TMO Traffic Highways Ltd

Data Protection Policy

TMO-GDPR-012 Rev 3

Introduction

The management of TMO Highways (TMO) are committed to adhere to all relevant UK laws, including but not limited to the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, in respect of personal data and the protection of the 'rights and freedoms' of individuals whose information TMO collects and processes.

Policy applicability

This policy applies to all staff (permanent and part-time) as well as contractors, all of whom have a collective responsibility for the proper processing of the personal data for which TMO is responsible. Any incident or potential data breach is to be reported to the Privacy Manager (see below) in the first instance and as soon as possible.

Appointment of the Privacy Manager (PM) and Data Protection Officer (DPO)

TMO appoints a member of staff, known as the Privacy Manager (PM), who is responsible for all aspects of personal data processing. This includes annual reviews, and the regular maintenance of media used to collect and process personal data, and its eventual return, destruction and/or deletion. The PM is also first point of contact for anyone seeking clarification on any aspect of data protection compliance. A detailed description of the PM's role is to be provided in separate documentation and reviewed annually.

The PM is to be supported by an external data protection officer (DPO) who is to assist in this role. Areas of responsibility and taskings for the PM and DPO are set out in

The roles and responsibilities of the PM and the DPO are set out in Annex A to this policy.

Scope of responsibility

Compliance with data protection legislation is the responsibility of all members of staff and contractors who process the personal data by or on behalf of TMO. Any misuse or abuse of personal data, whether intentionally or not, will be dealt with by TMO management for further action. This may include notifying the Information Commissioner's Office (ICO). A record of all such incidents is to be recorded in an Incident and Data Breach Register which is to be maintained by the PM.

Third party contractors working with TMO are expected to understand the basic premise of this policy and will, when necessary, be issued with a Privacy Notice and a data processing agreement if the contract does not include the relevant clauses from the UK GDPR.

Data protection principles

TMO will ensure that the processing of all personal data will be conducted in accordance

with the data protection principles shown, in so much that it will be:

- Processed lawfully, fairly and transparently
- Collected for a specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary (and no more)
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security

TMO is to be transparent and fair in all aspects of processing personal data. A privacy statement that explains in broader terms TMO's stance on data protection matters, is to be made available on the TMO website and be downloadable by website visitors.

Lawful conditions for processing

TMO collects personal data for a variety of reasons and the lawful condition for doing so will vary accordingly. In all instances, it will process personal data using one of the following lawful conditions:

- Using consent, given prior to any processing
- To meet its contractual obligations
- To comply with its legal obligations
- When acting in the vital interests of an individual
- When processing is necessary for tasks in the public interest
- In pursuit of TMO's stated legitimate interests, where it is assessed that its actions do not over-ride the rights and freedoms of the affected individual

Accountability

TMO is to be fully accountable for the way it processes all personal data and must be able to demonstrate its ability to meet its legal requirements as set out in the data protection legislation. This will be done through the implementation of policies, effective working practices, adhering to codes of conduct and implementing technical and organisational measures including breach notification procedures and incident response plans.

Transparency

Key to the good practice of processing personal data is for TMO to be transparent in its processes and the way it communicates with the people whose data is being processed.

TMO is to publish and maintain a website privacy statement that can viewed easily and be downloadable, as well as appropriate Privacy Notices (PN) to specific categories of people when necessary. The privacy statement and PN are to set out:

- What information is collected why it is collected and against which lawful basis
- The source of the personal data if it did not come directly from the data subject
- How that information is to be used

- To whom personal data might be disclosed
- How data subjects' rights can be exercised

Where the personal data is processed and stored

All personal data that we collect or generate in hard copy form is processed, stored and eventually destroyed on the premises of TMO. Other (non-paper) based data is gathered and processed by our Office IT system in our main office in Eye, Suffolk. All back-up servers are to be situated in the UK.

Where TMO engages a third-party IT support business, a data processing agreement is to be in place in addition to the service level agreement between the parties. Service provision for data storage is conditional on the servers being located in the UK.

Consent

Consent means any freely given, specific, informed, and unambiguous indication of an individual's wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Any requests for consent must be in a form of words to ensure consent would be valid. Additional information is to be provided at the time consent is being requested that will enable the consenting party to have access to the company website privacy statement.

If consent is indicated only verbally, then a record of this event is to be made including the date on which it was received and the manner it was given. The proper maintenance such records is necessary to enable TMO to be accountable for its actions and to be able to demonstrate that consent was given.

If consent to a particular purpose has not been received, TMO understands the lack of response to be that consent has not been given and the relevant processing activity will not take place.

When explicit consent is relied upon for the processing of sensitive (special category) data, TMO is to obtain a signed declaration (or equivalent) from the individual (or legal carer) before the processing activity commences.

In all instances, if consent is withdrawn, TMO will cease processing relating to the associated purpose and record the event.

Change of purpose of processing

From the outset, TMO will state the purpose for which personal data is collected. If this purpose is changed, the affected individuals will be contacted with the relevant information and further appropriate action will be taken if required. Processing of personal data against the new purpose will not commence until either permission has been received or the affected people have been informed.

Training

All TMO staff who routinely handle personal data as part of their role are to undertake regular training (at least annually) to instruct or remind them of the basics of data protection. The TMO privacy manager and assistant are to receive more thorough training as befits their roles. The training can be conducted by any competent staff member with the requisite experience and knowledge, on-line or delivered by an external trainer if necessary.

Third-Party support workers (contractors)

Those that support TMO's operations but are not employed by TMO (contractors) are to be briefed on their responsibilities regarding the handling of personal data. The extent of such briefings will depend on each role so is not specified in detail in this policy, however, the expectation is that as a minimum, contractors:

- Are made aware of this policy and who the identity of the PM
- Are made aware of any immediate role requirements such as returning job cards and deleting any personal data stored on 'Smart' phones for specific jobs upon completion of that job
- Delete any TMO related personal data other than that used for domestic purposes, prior to the end of their contracts
- Are made aware of the need for reporting incidents and possible data breaches and how they can do so
- Be issued with or given access to the TMO privacy statement
- Be issued with or given access to a contractor's specific privacy notice if needed

Security of data

TMO operates a 'need to know' principle but will always try to get the right balance between ensuring the privacy of the individual and being able to offer an effective and efficient service to its customers.

Whilst the overall responsibility for the implementation of data protection policies and procedures lies with the PM, all staff and permanent contractors are responsible for the personal data they process. This includes, but is not limited to, keeping information secure when not in use and keeping documentation out of sight of those that have no reason to view it.

IT Security

TMO uses a trusted third-party IT service provider to ensure, in so far it is possible, that all data processed meets the spirit of data protection laws in so far that the office IT system enable the appropriate level of confidentiality, availability and integrity of the personal data processed on-site.

Due diligence is applied to ensure that the service offering is appropriate to the needs of the

business and that the work force of the third-party understands their responsibilities in terms of respecting the confidential nature of the personal data it has access to. The engaged IT service provider is to be subject to a data processing agreement as required by Article 28 of the UK GDPR.

TMO engages a dedicated in-house IT support staff member who is responsible for the first line maintenance of the IT system and the application of appropriate security measures to be set out in TMO's Information Security (InfoSec) Policy.

Physical Security

The application of appropriate physical measures in an organisation is intricate to the responsible processing of information, particularly personal data. TMO adopts a layered approach to physical security such that there is no single point of failure. In brief, physical security is maintained through:

- A combination of on-site employees with dedicated security duties
- The use of combination coded locks for building access when doors are unlocked during office hours
- Use of lockable filing cabinets for storage of hard copy information and other storage media where the keys are assigned to nominated individuals
- Lockable doors that remain locked by default but opened during office hours and during performances when needed
- Controlled access to the master keys for all lockable doors
- Access lists that detail which staff are entitled to know combination codes or have access to the master keys

Use of on-site CCTV and Body Cameras

TMO has a legitimate interest to deploy CCTV systems for the detection and prevention of crime. The routine operation of the CCTV system is to be managed by Jamie Lange in accordance with the TMO CCTV operation policy.

Where CCTV is deployed, there is to be adequate signage to ensure anyone visiting the site is made aware that CCTV is in operation. Unless circumstances justify, images are not to be retained any longer than 14 days.

Body cameras (bodycam), when worn by TMO staff, are to be operated under controlled conditions by trained staff. Before bodycams are switched to record, anyone in the vicinity must be made aware that recording is about to commence. TMO must be prepared to respond to access requests resulting from this activity – also see Individuals' (Data Subjects') rights below.

Use of on-site fleet installed Dashcam CCTV

The TMO fleet of operational vehicles are fitted with CCTV, referred to as 'Dashcam'. TMO recognises that appropriate safeguarding measures must be taken to ensure the integrity of the images being recorded. Image files can be requested by the public and can also be used as evidence in criminal/civil proceedings, therefore the confidentiality, integrity, and accessibility is to be maintained at all times.

Given the potentially intrusive nature of this technology, the use of dashcam is to be subject to various controls underpinned by the following policies:

- TMO Dashcam Policy – top level
- Dashcam System Privacy Notice – to be made available or given access to the public upon request
- Dashcam Code of Conduct for management – for TMO management
- Fleet Drivers' Use and Management of Dashcam Policy – for TMO drivers
- Dashcam Data Subject Access Request (DSAR) Request Form – to be issued upon request

TMO's continued use of dashcam is subject to a review every 2 years in the form of a legitimate interest assessment (LIA) that builds upon the original LIA.

Security Responsibilities

The Finance Director is responsible for implementing security arrangements and reviewing them on a regular basis, recording findings and follow-up actions and to provide a summary at the regular staff meetings if requested. Separate security procedures document is to be developed and maintained to support this role.

Disclosure of data

The guiding principle of TMO is that personal data is not to be disclosed to third parties, which includes family members, friends and in some circumstances, the police, unless previously authorised or agreed to by the affected individual. Such authorisation or agreement must be demonstrable and normally involves:

- The signing of a confidentiality agreement or Non-Disclosure Agreements
- A court order

It follows that all staff and permanent contractors should exercise caution when asked to disclose personal data held by TMO to a third party. Any such requests must be supported by appropriate evidence that states its purpose and should be retained or recorded. Other than established or regular requests, guidance must be sought from the PM before disclosure. Exceptions to this might be when someone must disclose information to act in someone's vital interests; this is normally a 'life and death' situation.

If, subsequently, the disclosure of personal data was deemed to be inappropriate, then this is to be reported to the PM and recorded in the Incident and Data Breach Register. The PM is then to decide on further action as required.

Retention and disposal of data

TMO is to maintain a Retention Schedule and the to adopt internal measures such that staff do not retain personal data in a form that permits identification for longer than is needed or justified in law. Personal data may be stored beyond the schedule, after it has been reviewed and reduced to a minimum, for the purpose of maintaining records and statistics in support of its legitimate interest. In all cases the appropriate technical and procedural measures are to be taken to safeguard the rights and freedoms of the affected individuals.

Disposal and destruction of personal data will be conducted under controlled conditions under the guidance of the PM and in accordance with TMO's internal security procedures

Retention of personal data after the lawful condition for processing has ended

Regardless of the source of personal data held by TMO, once it is no longer needed or no lawful justification exists to retain it, the personal data is to be reduced, deleted or destroyed in accordance with this policy or the schedule set out in the website privacy statement and/or relevant Privacy Notices, within 3 months of the retention period ending.

Incident and data breach reporting

TMO staff are to be briefed that the misuse of personal data, whether intentional or otherwise, can have serious consequences for TMO's reputation. Any incident, that might expose someone (regardless of who) in such a way that their rights and freedoms are impacted, is to be reported to the PM. Subsequent action will be determined by the PM based on the severity of the incident. The PM is to seek the advice and guidance of the external DPO when necessary.

In all instances, incidents are to be recorded in a dedicated register. When appropriate, they are to be registered as a data breach. If reportable, data breaches are to be reported to the ICO within 72 hours of the data breach being established, by the DPO or the PM if the DPO is unavailable.

The TMO website

TMO maintains a website for publicity purposes and as a source of information to potential and actual customers. The website uses cookies to enhance user experience and to collect analytical data of the web browsers used to view the website. User consent must be sought before non-essential cookies are run. No attempt must be made to identify the individuals, via technical means or otherwise, that visit the website, unless there is a legal requirement to do so.

Individuals' (Data Subjects') rights

The UK GDPR puts much greater emphasis on transparency of processing and accountability by all parties involved in handling of personal data. It also extends the rights of individuals (referred to as "data subjects") in respect of their personal data. It should be noted that

these are limited and do not apply in all situations. These are shown below:

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights related to automated decision making and profiling.

TMO will ensure that individuals may exercise these rights including the handling of Data Subject Access Requests (DSAR) and complaints relating to the processing of an individual's personal data.

Data transfers

TMO does not ordinarily transfer personal data outside the UK and does not use services (such as back-ups) that rely on data processing outside the UK. If the situation arises that data might be transferred outside the EEA, the PM will assess the impact of such processing and seek further advice as necessary.

Information asset register/ data inventory

TMO is to maintain a high-level data inventory that identifies the flow of personal data into and out of the company. This is primarily used to identify the key areas where Privacy Notices (PN) should be issued and also to identify areas of security vulnerability, whether paper or IT related.

The above is based on an initial assessment of risk to individuals associated with the processing of their personal data. TMO is to conduct risk assessments annually and in response to an incident or data breach, whichever comes first, and instigate appropriate actions to reduce the possibility of mal-practice or non-conformance with this policy.

Data Protection Documentation

TMO will maintain sufficient documentation with respect to the processing of personal data, to be able to demonstrate that it is following structured processes in a responsible and lawful way. All documentation is to have an owner, be subject to version control and be approved, including updates, by TMO management. The documentation will cover a wide range of activities required to support the responsible application of data protection practices at TMO, the key documents are as follows:

- Data Protection Policy – an internal document available to all staff and permanent contractors
- Privacy Statement – a public document available on the website

- Privacy Notices – issued to anyone at the time their personal data is collected if they did not contact TMO via the website
- Record of data processing activity – high level only
- Information security (InfoSec) policy
- Incident and Data Breach Register – to be controlled by the PM
- CCTV Usage Policy
- Dashcam related policies – see above

Policy reviews and updates

Data protection related documentation is be reviewed annually as part of TMO's overall audit programme. Such activity may happen more frequently as advised by the PM, in particular to take account of:

- Incidents and data breaches that might require a review of existing procedures
- When compelled to do so by the ICO
- When a policy is still being developed

Document owner, approval and availability

The PM is the owner of this policy document and is responsible for ensuring it is reviewed in line with all requirements set out above. The document is subject to version control and approval by TMO management.

The document and any later versions are to be made available to all staff and seasonal contractors, such that they might reasonable have access to it in the normal course of their duties. This may involve its distribution by email or by post when appropriate. Its existence and selected content will also be highlighted during regular staff meetings.

v1.1
February 2023

Annexes:

A. Roles of the Privacy Manager and the External Data Protection Officer

Annex A

Roles of the Privacy Manager (PM) and the External Data Protection Officer

TMO Privacy Manager (PM)

The PM is appointed by TMO management to provide first line support to TMO staff on data protection law, its compliance and the implementation of related policies and procedures.

Specific tasks

In particular, the PM is to:

- Attend such training, either in person or on-line, to ensure they have the requisite level of data protection knowledge to be effective in the role
- Appoint a deputy PM and ensure that they have the requisite training and continuation training to fulfil the role
- Provide first line support to TMO staff regarding data protection matters and to assess incidents in accordance with TMO's incident reporting procedures
- Liaise with the DPO at the point when the PM needs additional guidance or when there is a legal necessity for the DPO to intervene
- Provide the DPO with access to TMO staff for the purposes of awareness briefing, reviewing extant processes and investigating incidents
- Provide the DPO with access to personal data and processing operations for the purposes of investigating incidents
- Provide a suitable workplace for the DPO and any related staff when visiting TMO's premises and access to virtual meeting facilities when required

External Data Protection Officer (DPO)

Based on the tasks described in the UK GDPR, the DPO shall:

- Advise TMO management on all matters relating to the processing of personal data, including the investigation of potential data breaches
- Routinely monitor how TMO meets the legislation through the implementation of policies, and assignment of responsibilities, awareness briefings, training, and audits
- Provide advice regarding the need for, and the processing of, Data Protection Impact Assessments (DPIA)
- Cooperate with the Information Commissioner's Office (ICO) and to be TMO's point of contact for the handling of data breaches and other appropriate matters
- Be available to all TMO staff members who wish to raise issues relating to the processing of their personal data and to exercise their rights.

These tasks shall take due regard of the risk associated with the processing operations, considering the nature, scope, context, and purposes of processing by TMO. Accordingly,

the DPO is bound by confidentiality concerning the performance of the duties and is, in any event, subject to the conditions set out in the UK GDPR for data processors.

Specific tasks as they apply to TMO

In particular, the DPO shall:

- Provide input at regular TMO management meetings as determined by mutual agreement
- Provide support to the PM on an as required basis without undue delay but within a maximum of 48 hours
- Work collaboratively with TMO to populate and update the Data Protection Risk Register and advise on risk mitigation measures
- Provide input to the creation and maintenance of TMO's privacy framework, including policies and procedures