TUNGSTEN NETWORK
Trusted connections. Streamlined transactions.

TUNGSTEN NETWORK AND GDPR

Clients' FAQs – version 1.0

Tungsten Network Ltd • Pountney Hill House, 6 Laurence Pountney Hill, London, EC4R 0BL, UK
T: +44 (0) 870 165 7410 • Web: www.tungsten.network.com

Registered in England and Wales Company No: 03958038. VAT No: GB 177 9072 67

Approvals Sheets

Document Owner(s)

Name	Role	Signature
Patrick Clark	Data Protection Officer & Legal Counsel	
Rafi Abdul Rahman	Senior Security and Compliance Officer	

Revision log

Revision	Date	Author	Notes
0	21/05/18	Lisette Yapo/Alphus Hinds	Working Draft
1	22/05/18	Rafi Abdul Rahman/Patrick Clark/ Simran Sandhu/Mahmud Choudhry/Alphus Hinds/Lisette Yapo	Revision and comments to the entire document

TUNGSTEN NETWORK
Trusted connections. Streamlined transactions.

Contents

Introduction

Tungsten Network is a leading global supply chain enabler. We have built the world's most trusted and compliant business transaction network and a suite of services designed to improve business outcomes for our clients.

Tungsten Network is committed to protecting the confidentiality, integrity and availability of our clients' systems and data. Data privacy and cyber security is of utmost importance to Tungsten Network, as is maintaining client trust and confidence.

Data protection has become increasingly important to both individuals and businesses. The new General Data Protection Regulation (GDPR) regime, effective from 25 May 2018, is designed to give individuals better control over their Personal Data and establish a standardised set of data protection rules across the European Economic Area (EEA). This regime applies to all organisations that process EEA Personal Data regardless of whether the organisation is in or out of the EEA geographical area.

Tungsten Network has taken a number of necessary steps in order to comply with GDPR over the past year, including:

- Engaging with PwC to assist in assessing Tungsten Network's readiness for the GDPR;
- Establishing a cross-company steering and working group, led by our Compliance and Assurance team;
- Leveraging our current industry best practices such as our IS027001 certification, Cyber Essentials certifications and Privacy Shield certification(s);
- Conducting a Data Privacy Impact Assessment (DPIA) across our business operations;
- Appointing a Data Protection Officer (our General Counsel);
- Upgrading our existing policies and practices including, but not limited to, data incident, data deletion and subject access requests;
- Conducting a thorough assessment of what Personal Data we hold (either as a Controller or Processor) and what the data flow of that is;
- Embedding privacy and security as an essential element of our product design and business operations processes;
- Reassessing and reevaluating our marketing practices including an assurance on what category of lawful processing applies;
- Conducting GDPR training for all employees and we will continue to do so;
- Conducting a detailed gap analysis assessment to identify the gaps within the business and implementing an action plan to reduce the risk of non-compliance to GDPR;
- Implementing encryption methods to safeguard Personal Data and carrying out regular audits and reviews to ensure confidentiality, availability and integrity of our processing systems and services; and

- Acquiring the latest best-of-breed proportionate technology for data discovery and classification.

Tungsten Network is committed to continually monitoring and improving its policies and practices including assessing how it keeps client data secure.

This document provides Tungsten Network's responses to the most frequently asked questions in relation GDPR and Data Privacy.

Company Corporation and Structure

For more than 16 years, Tungsten Network has been connecting Buyers to their Suppliers, enabling tax-compliant electronic invoicing. Processing more invoices, bringing on new Buyers and Suppliers, and adding new countries allows us to elevate the network effect for our members.

Tungsten Network is solely focused on bringing Buyers and their Suppliers closer together with unique technology that revolutionises invoice processing, maximises efficiency and improves cash flow management.

Tungsten Network has a number of offices and entities located in the following global areas:

Name	Location	Operations
Tungsten Network Ltd	London (UK)	Corporate Headquarters, sales, marketing and operations
Tungsten Network EOOD	Sofia, (Bulgaria)	Client support, technical support.
Tungsten Network Inc.	Atlanta and Ohio (USA)	Sales, marketing, support and operations
Tungsten Network Sdn Berhad	Kuala Lumpur (Malaysia)	Client and technical support, internal office administration

Personal Data

Questions	Response
Is Tungsten Network a Processor or Controller?	Tungsten Network is a "Processor" for all client Personal Data. This happens whether you are a "Buyer" (receiver of invoice information) or a "Supplier" (provider of invoice information).
What type of Personal Data does Tungsten Network process?	We "process" Personal Data that consists of (i) (business) contact details (ii) log in details and (iii) the day-to-day exchange of emails between Tungsten Network and its clients in order for it to fulfil our obligations to our clients. This typically consists of a name, business address, telephone number and/or email address. It can also consist of the occupation of a person.
What type of Personal Data does Tungsten Network not process?	Tungsten Network does not process any "sensitive" or any other category of "special" Personal Data of an EU citizen as part of its service provision.
Why is this Personal Data processed and for what purpose is it used?	The Personal Data that Tungsten Network processes is used to provide the services purchased by the client. For example, an invoice may contain the business contact details necessary for a Buyer to contact a Supplier about an invoice. A Buyer may provide us Supplier contact detail to aid in the Supplier enrolment process. We also may store log in details or business contact detail to provide support.
Has Tungsten Network assigned a Data Protection Officer that oversees data privacy?	Yes. Although not necessarily required in light of the Personal Data we process, we want to give our client's the comfort that a senior stakeholder in Tungsten Network is overseeing our data protection obligations. The person

	currently appointed is our General Counsel, a board member.

Collections and Purpose Limitation

Questions	Response
How is Personal Data collected?	The information is provisioned by clients via Tungsten Network's portal/systems and email in the following ways: i) Collected during campaign release i.e. Buyers provide their Suppliers contact details/ address/email and phone numbers. ii) Collected during Supplier enrollment i.e. the Supplier sales person will capture the Supplier's contact details during campaign enrollment. iii) Collected online i.e. Clients log into the Tungsten Network portal/download forms from the website. iv) Collected through emails received from clients to client facing teams to update their contact information.
Does Tungsten Network have a legitimate reason for collecting or processing the Personal Data?	Yes – for the provision of the services to a Client.
Where is the Personal Data stored?	Personal Data as part of service provision is stored within an encrypted Oracle database. In relation to day-to-day communications, Personal Data is stored in our internal CRM system.
Where is the location of stored Personal Data?	The Oracle database is located in Canary Wharf as the primary site and the disaster recovery site based in Slough, UK. This Database is managed and hosted by a company called Datapipe (which in itself is owned by Rackspace one of the leading managed service providers for data centers and the provisioning of private cloud environments).

	In summary all servers and EU Personal Data in our database is stored in the EU.
Is EU Personal Data ever processed outside of the EU	Yes. Due to the global nature of our business, it is necessary for a sub-set our business operations and infrastructure to have the capability of accessing invoice data and contact details outside of the EU. Invoice Data may contain Personal Data.
How do you protect Personal Data when it is transferred abroad or to third parties?	We use the approved transfer mechanisms allowed under GDRP and the applicable data protection laws to protect Personal Data. All sub-contractors who have access (or potential access) to client Personal Data are carefully vetted for their commitment to security by Tungsten Network's Procurement Department and minimum standards of conformance are expected including signing up to relevant undertakings and the "standard contractual clauses" (if Personal Data is processed out of the EEA). In relation to transfer of Personal Data to Tungsten Network's US subsidiaries, Tungsten Network has and will maintain its Privacy Shield certification.
How long is the Personal Data stored for?	Personal Data is stored in accordance with our Data Retention Policy, as well as any agreed client contractual obligations including archiving.

Security for Privacy/ Technical measures

Questions	Response
Is Personal Data encrypted at rest?	Yes. As a minimum AES (Advanced Encryption System) 256 bit encryption is used.
Is Personal Data encrypted in transit?	Yes. All data in transit is encrypted, as a minimum AES 256 bit encryption is used.
Does the application (Tungsten Network portal/systems) install cookies on the user's machine when accessing the application?	Yes. Please see our Privacy Policy.
What administrative access is there to Tungsten Network systems?	Role-based access is used to provision user/administration rights. A mature 'Identity Access Management' (IAM) system is used to control all administration access to the portal, system and database.
How often is the access control to the Personal Data reviewed?	There is continuous monitoring and user access rights are reviewed on a regular basis.
Do inactive user accounts get periodically disabled?	Yes. After 90 days.
Is Personal Data backed up as part of the data backup regime?	Yes. All data of our clients is backed up.
Describe what the backup process is for Personal Data that is collected and stored.	There are full and incremental backups of our Oracle database. Full backups are conducted weekly and incremental backups are conducted on a nightly basis. These backups are automatic and all Client data is encrypted.
Where are the physical backups containing Personal Data stored?	Physical data backups are stored on the database servers in Canary Wharf and Slough, UK. In addition, AWS encrypted S3 storage bucket is used to store data. Tungsten

	Network manages the S3 bucket encryption keys.
Are all end-point devices (i.e. computers) and servers used to process Personal Data (this includes remote access) password-protected after the boot sequence to prevent unauthorised access to Personal Data?	Yes. Tungsten Network applies a password policy requiring seven alpha numeric and upper and lower case characters. In addition, through sign-on via Active Directory (AD) Two-Factor Authentication (2FA) is enabled.

Individuals

Questions	Response
Does Tungsten Network know the basis on which it processes Persona Data?	Yes. As part of our GDPR readiness regime, we have assessed the various avenues we collect or process Personal Data (summarised for our clients on our updated Privacy Policy). In short, we have verified on what lawful basis we have processed Personal Data; whether it is via consent, legitimate use, to carry out a contract or otherwise.
Does Tungsten Network support Data Subjects Requests?	Yes. We have updated our Data Subject Access Request practices and policies to include the timelines necessary for GDPR as well as other factors.
Do you have procedures and templates formalised to assist Clients in responding to requests related to processing of Personal Data?	Yes, such procedures have been embedded into our updated Subject Access Request policy.

Privacy Program Management

Questions	Response
Do Tungsten Network employees undertake Data Privacy and Security Awareness training?	Yes. GDPR training is provided to all employees. There is also a program in place to continually train new employees and annually train existing employees. In addition, each year each employee undertakes training on best practice in relation to cyber security.
Do all employees of Tungsten Network have to sign a commitment to data protection and confidentiality?	Yes. This is part of the recruitment process for employees.
Does Tungsten Network conduct 'Privacy by Design' and Data Privacy Impact Assessments in relation to new development of systems, processes and products?	Yes. Our products and system development processes specifically incorporate our legal and security teams as part of that process.

Data Breach Readiness and Response

Questions	Answers
Does Tungsten Network have a documented Data Breach and Incident Management process?	Yes. Tungsten Network has always had an incident response process, which now has been updated in alignment with GDPR and our client requirements.

Certifications

Questions	Response
Does Tungsten Network maintain any certifications in respect to Privacy and Security?	Yes. Tungsten Network has and will maintain the following certifications: ISO 27001. This is a globally recognised a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures and includes legal, physical and technical controls in an organisation's information risk management process. In addition, Tungsten Network has the following certifications and compliance: Cyber Essentials Certification. This is a UK Government assurance scheme, as to compliance with a Government recognised level of information security. Compliance with National Institute of Standards and Technology (NIST) 800-54 Security Controls and with the requirements of the USA Government's Federal Information Security Management (FISMA) Act of 2002/ 2014.

	Finally, Tungsten Network is independently audited annually on its own internal controls under the ISAE 3402 regime. International Standard on Assurance Engagements (ISAE) No. 3402, provide an international assurance standard for documenting that a service organisation has adequate internal controls. It is equivalent to SAS 70 and SSAE 16, whereby ISAE 3402 prescribes Service Organization Control reports, which help give assurance to the organisation's clients and service users, who may have their own assurance needs.