TNS CONTRACTORS LTD

DATA PROTECTION POLICY

This policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties. The below definitions apply to this policy:

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company and Personal Data used in our business for our own commercial purposes.

- Data Protection Officer (DPO): the person appointed by us with responsibility for data protection compliance.
- Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.
- General Data Protection Regulation (GDPR): General Data Protection Regulation ((EU) 2016/679).

- Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

- Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

- Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
- Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This policy applies to all staff. You must read, understand and comply with this policy when Processing Personal Data on our behalf. This policy sets out what we expect from you. Your

compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

Scope
We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously
at all times.

The DPO is responsible for overseeing this policy and any queries you have regarding this policy should be directed to the DPO.

Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:
(a) the Data Subject has given his or her consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.
You must identify and document the legal ground being relied on for each Processing activity.

Consent
A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, explicit consent is usually required for Processing Sensitive Personal Data.
You will need to evidence consent captured and keep records of all consents so that the Company can demonstrate compliance with consent requirements.

Transparency (notifying data subjects)
The GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that Personal Data through a notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

Purpose limitation
Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

Data minimisation
Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job if it requires it. You cannot Process Personal Data for any reason unrelated to your job.

You may only collect Personal Data that you require for your job: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

Accuracy
Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Storage limitation
Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable notice.

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption where applicable). We will evaluate and test the effectiveness of those safeguards. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:
(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Reporting a Personal Data Breach
The GDPR requires us to notify Personal Data Breaches to the regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and follow their instructions. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer limitation
The GDPR restricts data transfers to countries outside the EEA (the EU countries and Iceland, Lichtenstein and Norway) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

You are not permitted to transfer Personal Data outside the EEA and should you be required to do so as part of your job you should seek guidance first from the DPO.

Data Subject's rights and requests
Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
(a) withdraw consent to Processing at any time;
(b) receive certain information about Processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and
(k) make a complaint to the supervisory authority.
You must verify the identity of an individual requesting data under any of the rights listed above.

You must immediately forward any Data Subject request you receive to the DPO.

Accountability
As a Data Controller we must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

Record keeping
The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

Privacy By Design and Data Protection Impact Assessment
We are required to implement privacy by design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

You must assess what privacy by design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:
(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of Processing; and
(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct data privacy impact assessments (DPIA) in respect to high risk Processing. A DPIA are tools and assessments used to identify and reduce risks of a data processing activity.
You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data.

For more information about what should be included in a DPIA please contact the DPO.

Direct marketing
We are subject to certain rules and privacy laws when marketing to our customers.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data
Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee or agent if the recipient has a job-related need to know the information and the transfer complies with GDPR.

You may only share the Personal Data we hold with third parties, such as our service providers if:
(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross border transfer restrictions; and
(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Access Control

"Access Control" is a key requirement to control access, the controls restrict access to machines and many applications by requiring a logon for authentication. Typically, this is an assigned "User Identity (UserID)" and password issued by IT. System managers must determine what controls to apply for permitting users the appropriate level of access.

User Accounts are created and managed in accordance with internal Policy and Standards (Network, Computer and Applications). Line managers are responsible for:

• Requesting that the IT Department creates computer accounts for new staff before they take up their employment via the appropriate process

• Informing the IT department of those leaving their employment and providing adequate notice, at least 2 weeks in advance

• Notifying the IT Service desk promptly of a user's prolonged absence of three months, or longer in which case their computer accounts will be disabled (note that IT will also monitor the usage of all user accounts and will routinely disable those that have not been used for a period of 60 days whether)

• When accounts are closed, any data held within the account including Email, folders, and files will be deleted after having been archived for a period of:

• 6 months on ceasing to be employed

• The system will not provide help messages during log-on

• The system restricts any incorrect log-on attempts to five, recording each event

• Following five unsuccessful log-on attempts, the account is disabled for a period

• Initial passwords changed by the user after first successful log-on

• Users accounts locked after 5 unsuccessful attempts to logon

Remote Access

A secure VPN solution is installed on all Laptop user devices for Remote Access, all staff must ensure that when using VPN that:

• It is only to be accessed by authorised users

• Should not be used on non-company devices such as personal home computers

Firewall Rules

Firewall rules specify (either allow or deny) the flow of traffic through the firewall device. Firewall rules are typically written based on a source object (IP address/range, DNS Name, or group), destination object (IP address/range, DNS Name, or group), Port/Protocol and action.

All firewall implementations adopt the principal of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Overtly broad rules may be allowed for specific groups of individuals (not systems). Approval must be granted by the Director or their designee.

The use of overly permissive firewall rules is prohibited (i.e., ANY/ANY/ALL rules).

Training

All employees will be trained in the this policy and understand its contents on an annual basis or as when new systems are introduced or if legislation changes.

Samuel Rayner

Samuel Rayner

Director – TNS CONTRACTORS LTD
Date – 07/09/2023