document setting out current standard of service delivery and terms and conditions under which the service is offered.

Our statement

Computer Talk Ltd have updated its Terms and Conditions of Service and General Terms and Conditions to reflect the changes in Data Protection and GDPR compliance. Updated Privacy Policies and Statements detailing how the Personal data is collected, stored and used is available on our website https://www.computertalk.co.uk/privacy-policy/

These will be issued to the Customer in due course. They will also be available on Computer Talk's website.

3. Demonstrating compliance

Requirements

GDPR requires organisations to demonstrate compliance. Processors are under an obligation to maintain a record of all categories of processing activities. These records must be provided to the Information Commissioner's Office (ICO) on request. This must include details of:

- the controllers they act for
- any other processors
- a data protection office (DPO)
- the categories of processing carried out
- details of any transfers to third countries
- a general description of technical and organisational security measures.

Processors must assess their need to comply by understanding whether they have fewer than 250 employees. If so, and unless the processing does not pose a risk to the rights and freedoms of individuals, is not more than occasional and does not include special categories of data (sensitive personal data), then the requirements are reduced.

Our statement

Computer Talk Ltd has assessed its requirement in order to comply with the General Data Protection Regulations. We are committed to improving, documenting and monitoring our processes and procedures to ensure we follow GDPR compliant methods. We believe that treating personal data and sensitive data as securely as possible, and recognising the rights that individuals have with regards to their data is in the best interests of the Company, its employees, its customers, and vendors.

4. Access Control & Security

a. Requirements

Processors, like Controllers are required to implement 'appropriate' security measures. What is 'appropriate' is assessed in terms of a variety of factors including the sensitivity of the data, the risks to the individuals associated with and processing or breaches of security, the state of the currently available technologies, the costs of implementation and the nature of the processing. These measures might include pseudonymisation and encryption. Regular testing of the effectiveness of any security measures is also required where appropriate.

Our statement

Computer Talk Ltd sets high security measures for the data held on its system. We use a mixture of: encryption; Enterprise Antivirus and Malware; complex password protection requirements; locked filing cabinets; double locked rooms; restricted access; and secure cloud services. Where we store data off premise (like in the Cloud) we have taken suitable checks on the GDPR compliance and security measures of these services.

Each Computer Talk technician has their own identity and password to gain access to our internal systems, and a different unique identity to gain access to Data Controller's sites. Using individual identities enables us to track logons to both our own and customer systems. These accounts can be disabled quickly and easily to render all access denied.

Where employees of Computer Talk have access to data on the Data Controller's systems (for example technicians who require access to perform their support tasks in line with our contract with the Data Controller), we have rigorous security measures and checks in place to ensure the safety of such data.

To gain access to the password required for a customer site, technicians have to log in to a secure password managed system which controls access to customer logons for specific products. This access is monitored and logged.

b. Requirements

Where suppliers have access to Customer data, please confirm staff vetting procedures (e.g. DBS checking procedures), confidentiality clauses in employment contracts and any monitoring/reviewing/auditing of employee activities.

Our statement

All employees of Computer Talk Ltd are subject to an Enhanced DBS check prior to their appointment and have confidentiality and NDA clauses within the employment contract. All employees must understand and sign this contract upon appointment. Our employee pre-employment checklist includes the following:

- Enhanced Disclosure and Barring System (DBS) formerly CRB (Criminal Records Bureau) Reference Check
- Employment Verification on work history
- Reference checks
- Right to Work Verification – Asylum & Immigration paperwork checklist
- Education Verification – authenticate education history
- Credential Verification – IT qualification checks
- DVLA Report - suitability and reliability of candidates driving company vehicles

All members of staff have their own identity and password to gain access to Computer Talks internal systems and a different unique identity and password to gain access to Customer sites. Using individual identities enables us to track logons for both our own and customer systems. These accounts can be disabled quickly and easily which would render all access denied.

Computer Talk uses internal monitoring systems to record some activities on company devices both in and out of the office. Whilst this system provides duty of care services for the business it also monitors the use of applications and browser activity.

We also use products which facilitate access to our customer sites in order to provide support services.

AEM (Autotask Endpoint Management) allows remote access to our Customer Networks in order to carry out our duties under the contract. AEM is a cloud based system which links in to our help desk from which staff can check on the status of Servers and if required log on to them. Use of this system is logged to show when access took place and by whom. Users can disabled quickly and easily which would render all access denied.

PassPortal is a password management system enabling us to control access to customer logons for specific products related to that site. Technicians are required to logon to PassPortal to gain access to the password for an individual site and is recorded. Users can be disabled quickly and easily which would render all access denied

c. Requirements

Where services include disposal of IT hardware – what standard of secure destruction is employed?

Our statement

Computer Talk Ltd does not dispose of IT hardware containing personal data. Where requests are made we recommend a third party partner who provide the following services:

- Free collections using GPS-tracked vehicles fitted with 4 cameras and load weighting
- Fully accredited facility with certifications including ISO 27001: Information Security Management, ADISA Distinction with Honours, DIPCOG and Cyber Essentials.
- Secure data description using industry-leading data wiping software Blancco

Where the nature of the work involves hardware disposal (that does not contain personal data), the Customer will be required to list all equipment to be collected prior to the collection date. Upon collection Computer Talk will provide the Customer with a Waste Transfer Note detailing our Waste Carrier License No. and Storage Exemption Notice. This must be signed by the Customer before the equipment can be removed from site.

d. Requirements

Data Controllers have a requirement to receive certification of the completed work.

Our statement

At the end of works completed by Computer Talk, the Customer will receive an email confirmation of the completed work, and/or a sign off and an acceptance sheet (depending on the work carried out).

e. Requirements

Where devices are removed from site by a Data Processor, how secure are the premises in which they work and what requirements are in place to safeguard any data on the device to which an operative may have access?

Our statement

Where devices are removed from a Customer site they are stored and repaired within a secured environment with limited access and protected by a door entry system. This room and the office building is monitored by CCTV and the Offices are locked by way of secure locks and shutters. The Offices are protected by an alarm and monitoring system 24/7 365 when unattended.

Computer Talk also operates a Clear Workspace Policy to encompass office, home, and site working with paper documents shredded when no longer required or locked away in a secure drawer.

5. Breach Notification

Requirements

There are enhanced breach notification requirements on both Data Controllers and Data Processors. Processers are required to notify their relevant controller of any breach without undue delay after becoming aware of it. Controllers have 72 hours to notify the Information Commissioner's Office (ICO) from the point the breach is detected, therefore reporting from the Processor to the Controller is required well within this time period. Your organisation will need to evidence effective process to identify and report breaches of your security measures to the Data Controller promptly, allowing the Controller time to deliberate and comply with the 72 hour rule.

Our statement

Computer Talk Ltd have a clearly defined internal process for all employees and are trained to follow this process should they suspect a breach has occurred. This process is straightforward and highlights the urgency of following the process. A dedicated eMail account has been created to monitor such breaches, which give priority to and alert members of staff responsible for GDPR so that actions can be taken without undue delay to notify the Data Controller.

We will notify you (and the ICO) of any breach that is likely to result in a high risk to your rights and freedoms without undue delay.

6. Data Protection Officers

Requirements

Both Controllers and Processors are required to appoint DPOs in certain situations, including where they are a public authority or body, where the data processing activities require regular monitoring of data subjects on a large scale, or where the core activities of the processing involve large amounts of special (sensitive) data or data relating to criminal convictions and offences. The primary role of the DPO is to assist the processor with, and advise on, compliance with GDPR. Processors may also choose to appoint a DPO even if they do not fall into one of the specified categories.

Our statement

We have assessed the requirement and determined that a DPO is not required for our internal compliance. However, due to the sensitivity of the Data we may Process for our Customers we have chosen to appoint a member of staff [Emily Jamieson] who can advise in GDPR compliance supported by our external advisors Mentor HR Services.

Overall responsibility for Data Protection lies with the Directors of the Company (Andrew Winterford and Liam O'Mahony).

7. Transfers to third countries

Requirements

The Processor has to exercise a degree of independence from the Controller when deciding whether or not it can transfer personal data to a third country. While processors are required to follow the relevant Data Controller's instructions with regard to the data processing, no matter what those instructions are, they may only transfer personal data to a third country (in the absence of an adequacy decision) if the Controller or Processor has provided appropriate safeguards and on condition that data subjects have enforceable rights in that country with respect to the data.

Our statement

It is very unlikely that Computer Talk Ltd will transfer any data to a third country.

Computer Talk Ltd will only transfer data to third countries and companies that have similar data safeguarding measures in place. Unless required to do so by law, we will always seek to gain documented consent from the Data Controller before passing on any data.

Signed:

Print Name: Andrew Winterford

Role: Director

Date: 2nd May 2018