TRANSPORT FOR THE NORTH

General Data Protection Regulation (GDPR) Governance Framework

Internal Audit Report 4.22/23

Revised Final v2

3 January 2023

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

This document is Not for Publication - Confidential

EXECUTIVE SUMMARY

Why we completed this assignment

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our assignment and provide you with the assurance you require and 100 per cent of our assignment has been conducted remotely.

From 25 May 2018 the General Data Protection Regulation (GDPR) replaced the EU Directive 95/46/EC. The UK Data Protection Act 2018 embeds significant elements of the GDPR into UK legislation. A Government consultation called 'Data: a new direction' on the future for UK data protection legislation closed in November 2021. The outcomes were published on 23 June 2022 and there may be further changes to data protection requirements to follow.

Whilst many of the GDPR's main concepts and principles (and thus those of the UK DPA 2018) remain largely the same as those in the Data Protection Act 1998, there were significant new elements and enhancements which required companies and organisations to perform some specific compliance activities for the first time. GDPR placed greater emphasis on the documentation that data controllers must keep demonstrating their accountability.

We have been commissioned by Transport for the North ('TfN') to undertake an assignment which considers the TfN's GDPR current data governance processes, procedures and controls. Our report is a factual report and we do not provide a level of assurance, or internal audit opinion, and this report should not be taken to provide such.

Headline findings

This report has been prepared in full and details of our testing and findings can be seen in our Detailed Findings and Actions section of this report. We confirmed that TfN has some elements of a data governance framework in place in the form of policies. However, we have raised a number of management actions which will assist in improving and embedding the current framework. Our work noted the following:

Business processes and data discovery:

TfN does not retain a comprehensive and accurate record of the location and origin of personal data held in-house and shared with third parties. Without this, there is an increased risk of non-compliance with the requirements relating to information held.

Awareness:

Although training and staff awareness has been completed as part of induction training, we noted that this training is only refreshed periodically after induction. We would advise the implementation of annual refresher training, to strengthen staff understanding and awareness of GDPR requirements.

Data policy, roles and responsibilities

Through review of the Data Protection Policy, we noted that it does not reflect current roles and responsibilities in relation to data protection. Furthermore, we noted that roles and responsibilities in relation to data protection were not fully defined within the organisation.

DETAILED FINDINGS AND ACTIONS

The results of our testing are set out below.

ICO Area: Business processes and data discovery	
Area 1	A main focus of GDPR is protecting the rights of individuals who are referred to as data subjects. Personal data collected from data subjects should be audited and documented to ascertain what is being held and for what purpose. TfN does not keep a comprehensive and accurate record of the location and origin of personal data held in-house and shared with third parties.
Findings / Implications	Through review of evidence and discussions with both the Senior Lawyer and IT and Information Manager, we were informed that initial data mapping has taken place with regards to the systems that hold personal data. These include: • Dynamics 365 – HR; • Dynamics 365 – Finance; • SharePoint; • Emails; and • Cloud Storage. For each system, TfN has documented the following: • Data Owner; • Data Processor; • Data Types; • System Background/ Overview; • Purpose of the Data; • Security Restrictions in Place; • Process of Access; • Process of Use; and • Risk Management and Key Issues. We were also provided with a template document which TfN plans to populate to produce a formal record of processing activities (ROPA). However, as TfN does not have a comprehensive and accurate record of the location and origin of personal data held in-house and shared with third parties, there is an increased risk of non-compliance with the requirements relating to information held. Examples of potential non-compliance include: • Non-compliance with the requirement to have a ROPA containing a specified set of information about personal data that is processed; • The inability to notify third parties of any inaccuracies in data shared with them, due to lack of awareness of the information sharing arrangements in question; and • Non-compliance with the GDPR accountability principle by demonstrating that the organisation has effective policies and procedures in place for the management of personal data.

ICO Area: Business processes and data discovery			
Management Action 1	A formal record of processing activities (ROPA) will be produced and maintained which will include: • The organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the Data Protection Officer (DPO)); • The purposes of the processing; • A description of the categories of individuals and of personal data; • The categories of recipients of personal data; • Details of transfers to third countries, including a record of the transfer mechanism safeguards in place; • Information required for privacy notices, such as the lawful basis for the processing and the source of the personal data; • Information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018 (DPA 2018); • Records of consent; • Controller-processor contracts; • The location of personal data; • Data Privacy Impact Assessment reports; • Retention schedules; and • A description of the technical and organisational security measures in place Once completed, a process will be implemented to ensure that this central record is accurate and remains up to date to ensure that the organisation continues to hold a comprehensive, accurate and up to date record of all the personal data held. This could be undertaken via regular (at least annual) data audits with nominated data owners to capture any changes.	**Responsible Owner:** Data Protection Officer	**Date:** 30 April 2023

ICO Area: Third parties	
Area 2	Although data audits to confirm personal data compliance have been undertaken, a comprehensive and accurate record of the location and origin of all personal data held in-house and shared with third parties is not retained.
Findings / Implications	As detailed above (at Area 1), there is currently no comprehensive and accurate record of the location and origin of all personal data held in house and shared with third parties. As such, there is an increased risk of non-compliance with the requirements relating to information held.
Management Action	See Management Action 1.

ICO Area: Data ownership	
Area 3	Data owners have been identified.
Findings / Implications	As identified at Area 1 above, data owners have been identified as part of the initial data mapping that has taken place regarding the systems that hold personal data. However as detailed above at Area 1, TfN should ensure that these data owners are actively involved in populating the ROPA.
Management Action	None.

ICO Area: Data security system level controls	
Area 4	TfN has appropriate data and system access controls and rights in place, which ensure that data or systems are only accessed by their intended user.
Findings / Implications	Through discussions with the IT and Information Manager, we were informed that TfN has documented their IT systems that manage data and we were provided with the resulting Data Map. We were also informed that TfN utilises Microsoft Azure to ensure role-based access control. TfN also utilises web-based systems which have tiered access rights and multi-factor authentication. TfN has a documented IT Policy which details how the organisation ensures that appropriate measures are put in place to protect corporate information and the Information Technology Services (ITS), systems, infrastructure and equipment of TfN. We noted that the IT Policy referred on page 6 to the 'General Data Protection Act 2016'. Whilst no formal management action is raised, at the next update it should be clarified whether TfN intended to reference the General Data Protection Regulation 2016, or the Data Protection Act 2018.
Management Action	None.

ICO Area: Data storage and retention	
Area 5	TfN has identified systems and applications used to retain and store data. There is a Record Retention Policy in place.
Findings / Implications	The Record Retention Policy was last reviewed in January 2022. The Policy sets out the length of time that TfN's records should be retained and the processes for disposing of records at the end of the retention period.
Management Action	None.

ICO Area: Data Privacy Impact Assessment	
Area 6	A documented Data Privacy Impact Assessment (DPIA) template has been developed. A DPIA is a process which helps an organisation to identify and reduce the data protection risks of a project. An effective DPIA should be used throughout the development and implementation of a project, using existing project management processes. A DPIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the rights of the individuals involved.
Findings / Implications	TfN has a documented DPIA template which should be completed at the beginning of any major project involving the use of personal data, if there is a significant change to an existing process, or a risk of a personal data breach (it should be noted that we were not provided with any examples of completed DPIAs during our review). As detailed above (at Area 1), TfN should ensure that any DPIA information is captured within the ROPA.
Management Action	None.

ICO Area: Awareness			
Area 7	TfN distribute emails to staff in relation to current data protection issues to raise awareness. Members of staff employed by TfN are made aware of their GDPR obligations through relevant training.		
Findings / Implications	We were provided with a recent example of raising awareness detailing a phishing attack. Furthermore, we were informed by the IT and Information Manager that TfN is currently looking into incorporating Office 365 phishing tests into the organisation. The Senior Lawyer and IT and Information Manager informed us that members of staff employed by TfN are made aware of their GDPR obligations through induction training (evidenced through a report showing recent new starters who have received an induction). The induction course features a series of videos around GDPR, different types of data and the risks of data breaches and how to safely share data. We were provided with a copy of the training which covers the following areas: • Personal Data; • Data Protection Principles; • Data Breaches; • Subject Rights; • Governance and Accountability; • Key Tasks of the DPO; • Fines; and • New Concepts. At the end of the training, staff are required to complete a quiz to assess their understanding of GDPR from the training. Although training and staff awareness has been completed as part of induction training, we noted that this training is only refreshed periodically after induction. It would be prudent to provide annual refresher training, to ensure that staff are sufficiently trained and aware of current GDPR requirements.		
Management Action 2	Refresher training for existing staff will be undertaken annually to reflect GDPR requirements.	**Responsible Owner:** Data Protection Officer	**Date:** 31 March 2023

ICO Area: Data policy, roles and responsibilities			
Area 8	A Data Protection Policy is in place, which has been updated and references the changes as a result of the GDPR.		
Findings / Implications	We confirmed that TfN has a Data Protection Policy which was last reviewed in January 2022. The Policy includes information relating to: • Key Definitions; • Responsibilities; • Data Protection Code of Practice; • Data Subject Access Requests; and • Data Breach Procedure and Communications Plan. Through review of the Policy, we noted that it does not reflect current roles and responsibilities in relation to data protection. The Policy makes reference to the Head of Legal Services in their capacity as Monitoring Officer and the Data Protection Officer for the organisation. As such, this needs updating. We also noted that the version control table had been maintained, but the date in the footer had not been updated.		
Management Action 3	The Data Protection Policy will be reviewed and updated to ensure that it reflects current roles and responsibilities. The date in the footer will be updated to align to the version control table.	**Responsible Owner:** Data Protection Officer	**Date:** 31 March 2023

ICO Area: Data policy, roles and responsibilities			
Area 9	TfN has a number of individuals assigned with data protection responsibilities. These include: • Monitoring Officer; • Senior Lawyer; • Governance, Data Protection and Contracts Lawyer (also designated as the Data Protection Officer) • and • IT and Information Manager.		
Findings / Implications	Through discussions with the Senior Lawyer and IT and Information Manager we were provided with a role profile for the Governance, Data Protection and Contracts Lawyer which details the responsibility to act as TfN's Information Officer and Data Protection Officer working with senior managers across the organisation to ensure on-going compliance with the Data Protection Act (including UK GDPR) and Freedom of Information Act and wider information law including maintenance of TfN's Publication Scheme. This role was filled on an interim basis and has now been permanently recruited to and the new lawyer commenced post on 12 December 2022.		
Management Action 4	Management will ensure that the incoming Data Protection Officer receives appropriate training to undertake the role effectively.	**Responsible Owner:** Head of Legal and Monitoring Officer / Senior Lawyer	**Date:** 31 January 2023

ICO Area: Individuals' rights	
Area 10	The GDPR created some new rights for individuals and strengthened some of the rights that had already existed. The GDPR provides the following rights for individuals: • Right to be informed; • Right of access; • Right to rectification; • Right to erasure; • Right to restrict processing; • Right to data portability; • Right to object; and • Rights in relation to automated decision making and profiling. Individuals are informed of their rights through the Data Protection Policy, and Privacy Policy. TfN also has a Data Subject Access Request Procedure in place.
Findings / Implications	Through review of the documentation, we confirmed that both the Data Protection Policy and Privacy Policy provide details on individual rights. The Data Subject Access Request Procedure details the processes in relation to Subject Access Request. We also confirmed that TfN keep a record of Subject Access Requests, we reviewed the template log and we were informed that no Subject Access Requests have been received.
Management Action	None.

ICO Area: Consent – Seeking Consent	
Area 11	TfN has defined its process for seeking, obtaining and recording consent, to ensure that personal data is handled in line with changes in those processes contained within the GDPR, including where explicit consent is obtained.
Findings / Implications	As identified at Area 10 above, TfN has a Privacy Policy outlining how it uses personal data and records that come under the GDPR. We confirmed that the Privacy Policy details which personal data TfN holds and how this data is used. The Privacy Policy also details the lawful basis upon which TfN collects and uses personal information. Through review of the TfN website, we confirmed that the Privacy Policy is available on the public website. TfN also ensures that, where necessary, it records explicit consent. This includes specific information related to photograph/ video usage. Given that TfN was formed in 2018, there was no need to undertake an exercise to identify whether explicit consent has previously been obtained and therefore, whether retrospective consent is required.
Management Action	None.

ICO Area: Data Breaches	
Area 12	A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal details. This means that a breach is more than just losing personal data. TfN has a Data Breach Procedure which details how to identify a data breach and the resulting actions to take. The procedure is supported by the data protection incident reporting form.
Findings / Implications	TfN Data Protection Policy includes a Data Breach Procedure as an appendix. We confirmed that the procedure includes guidance in relation to the response and reporting of a personal data breach. The procedure is supported by the data protection incident reporting form. Through discussions with the Senior Lawyer and IT and Information Manager we were informed that TfN maintains a Data Breach Log. We were informed that there had not been any data breaches during 2021/22. We noted that there may be a possible risk of under-reporting which could be a result of the lack of refresher training for current TfN staff.
Management Action	None.

APPENDIX A: SCOPE

Scope of the assignment

The scope of the assignment has been agreed by management as follows:

1. **Business processes and data discovery**

Based on the documentation and information provided inspection of the management control processes designed to identify and document all in scope data across the organisation. Related data inflows and outflows focussing in particular on:

- the existence of process and data mapping;
- processes to classify data;
- identification of data flows to third parties; and
- methods of data storage and transfer.

2. **Third parties**

Based on the assessment set out at (1), we will carry out the following:

- inspection of the methods used to identity third parties to whom the 'in scope' data is transferred.
- identification of methods used to assess contractual data confidentiality existence and coverage.

3. **Data ownership**

- Based on the documentation and information at 1 above, note the existence of processes used to identify/allocate data owners.

4. **Data security system level controls**

- Test data security controls agreed by you over data inflow, data repository and data outflow and report results by reference to recognised good practice.

5. **Data storage and retention**

- Based on documentation and information at 1 above, comment on the existence of data retention and storage policies.

6. **Awareness**

- Based on the documentation and information at 1 above, comment on the existence of GDPR awareness processes.

7. Data policy, roles and responsibilities

- Based on the documentation and information at 1 above, comment on the existence and scope of current data policies.
- Based on the documentation and information at 1 above, comment on the existence and designation of data protection roles and responsibilities.
- Comment on current roles by reference to recognised good practice.

8. Individuals' rights

- Based on the documentation and information at 1 above, comment on the existence of procedures for updating, deleting, and reporting personal data at department and organisation level.

9. Consent

- Based on the documentation and information at 1 above, comment on the existence of processes in place to capture data consent.

10. Data breaches

- Based on the documentation and information at 1 above, comment on processes in place for the detection, reporting and investigation of personal data breaches.

Limitations to the scope of our work:

- The assignment is delivered as 'agreed upon procedures' and therefore will not result in a formal assurance level or opinion;
- The scope of our work is limited to those areas examined and reported upon in the context of the objectives set out above. It should not, therefore, be considered as a comprehensive review of all aspects of compliance with the principles of the GDPR;
- The audit will confirm the presence or absence of controls rather than detailed testing of specific areas or an assessment of whether policies and procedures are fit for purpose;
- The information in the report should therefore not be considered to detail all areas where error, risks or areas of non-compliance may exist either now or in the future;
- IT related controls are outside the scope of this review;
- The information provided in our review does not replace or negate the need for professional legal advice. We will not confirm compliance with GDPR and / or provide any legal or regulatory advice;
- The results of our work are reliant on the quality and completeness of the information provided to us; and
- Our work does not provide any guarantee against errors, loss or fraud or provide an assurance that error, loss or fraud does not exist.

Debrief held	22 November 2022
Draft report issued	23 November 2022
Responses received	5 December 2022
Final report issued	7 December 2022
Revised final report issued	22 December 2022 3 January 2023

Internal audit Contacts	Lisa Randall, Head of Internal Audit lisa.randall@rsmuk.com / 07730 300 309 Alex Hire, Senior Manager alex.hire@rsmuk.com / 07970 641 757 Ciaran Barker, Assistant Manager ciaran.barker@rsmuk.com / 01782 216 000
Client sponsor	Paul Kelly, Finance Director
Distribution	Paul Kelly, Finance Director Emma Young, Senior Lawyer Danny Chapman, IT and Information Manager

rsmuk.com