

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

IA AUDIT PROGRAMME AND RISK/CONTROL EVALUATION

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
<b>Risk area: Roles and responsibilities</b>				
<b>Risk:</b> Lack of awareness of GDPR responsibilities				

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
1.	<p>There is an appropriate structure in place, comprising:</p> <ul style="list-style-type: none"> <li>A central team, which provides guidance, advice, monitoring etc on GDPR matters.</li> <li>The TfL business areas, who in the course of their day-to-day operations, are undertaking measures to ensure compliance with the relevant GDPR laws, regulations and policies.</li> </ul>	Determine if such a structure exists.	<p>A central Privacy and Data protection team headed by James Newman consisting of 4 individuals provide guidance , advice to ensure all business areas as aware and taking steps to be GDPR complaint.</p> <p>GDPR team</p> <p>James as part of this venture has sent out GDPR comms to various directorates for allowing GDPR preparation to get commenced .</p> <p>Presentations have been delivered to the following :</p> <p>TfL Analysts Conference" (last September), members of the IRM Stakeholder Network (last month) and colleagues from the following departments</p> <ul style="list-style-type: none"> <li>Employment Law Team</li> <li>Planning</li> <li>Commercial (a number of</li> </ul>	

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
			<p>teams)</p> <ul style="list-style-type: none"> <li>• London Transport Museum</li> <li>• TfL Online</li> <li>• Contact Centre Operations</li> <li>• HR Services</li> </ul> <p>Does it cover all subsidiaries?</p> <p>James email dated 16<sup>th</sup> June</p> <p>Questionnaire was sent to all 60 custodians to get info on where they are with the GDPR prep</p>	
2.	The central team has appointed data	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> </ul>	We don't have a data protection officer appointed as yet. James	

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	protection officer for the whole of the business or individual appointments for each legal entity and/or jurisdiction	<ul style="list-style-type: none"> <li>Review any such documents.</li> </ul>	<p>does carry out duties of a DPO but his official title does not reflect his role and responsibilities.</p> <p>However as per GPDR all public limited are required to appoint a DPO</p>	
3.	GDPR duties are included in the job descriptions of the staff who have specific DP responsibilities.	Review a sample of job descriptions to determine if this is the case.		
4.	The central team provides support, guidance and advice to the various teams in the execution of the GDPR duties.	Interview the relevant person to find out.	<p>Same as 1 above the emails sent by James to business areas/key stakeholders is dated jan 2016 . any latest communication ?</p> <p>Refer james email 16<sup>th</sup> June</p>	
<b>Risk area:</b> Progress towards meeting the 12 steps				
<b>Risk:</b> Failure to comply with the 12 steps effectively				
5.	Central team has taken measures to ensure	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> </ul>	The central team has sent emails to all stakeholders to educate	

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	that all business areas are complying with the 12 steps	<ul style="list-style-type: none"> <li>Review relevant documentation and testing spreadsheet</li> </ul>	them about the GDPR rules. James sent	
6.	<p>All Personal data custodians (PDC) are aware of the new GDPR regulations</p> <p>Awareness – GDPR step 1</p>	<p>Interview the person/ review the questionnaire</p> <p>Testing spreadsheet GDPR steps (1) – point 1</p>	<a href="#"><u>A questionnaire was sent to all the PD custodians. The questionnaire had all questions relating o GDPR awareness.</u></a>	
7.	<p>Business areas/PDC have plans in place to review the nature of personal data being collected, its access storage, retention,</p> <p>Information you hold- GDPR step 2</p>	<p>Interview the person/ review the questionnaire</p> <p>Testing spreadsheet GDPR steps (1) – point 2</p>	<a href="#"><u>A questionnaire was sent to all the PD custodians. The questionnaire had all questions relating o GDPR awareness.</u></a>	
8.	<p>We have reviewed current privacy notices and put a plan in place for necessary changes in time for GPDR implementation.</p>	<p>Interview the person/ review the questionnaire.</p> <p>Testing spreadsheet GDPR steps (1) – point 3</p>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	Communicating privacy information -- GDPR step 3			
9.	Plans are in place to update all procedures to ensure it covers all rights individuals have, including how personal data will be deleted or provide data electronically and in a commonly used format (Data Portability).  Individuals' rights --- GDPR step 4	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (1) – point 4		
10.	Policies and procedures are being set up to demonstrate the reasons/criteria why we refuse a	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (1) – point 5		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	subject access request and also to capture, record and act on those requests.  Subject Access requests--- GDPR step 5			
11.	We have identified the legal basis for various types of data processing we carry out and document it.  Legal Basis for processing personal data--- GDPR step 6	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (1) – point 6		
12.	All business areas have put/are putting processes in place to review the ways in which TfL obtains consents	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (2) – point 7		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	Consent- GDPR step 7			
13.	We have reviewed and updated our systems that can verify individuals' ages and if the user is a child to gather parental or guardian consent for the data processing activity  Children - GDPR step 8	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (2) – point 8		
14.	We have drafted or are drafting procedures to detect report, manage, investigate and record a personal data breach  Data breach- GPPR step 9	Interview the person/ review the questionnaire  Testing spreadsheet GDPR steps (2) – point 9		
15.	Any instances of non-compliance are logged and analysis undertaken to identify trends in	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> </ul>		



<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	non-compliance; vital in preventing minor data protection breaches from becoming an issue.			
16.	Processes have been established for reporting data breaches to the data protection officer to ensure that data breaches are brought to the attention of the regulator within the time frames laid down by the GDPR.  Breach notification procedures are being tested regularly to ensure that they are being followed and are working effectively before the GDPR act comes in force next year	Review if this is the case		
17.	IG Investigates any	<ul style="list-style-type: none"> <li>Interview the relevant</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	<p>actual or suspected unauthorised disclosure of personal data and recommending measures to prevent the reoccurrence of such breaches.</p> <p>In case of data breach, Process is in place to make the Senior management aware of it and provide adequate support to prevent it from occurring .</p>	<p>person to find out.</p> <ul style="list-style-type: none"> <li>Obtain any evidence of this</li> </ul>		
18.	<p>We have put plans in place to review and updated our existing compliance procedures and also assessed the situations where it will be necessary to conduct a DPIA.</p> <p>Data Protection by Design and Data</p>	<p>Interview the person/ review the questionnaire</p> <p>Testing spreadsheet GDPR steps (2) – point 10</p>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	Protection Impact Assessments DPIA- GPPR step 10			
19.	<p>We have a designated a Data Protection Officer (DPO) on group wide basis.</p> <p>Data Protection Officers- GPPR step 11</p>	<p>Interview the person/ review the questionnaire/Job description</p> <p>Testing spreadsheet GDPR steps (2) – point 11</p>		
20.	<p>We have plans to put a process in place to review the processing of personal information carried out on behalf of TfL in countries outside of the EEA and have assessed whether they are protected by adequate safeguards to support GDPR.</p>	<p>Interview the person/ review the questionnaire</p> <p>Testing spreadsheet GDPR steps (2) – point 12</p>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	International - GPPR step 12			
21.	There are policies in place that have been reviewed by central team to ensure that all business areas keep records of the ways in which they are processing personal info	Review policies and interview the person		
<b>Risk:</b> No training provided to areas involving high risk or high volume processing				
8	Bespoke training and/or workshops provided to areas of organisation which involve high risk or high volume processing,	<ul style="list-style-type: none"> <li>Determine if this is the case.</li> </ul>		
<b>Risk area: Policies and procedures</b>				
<b>Risk:</b> Absence of policies and procedures, resulting in unsatisfactory performance, which can lead to breaches of the relevant				

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
legislation				
22.	<p>The responsibility for developing policies aimed at ensuring compliance with the GDPR Act and other GDPR legislation has been appropriately assigned. Eg: Data portability and data deletion rights, right to be forgotten.</p> <p>(step 3 (a) of Practicalities of implementing GDPR compliance programme)</p> <p>The link is Article on GDPR programme – PL &amp; B report</p>	<p>Interview the relevant person to find out.</p> <p>Determine if the exercise to determine which provisions of the GDPR will apply to TfL has been undertaken</p>		
23.	There are draft policies in place for ensuring compliance with the GDPR Act and	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> <li>Review any policies, and determine if they</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	<p>other GDPR legislation.</p> <p>The policies cover the key GDPR requirements.</p> <p>(step 3 (a) of Practicalities of implementing GDPR compliance programme.</p> <p>The key areas are:</p> <ul style="list-style-type: none"> <li>➤ how to</li> <li>➤ recognize and comply with individuals rights;</li> <li>➤ how and when your organisation uses data protection impact assessments;</li> <li>➤ dealing with data breaches and the notification of data</li> </ul>	<p>cover the key areas.like</p> <ul style="list-style-type: none"> <li>• definition of Personal data</li> <li>• procedures for collection and use of sensitive personal data</li> <li>• for secure destruction of personal data</li> <li>• Maintain Data Privacy Policy</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	breaches; and ➤ the organisational and technical security measures in place to safeguard personal data			
24.	<p>Appropriate measures have been put in place to comply with GDPR requirements. The measures implemented have been tested to ensure that these are working as anticipated. For example, implementing background screening of employees with access to sensitive financial data to ensure that data is kept secure.</p> <p>(step 3 (c) of Practicalities of implementing GDPR</p>	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	compliance programme			
25.	The policies are underpinned by more detailed corporate and local guidance and procedures, which cover all the key areas.	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Review any procedures and determine if they cover the key areas.</li> <li>• Determine if they are structured and written in an easy to use format</li> <li>• They are readily accessible to all individuals within TfL who handle personal data.</li> </ul>		
26.	The responsibility for developing procedures and guidance for ensuring compliance with GDPR legislation in the business areas has been appropriately assigned.	Interview the relevant persons in a sample of business areas to find out.		



<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
27.	<p>There are procedures for ensuring that where appropriate (eg where a third party processes personal data for TfL), contracts between TfL and third parties include adequate clauses for complying with the GDPR Act and other GDPR legislation and cover off any additional risks (and liabilities) TfL may face in the event of a breach</p> <p>This will entail TfL Commercial involving IG early in the procurement process to ensure the GDPR implications and requirements are ascertained, and the relevant clauses included in the contract.</p>	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Review any procedures and also ensure that the third party has a right to have access to the data in the first place.</li> <li>• Test a sample of contracts for compliance.</li> <li>• Review if the clauses required as per Article 28 are now included in the contracts. Refer Testing spreadsheet.</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	step 3 (d) of Practicalities of implementing GDPR compliance programme			
28.	There are procedures for ensuring input from the central team for all projects, schemes or initiatives that have a GDPR aspect, in order to ensure compliance with the GDPR Act.	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Obtain examples of such projects/initiatives.</li> </ul>		
29.	IG has a means of becoming aware of the new GDPR legislation, regulations, standards etc or changes to existing ones that will affect TfL.	Interview the relevant person to find out.		
30.	The policies and guidance have been effectively communicated to all	Obtain evidence of the communication of policies and guidance to TfL employees.		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	TfL employees.			
31.	Any procedures or guidance have been effectively communicated to the relevant staff in the business areas.	Obtain evidence of the communication of procedures to the relevant employees.		
32.	We have introduced appropriate technical and organizational measures to demonstrate compliance to the accountability principles.	<ul style="list-style-type: none"> <li>Interview the person and review if we have drafted internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies</li> <li>Refer testing spreadsheet accountability principle tabs</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
<b>Risk:</b> Failure to keep policies and procedures up to date				
33.	The responsibility for reviewing the policies and procedures to ensure they are current has been appropriately assigned.	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Obtain evidence of reviews to ensure currency.</li> </ul>		
34.	<p>Independent testing and quality assurance frameworks are established to ensure that data protection processes and procedures are being adhered to.</p> <p>step 3 (e) of Practicalities of implementing GDPR compliance programme</p>	<ul style="list-style-type: none"> <li>• Review if this is the case</li> </ul>		
<b>Risk area: Risk management</b>				
<b>Risk:</b> Absence of an effective risk management process				

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
35.	The DPO has been assigned the responsibility to work with each business area to identify the level of privacy risks that TfL is exposed to and how they can be mitigated.	<p>Review whether the level of privacy risk is determined based on what personal data is processed, why is it processed who is it shared with and location in which it is processed.</p> <p>Review the data mapping exercise as set out in Article 30 that requires data controllers to maintain a record of processing activities</p> <p>Test spreadsheet</p>		
36.	Information Governance maintains a corporate risk register, on which key GDPR risks and the processes for managing them, as	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Review the risk register if there is one.</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	well as any planned corrective action are recorded. Risks and associated actions are regularly reviewed and updated.  If the register is kept outside of ARM, risks are transferred to ARM when appropriate.			
37.	The responsibility for maintaining the register has been appropriately assigned.	Determine if this responsibility has been assigned, and if so, to the appropriate person.		
38.	Where relevant, business areas have included GDPR risks (Privacy risks) in their risk registers.	For a sample of business areas: <ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Review the risk register if there is one.</li> </ul>		
<b>Risk area: Monitoring of actions to ensure compliance</b>				
<b>Risk:</b> Non-compliance, potentially resulting in fines and/or reputational damage to TfL				

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
39.	TfL has a steering group and small sub-groups that meet regularly to ensure that the scope of GDPR work is clear and deadlines can be met.  (Checklist as per practicalities of implementing a GDPR compliance programme)	Interview the relevant person to find out. And review minutes/actions/outcomes		
40.	The DPO has build a compliance program for GDPR	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Ensure that the program incorporates training and awareness-raising programs.</li> </ul>		
41.	The responsibility for reviewing and updating existing compliance	Interview the relevant person to find out.		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	procedures has been assigned.			
42.	An implementation plan has been prepared identifying discrepancies between the controls called for by the GDPR and the actual practices in TfL and contains targeted actions relevant to specific areas within organization to close the compliance gap	Review if this is the case		
43.	In accordance with the Privacy and GDPR Policy, IG:  Provides advice and guidance on the implementation and interpretation of the policy	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> <li>• Obtain any evidence of this.</li> </ul>		
44.	IG promotes and enforces compliance	<ul style="list-style-type: none"> <li>• Interview the relevant person to find out.</li> </ul>		



<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
	with the policy (compliance with which will result in adhering to the GDPR Act) by conducting a gap analysis of current data protection processes against GDPR requirements to identify work streams.	<ul style="list-style-type: none"> <li>Obtain any evidence of this.</li> </ul>		
45.	IG Liaises with the Information Commissioner's Office on any matter relating to TfL's compliance with the GDPR Act and/or the Privacy and DP Policy.	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> <li>Obtain any evidence of this.</li> </ul>		
46.	The responsibility for monitoring and ensuring compliance with the GDPR clauses of contracts with third parties has been appropriately assigned.	<ul style="list-style-type: none"> <li>Interview the relevant person to find out.</li> <li>If possible, review a sample of contracts to determine if there is any monitoring.</li> </ul>		

<b>Audit Ref:</b>	IA 17 108	<b>Audit Title:</b>	Preparation for GDPR
-------------------	-----------	---------------------	----------------------

Ref	Expected Control / Risk Mitigation	Test	Results & Supporting Evidence	Evaluation & Conclusion
47.	In order to enable senior management to play an oversight and monitoring role, IG regularly reports on key aspects of DP, GDPR, including any breaches, to an appropriate level of senior management	Interview the relevant person to find out.		