

EDMOND

Assessment Template	TfL Data Protection Impact Assessment 2.0
Assessment Workflow	TRUSTe Default Workflow
Assessment Description	-
Division	-
Subsidiaries	-
Assessment Labels	-

Created By	Lee McGirr
Date Created	Mar 13, 2017
Last Modified	May 30, 2017
Assessment Age	78 days

Assessment Owner	Lee McGirr
Approvers	Lee McGirr - Approved
Respondents	Aled Davies

Assessment Status	12 - <i>Completed</i> 0 - <i>In Progress</i> 0 - <i>Not Started</i>
Issues by Risk	0 - <i>Unspecified</i> 0 - <i>Critical</i> 0 - <i>High</i> 0 - <i>Med</i> 0 - <i>Med-Low</i> 0 - <i>Low</i>
Tasks	3 - Done 0 - Pending

∨ **Comments and Attachments**

No Comments

Assessment

Will TfL be processing personal data?

Personal data means data which relates to a living individual who can be identified either: (1) from that data; or (2) from that data in combination with other data which is in the possession of (or is likely to come into the possession of) TfL. Personal data is not just an individual's name, image or contact details. If TfL is able to identify an individual using any form of unique identifier this should be viewed as their personal data. The definition also specifically includes opinions about the individual, or details of any planned course of action which will directly affect them (eg a pending prosecution for fare evasion).

1

Below are some categories of personal data routinely processed by TfL. Please select all of those that will be processed in connection with this project or initiative. If it involves the processing a category of personal data not included as an option, please select "Other" and provide further details.

Status	No Issues
Response	None
Recommendation	-
Comments & Attachments	<p>Aled Davies commented on 3/16/17 11:19 AM</p> <p>"No personal data will be processed as part of this project however some datasets derived from personal data will be used. Therefore this assessment has been completed to highlight this and to explain the safeguards put in place to protect data, whether personal or otherwise."</p>

2

Will information which falls within any of the following special categories of sensitive personal data be processed as a result of this project or initiative?

Status	No Issues
Response	No
Recommendation	-
Comments & Attachments	

Personal Information Custodian approval

TfL's Privacy and Data Protection Policy states that a Personal Information Custodian ("PIC") is the senior manager (normally a Director or Head of Department) responsible for the way in which personal data is processed within their assigned area of control. PIC's are responsible for:

1. Ensuring that TfL personnel within their area of control are aware of this policy and are adequately trained in the handling of personal data
2. The assessment and reporting of privacy risk associated with the processing of personal data within their area of control
3. Ensuring that a DPIA is carried out as part of the development and implementation of any new/amended business process or IT system which is to be used to process personal data
4. Implementing appropriate procedures to ensure compliance with restrictions on the processing of personal data within their area of control

3

Do you have approval from the relevant Personal Information Custodian(s) to proceed with this project or initiative?	
Status	No Issues
Response	Yes
Recommendation	
Comments &	

Attachments

3.1

Please confirm the name(s) and job title(s) of the Personal Information Custodian(s) who approved this project or initiative? Please attach appropriate evidence, for example an email approval or signed Statement of Work (SOW)/Project Initiation Document (PID).	
Status	No Issues
Response	Alex Williams, MD City Planning
Recommendation	-
Comments & Attachments	<i>No comments</i>

Overview and business case

4

Please provide a brief description of this project or initiative and attach a simple data flow diagram below. You can also attach a copy of your business case, statement of works (SOW) or project initiation document (PID).

Status	No Issues
Response	Estimating Demand from Mobile Network Data (EDMOND) involves setting up a 4 year contract (via a full OJEU process) to procure trip pattern and other data in a format suitable for input to TfL's Strategic and Tactical highway models. The project will use mobile phone data as a primary source with other TfL and external data sources fused as required (full methodology not known until completion the first phase of the project).
Recommendation	-
Comments & Attachments	<p>Robin Forrest commented on 5/9/17 3:01 PM Attachment #1: EDMOND DPIA Data Source List.pdf</p> <p>Robin Forrest commented on 3/16/17 11:31 AM "Draft - attach data flow diagram"</p>

5

Please provide an overview of the benefits to TfL and its stakeholders (including customers and/or employees) and explain how those benefits outweigh any potential impact on the privacy of the individuals whose data will be processed. Include any regulatory, operational or commercial benefits.

Status	No Issues
Response	<p>Commercial benefits: Better quality data on trip patterns feeding into TfL's models, providing better quality modelling to support long term policy and infrastructure investment decisions.</p> <p>Operational Benefits: Eliminates disruption to the road network brought about by the need to stop vehicles for survey purposes. Provides data that can be used for other TfL use cases such as multi-model transport planning and fills gaps in our understanding of travel by National Rail. Benefits to TfL customers/employees: Replaces the need for more disruptive data collection methods involving stopping vehicles on the road for interview. Customers such as boroughs and developers that use our model (through our accreditation and licensing process) get access to better quality models which reflect current trip patterns more accurately and lead to better assessment of scheme/ policy impacts.</p>
Recommendation	-
Comments & Attachments	

6

--	--

Please provide details of any previous DPIA (or Privacy Impact Assessment) carried out in relation to any elements of this project or initiative. You can also attach a copy below.

Status	No Issues
Response	Privacy impact assessment completed 08/10/2015
Recommendation	-
Comments & Attachments	<i>No comments</i>

Stakeholders

7

Has everyone directly involved in the design and delivery of this project or initiative completed TfL's "My role in privacy and data protection" (<http://intranet.tfl/our-organisation/information-governance/managing-personal-information/training-and-awareness.aspx>) eLearning course?

Status	No Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

8

From the list provided, please identify all of the relevant internal stakeholders for this project or initiative.

Status	No Issues
Response	Other, Commercial (procurement), Press Office, Legal, Information and Records Management Team
Recommendation	
Comments &	

Attachments

8.1

Please provide details of any other relevant internal stakeholders, outside of your immediate team/department.

Status	No Issues
Response	Others: Road Space Management (Surface), Analytics, Transport Planning (Surface), Strategy & Planning (Surface),
Recommendation	-
Comments &	

Attachments

9

From the list provided, please identify all of the relevant external stakeholders for this project or initiative.

Status	No Issues
Response	Customers and/or members of the public, Contractors/consultants, Information Commissioner's Office
Recommendation	

Comments & Attachments	
9.1	Please select the type of consultation exercise conducted with customers and/or members of the public. Please also attach any supporting evidence/outcomes (research reports etc).
Status	No Issues
Response	Focus groups
Recommendation	-
Comments & Attachments	<i>No comments</i>

10	Have you already notified all of the internal and external stakeholders identified in your responses to questions two and three, about this project or initiative?
Status	No Issues
Response	Yes
Recommendation	-
Comments & Attachments	

11	Have any of the internal or external stakeholders for this project or initiative expressed any concerns or reservations about the way in which TfL is intending to process personal data?
Status	No Issues
Response	Yes
Recommendation	-
Comments & Attachments	

11.1	Please provide a summary of their concerns and describe any mitigating actions taken to try and address them. If you believe their concerns do not require any mitigation, please explain why.
Status	No Issues
Response	Concerns were raised due to the processing of aggregate data derived from personal data. The Privacy and Data Protection team have provided input throughout the project and will

	continue to do so. A Privacy Impact Assessment was completed at an earlier stage and this extended DPIA is now being completed. The necessary safeguards were put in place at procurement stage and will continue to be adhered to by TfL and its consultants and sub-consultants throughout the lifetime of the project.
Recommendation	-
Comments &	

Attachments**Suppliers and third parties**

This section covers the use of external service providers to process personal data as a result of this project or initiative; and the disclosure of personal data to third parties (eg statutory law enforcement agencies and local authorities).

12

As part of this project or initiative, will any external service provider(s) be involved in processing personal data on behalf of TfL?

Status	No Issues
Response	No
Recommendation	-
Comments &	

Attachments

13

Will personal data be disclosed to any third party organisation(s) on a routine basis as a result of this project or initiative? Please select all that apply from the list below.

Status	No Issues
Response	None
Recommendation	-
Comments &	

Attachments

Benchmarking

14

Are you aware of any other TfL business area(s) currently undertaking similar processing of personal data?	
Status	With Issues
Response	No
Recommendation	Confirm who.
Comments &	

Attachments

15

Have you identified any other organisation(s) currently undertaking similar processing of personal data?	
Status	No Issues
Response	Yes
Recommendation	
Comments &	

Attachments

15.1

Please specify which organisation(s) and tell us if you have already engaged with them to discuss this project or initiative.	
Status	No Issues
Response	Ahead of the project TfL held meetings with other public sector organisations from across the UK and Ireland, including organisations who have previously undertaken, or are currently undertaking, similar processing of personal data. TfL also carried out extensive industry engagement ahead of the procurement process, including an industry day and market engagement questionnaire. In total TfL engaged with 80 organisations, many of which have undertaken, or are currently undertaking, similar processing of personal data.
Recommendation	-
Comments &	

Attachments

16

Are you aware of any external data privacy or security standards, guidelines or codes of practice which are relevant to this project or initiative?	
Status	No Issues
Response	
Recommendation	
Comments &	

Response	Yes
Recommendation	
Comments &	

Attachments

16.1

Please provide details and include a hyperlink (if available online) or attach copies.

Status	No Issues
Response	Data Protection Act, ICO's guidance ("Big data, artificial intelligence, machine learning and data protection", "Anonymisation")
Recommendation	-
Comments &	

Attachments

Fairness and transparency

17

How will individuals be notified that their personal data is being processed as a result of this project or initiative? For example, using a privacy notice presented at the point of collection (on an online or paper form), signage, an audio announcement, a webpage, etc. Please attach copies of any relevant drafts/designs.

Status	No Issues
Response	TfL are issuing a press release as well as a webpage providing information about the project. All data has been anonymised so individuals can not be identified from the data being processed.
Recommendation	-
Comments &	

Attachments

18

Which of the following processing conditions will apply to this project or initiative?

Status	No Issues
Response	Processing is necessary for the performance of (or to enter into) a contract with the individual
Recommendation	-
Comments &	

Attachments

19

As a result of this project or initiative, will TfL be processing personal data for the purposes of profiling individuals (eg to segment or categorise them based on predetermined criteria)?

Status	No Issues
Response	No
Recommendation	-
Comments &	

Attachments

20

Please provide (or attach) details of the process or mechanism which will allow individuals to access their own personal data (which will be processed as a result of this project or initiative).

Status	No Issues

Response	Information is available on the TfL website: https://tfl.gov.uk/corporate/privacy-and-cookies/access-your-data
Recommendation	-
Comments &	

Attachments

21

Will there be a process or mechanism which will allow individuals to transfer their personal data to another service provider (eg a train operating company or public transport authority) in a machine readable format?	
Status	No Issues
Response	No
Recommendation	-
Comments &	

Attachments

22

Please provide (or attach) details of the process or mechanism which will allow individuals to restrict or prevent the on going processing of their personal data (which will be processed as a result of this project or initiative). For example, opt-out/unsubscribe preferences or the ability to ask for their personal data to be deleted via a dedicated email address or online form.	
Status	No Issues
Response	All data has been aggregated and/or anonymised, therefore there is no mechanism to identify individuals' data in order to remove it from the dataset.
Recommendation	-
Comments &	

Attachments

23

Are there any plans to combine personal data processed as part of this project or initiative with externally sourced data sets (eg bought-in marketing lists or mobile phone tracking data provided by telecoms service providers)?	
Status	No Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

--

23.1

Please provide (or attach) details of the data you will be using and its source(s)?

Status	No Issues
Response	Mobile phone event data provided by Telefonica. Please see attachment in question 4.
Recommendation	-
Comments & Attachments	

Data minimisation and disposal

24

What will be done to ensure that personal data processed as a result of this project or initiative, is relevant and necessary for its stated purpose(s)? For example, cleansing the data to remove any irrelevant content not required to achieve the stated purpose(s).

Status	No Issues
Response	Each dataset will be considered individually to determine which parts of the data are relevant for the purposes of this project and only these parts will be processed.
Recommendation	-
Comments &	

Attachments

25

Will any techniques be used to minimise the amount of personal data being processed as a result of this project or initiative? For example, hashing, tokenising, aggregating or pseudonymising it?

Status	No Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

25.1

Please describe the data minimisation techniques or methodologies you will be using; and the categories of personal data to which they will be applied.

Status	No Issues
Response	As mentioned previously all datasets will be aggregated and/or anonymised.
Recommendation	-
Comments &	

Attachments

26

Have you already identified the retention periods which will be applied to the personal data which will be processed as a result of this project or initiative?

Status	No Issues
Response	

	No
Recommendation	-
Comments & Attachments	Robin Forrest commented on 5/9/17 2:30 PM "Personal data will not be stored as part of this project."

Data accuracy and quality

27

What will be done to ensure that the personal data processed as part of this project or initiative is as accurate as possible (for example a validation process and/or allowing individual data subjects to update their details using an online account)?

Status	No Issues
Response	Inferences drawn from the processing of the mobile data will be verified and validated as part of the project to ensure that conclusions drawn are as accurate as possible.
Recommendation	-
Comments & Attachments	

Data storage and security

28

How will personal data processed as a result of this project or initiative be stored? Please select all of the relevant locations.

Status	No Issues
Response	On premise - Service provider IT infrastructure
Recommendation	-
Comments & Attachments	<p>Robin Forrest commented on 3/16/17 12:08 PM</p> <p>"No personal data will be stored as part of this project. All of the O2 data is anonymised by eliminating personal data (such as name, address, phone number) and hashing it with an ID. IDs are aggregated to crowd level, so that no individuals are identifiable. Our servers will be partitioned with access only allowable through authorised users. No information will be stored on hard drives of machines."</p>

29

Where will personal data be physically located whilst being processed (including stored)?

Status	No Issues
Response	UK
Recommendation	
Comments & Attachments	<p>Robin Forrest commented on 3/16/17 12:09 PM</p> <p>"No personal data will be stored. O2 have strict privacy controls in place to keep customers' data safe and secure within a dedicated data warehouse, and only aggregated insights showing the behaviour of crowds is passed to clients. Our servers will be partitioned with access only allowable through authorised users. No information will be stored on hard drives of machines."</p>

30

Who will have access to personal data processed as a result of this project or initiative? Please provide the names of relevant roles and teams (within TfL and any external service providers or partner organisations identified in Question 12), not the names of specific individuals.

Status	No Issues
Response	O2 does handle personal data. However, the data that reaches the SmartSteps database (which will be used for this project) is not considered personal due to the processing that has

	occurred prior to the data entering the database. In relation to the data on the SmartSteps database and other project information, only authorised users will be allowed to access information with the partition of our server space.
Recommendation	-
Comments &	

Attachments

31

Will individuals with access to personal data as a result of this project or initiative be subject to any screening or vetting? For example, Disclosure and Barring Service ("DBS") or financial probity checks.

Status	No Issues
Response	The project team will have no access to personal data. All events processed are by-products of the core telephony network with the records anonymised prior to being stored in the analysis platform, so all analysis of behaviour is done in a completely anonymous separate environment.
Recommendation	-
Comments &	

Attachments

32

How will access to the personal data processed as a result of this project or initiative be restricted and controlled? Please select all that apply.

Status	No Issues
Response	Read-only system access, Password protected user accounts
Recommendation	-
Comments & Attachments	Robin Forrest commented on 3/16/17 12:09 PM "We envisage no personal data will be stored. However, we will ensure that all electronic storage folders will access permissions with password protected user accounts. There will also be read-only system access to relevant files."

33

If an individual (including the data subject themselves; a colleague from a business area or service provider that doesn't normally have access to the data; or any other third parties) requests access to personal data processed as a result of this project or initiative; will there be a procedure in place to verify their identity and ensure that they are authorised to see it?

Status	No Issues
---------------	-----------

Response	No
Recommendation	-
Comments &	

Attachments

34

What other measures and controls will be in place to protect personal data processed as a result of this project or initiative? Please summarise the relevant safeguards under each of the following three headings:

Physical - access (eg secure office space and storage cabinets); clear desk policy; confidential waste disposal arrangements; etc

Technological - encryption; anti-virus; firewalls; intrusion detection; Data Loss Prevention ("DLP"); etc

Organisational - documented policies and procedures; information asset registers; retention and disposal schedules; training; etc

Status	No Issues
Response	No personal data will be stored. No confidential information for this project will be stored on hard drives or in paper format on desks. Encryption of protected files received will be put in place. A register of all incoming files and their locations will be kept.
Recommendation	-
Comments &	

Attachments

35

Have you discussed your project or initiative with the TfL Cyber Security and Incident Response Team (CSIRT)?

Status	With Issues
Response	No
Recommendation	Please contact CSIRT (cybersec@tfl.gov.uk (mailto:cybersec@tfl.gov.uk)) to discuss any cyber security risks and/or issues associated with this project or initiative before completing this DPIA questionnaire.
Comments &	

Attachments

Assurance and complaints

36

Is there a documented process for addressing, escalating and resolving privacy and data protection related complaints from individuals whose data will be processed as a result of this project or initiative?

Status	No Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

36.1

Please describe (or attach a copy of) the relevant process for dealing with privacy and data protection related complaints.

Status	No Issues
Response	Process will be described on the webpage. Any queries or complaints can be addressed to privacy@tfl.gov.uk .
Recommendation	-
Comments &	

Attachments

37

Is there a documented process for monitoring on-going compliance with privacy and data protection requirements as part of this project or initiative?

Status	No Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

37.1

Please describe (or attach a copy of) the process which will be used to monitor compliance with privacy and data protection requirements.

Status	No Issues
Response	

	The privacy and data protection requirements will be raised regularly at project management and methodology workshops to ensure that these have a high profile as the project progresses. This DPIA will be reviewed and if necessary updated at quarterly intervals to keep it up to date and relevant.
Recommendation	-
Comments &	

Attachments**Open data**

38

Do you intend to make any data or analysis derived from the processing of personal data as a result of the project or initiative, available in connection with TfL's transparency and/or open data obligations?

Status	With Issues
Response	Yes
Recommendation	-
Comments &	

Attachments

38.1

Please provide details of where the data or analysis will be published; and if appropriate, how it will be pseudonymised/depersonalised before publication.

Status	No Issues
Response	Analysis will be freely available but it will not be personal data and therefore will not require pseudonymisation/depersonalisation.
Recommendation	-
Comments &	

Attachments

Tasks

Priority	Task Name	Type	Assigned To	Created By	Due Date	Status
----------	-----------	------	-------------	------------	----------	--------

Logs

Date Created	Action	Taken By
5/30/17 11:58 AM	Project Approved	
5/30/17 11:58 AM	Approval Completed	
5/30/17 11:56 AM	Acceptance Completed	
5/17/17 9:36 AM	Survey Submitted	
5/17/17 9:36 AM	Survey Completed	
3/16/17 11:21 AM	Survey Submitted	
3/14/17 11:20 AM	Survey Sent	
3/14/17 11:20 AM	Project Published	
3/13/17 9:13 AM	Project Created	