



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

1. Purpose and objectives

This policy forms part of TLS Limited's ('The Company') commitment to the safeguarding of personal data processed by its staff. (Processing has a very broad definition, and includes activities such as creating, storing, consulting, amending, disclosing and destroying data.) Its objectives are:

- To help staff recognise personal data; and
- To help them understand their obligations with respect to personal data.

2. Introduction

The Company processes the personal data of living individuals such as its staff, temporary workers, contractors and customers. This processing is regulated by the Data Protection Act 1998 (DPA). The UK's regulator for the DPA is the Information Commissioner's Office.

It is the duty of data controllers such as the Company to comply with the data protection principles (see the Annex to this Policy) with respect to personal data. This policy describes how the Company will discharge its duties in order to ensure continuing compliance with the DPA in general and the data protection principles and rights of data subjects in particular. The principles are listed in the Annex to this Policy.

3. Scope

The policy applies to all staff of the Company and all other computer, network or information users authorised by the Company. The policy relates to electronic information, paper files and records created for the purposes of the Company's business.

4. Definitions

Personal Data[1]

"Personal data" means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual"

Sensitive personal data[2]

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC



Ref: P009	TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy
-----------	--

Information about:

- the racial or ethnic origin of data subjects
 - their political opinions
 - their religious beliefs or other beliefs of a similar nature
 - whether they are members of a trade union
 - their physical or mental health or condition
 - their sexual life
-
- the commission or alleged commission by them of any offence, and any proceedings for such offences.

Although the DPA does not define 'health', the term should be understood broadly, to include preventative medicine, medical diagnosis, DNA sequences, medical research, provision of care and treatment and the management of healthcare services.

Personal demographic data, such as personal addresses and financial data (including salaries) are not sensitive personal data, but should be treated with similar care.

Manual Personal Data

Personal data recorded as part of a relevant filing system in paper or other non-electronic format.

Processing[3]

Obtaining, recording or holding personal data. This includes organisation, adaptation or alteration; retrieval, consultation or use; disclosure; and alignment, combination, blocking, erasure or destruction.

Relevant Filing System[3]

Manual personal data structured by reference to individuals in such a way that information relating to a particular individual is readily accessible.

Data Holding

A collection of one or more data sets or files that are being processed for permitted purposes under the direction of a clearly identified member of the Company's staff - the Data Owner.

Data Controller

As the organisation which determines the purposes of the processing, the Company is the Data Controller for the personal data that it manages.

Ref: P009	Revision No: 10	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------



Ref: P009	TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy
-----------	--

Data Protection Officer

The Company member of staff with lead responsibility for Company's compliance with the DPA currently Paul Chamley.

Data Owner

The Company's member of staff with lead responsibility for permitting and managing the retention and processing of a data holding for which The Company is the Data Controller currently Paul Chamley. Data Owners delegate responsibility for personal data elements to Data Custodians.

Data Custodian

The individual unit or person identified by the data owner to be responsible for the collection, creation, modification and deletion of specified personal data element(s)

Data Subject[4]

A living individual who is the subject of personal data

Data Processor[4]

Any third party (other than the Company's staff) who processes personal data on behalf of and on the instructions of the Data Controller (for example external contractors).

5. Roles and responsibilities

Data Protection Officer

The Data Protection Officer has primary responsibility for the Company's compliance with the DPA. This comprises:

- maintaining the Company's notification with the Information Commissioner's Office
- ensuring completion of the Annual Survey of Personal Data Holdings
- handling subject access requests and requests from third parties for personal data
- promoting and maintaining awareness of the DPA and regulations, including training
- investigating losses and unauthorised disclosures of personal data.

The DPO is the Company's main contact for the Information Commissioner's Office.

Data Owner

Ref: P009	Revision No: 10	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

Data Owners are responsible for:

- establishing and monitoring measures, in accordance with this policy, to protect any holdings of personal data for which they are responsible
- ensuring that those holdings are registered as part of the annual survey of personal data holdings
- ensuring that any transfer of personal data to third parties is authorised, lawful and uses appropriate safe transport mechanisms such as encryption.
- authorising the downloading of electronic personal data on to portable devices or the removal of manual personal data from any Company premises
- informing the DPO when new holdings of personal data are established or when the purposes of processing change.

Data Custodians

Data Custodians should ensure that their processing of personal data is compatible with the data protection principles, including the security and integrity of data sets.

Data Processors

Data processors have a contractual responsibility to act only on the Company's instructions and to ensure that their processing of personal data provided by THE COMPANY is carried out in compliance with this policy and in accordance with the eight data protection principles. There should be a written agreement with data processors which adequately addresses these responsibilities.

Staff

All staff are responsible for:

- ensuring that their processing of personal data, including research data, in all formats (e.g. electronic, microfiche, paper, etc.) is compatible with the data protection principles
- raising any concerns in respect of the processing of personal data with the Data Protection Officer
- promptly passing on to the Data Protection Officer all subject access requests and requests from third parties for personal data
- reporting losses or unauthorised disclosures of personal data to the Data Protection Coordinator.

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC

Uncontrolled if Printed or Copied



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

In order that the Company can continue to comply with the fourth data protection principle, staff should ensure the personal data they provide about themselves is up to date.

6. Security of personal data

All staff processing personal data should ensure that the data is secure. Appropriate measures must be taken to prevent unauthorised access, disclosure and loss. Staff whose work includes responsibility for supervision of temporary workers have a duty to ensure that temporary workers observe the eight principles of the Act.

It is rarely necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by the Company. Similarly, manual personal data should not be regularly removed from the Company premises. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to the Company should be used wherever possible.

Downloading personal data on to portable devices or taking manual personal data off-site must be authorised in writing by the Data Owner, who must explain and justify the operational need in relation to the volume and sensitivity of the data. The data must be strongly encrypted. Users should only store the data necessary for their immediate needs and should remove the data as soon as possible. To avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure

Manual personal data and portable electronic devices should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

In order to comply with the fifth data protection principle personal data should be securely destroyed when no longer required, with consideration for the format of the data.

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the data owner and protected by adequate contractual provisions.

All losses of personal data must be reported to the Data Protection Officer. Negligent loss or unauthorised disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

7. Access to personal data

7.1 Subject access rights

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

Data subjects have a right of access to their personal data. Subject access requests must be made in writing and sent to the Data Protection Officer. Data subjects must prove their identity.

Copies will be provided in permanent form promptly and in any event within 40 days. In the case of a request made in relation to examination marks or results, the timescale is extended to the earlier of:

- five months from the day on which the request was received; or
- 40 days from the announcement of the examination results.

Some personal data are exempt from the right of subject access, including confidential references provided by the Company.

The Company does not charge a fee for subject access requests.

Although the DPA applies only to living individuals, data about deceased persons who at the time of processing would be under 100 years old should be treated as personal data, unless the information is the subject of a valid request under Freedom of Information legislation.

7.2 Monitoring

It is sometimes necessary for the Company to monitor information and communications. This may include personal data.

7.3 Third party access

In certain circumstances the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Data Protection Officer. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

8. Records Management

Records in all formats containing personal data must be created, stored and disposed of in accordance with the Data Protection Principles. If stored they must be authentic, reliable and usable and capable of speedy and efficient retrieval. They must be retained for no longer than the periods permitted by law and then disposed of securely and confidentially.

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

9. Compliance with GDPR 2018

Traffic Labour Supplies Ltd. have opted to use the Usercentric Consent Management Checklist for GDPR Compliance as a guide for its programme to comply with GDPR 2018.

As Traffic Labour Supplier Ltd. keeps a very limited amount of personal data for its employees and self-employed partners, much of the checklist is not applicable. However, Traffic Labour Supplies Ltd. are committed to complying with GDPR 2018 where it is applicable to the Company.

The following is an outline of the guidance given in the checklist:

Usercentrics – Consent Management Checklist for GDPR Compliance

1. Determine if your company is required to comply
2. Create a comprehensive privacy policy
3. Inform users about their rights
4. Obtain valid consent from users
5. Ensure user access even if they decline consent
6. Stop data collection or processing as soon as the user opts out
7. Securely document and store consent received from users and be able to provide information when required
8. Review and update the Privacy Policy (i.e. this policy, P009 – TLS Data Protection, Privacy & GDPR Policy)
9. Re-offer opt-in consent every 12 months

Further detail about the content of this checklist and other information about data protection, privacy and GDPR 2018 compliance can be found in TLS IMS>23 Data Protection, Security, Privacy & GDPR

10. Annex

THE DATA PROTECTION PRINCIPLES

It is the duty of data controllers and data processors to comply with all the data protection principles. These are set out in Schedule 1 of the Data Protection Act 1998, from which the following extract is taken:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC



Ref: P009

TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

[1] DPA section 1

[2] DPA section 2

[3] DPA section 1

[4] DPA section 1

Paul Chamley

A handwritten signature in blue ink, appearing to read 'P. Chamley'.

Managing Director

Ref: P009

Revision No: 10

Date Issued: 17/01/2026

Approved By: PC

Uncontrolled if Printed or Copied



Ref: P009	TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy
-----------	--

Revision History

Revision	Date	What has changed?	Who has written it?	Who has approved it?
00	14/06/2019	First Issue	AG	JB
01	03/07/2019	Changed logo and added related documents, records and revision history tables	AG	JB
02	31/10/2019	Review and update names following company change of ownership	AG	PC
03	31/10/2020	Reviewed and TA logo added	Systems Manager	MD
04	31/10/2021	Reviewed	Systems Manager	MD
05	24/01/2023	New TLS Group Logo added	Systems Manager	MD
06	03/05/2023	Name change to data protection officer	Systems Manager	MD
07	17/01/2024	Addition of section for complying with GDPR (for Achilles CAS Desktop Assessment)	Systems Manager	MD
08	17/01/2025	Annual review	Systems Manager	MD
09	14/08/2025	Added full company name to title for Construction Line	Systems Manager	MD
10	17/01/2026	Review	Systems Manager	MD

Ref: P009	Revision No: 10	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------



Ref: P009	TLS (Traffic Labour Supplies Ltd) Data Protection, Privacy & GDPR Policy
-----------	--

--	--	--	--	--

Ref: P009	Revision No: 10	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------

Uncontrolled if Printed or Copied