F7526 A3 Data Protection Impact Assessment (DPIA) Checklist

Any initiative, project or proposal to change processes that involves the processing of personal information (or the use of privacy intrusive technologies) is likely to give rise to various privacy and data protection concerns. Undertaking a DPIA helps to ensure that data protection risks are identified as soon as possible. A DPIA should continue to be maintained and updated throughout the project lifecycle. The GDPR makes a Data Protection Impact Assessment (DPIA) mandatory for certain types of processing, or any other processing that is likely to result in a high risk to individual's interests.

This assessment tool is designed to examine a new project / initiative, or a significant change to an existing process at an early stage. It will result in an initial assessment of privacy risk and determine which level of further assessment is necessary. The Privacy and Data Protection team will assess the completed DPIA and may request further information to assist in the identification and mitigation of privacy risks.

Your details			
Name:	Lizzie Meadows	Date DPIA completed	07 January 2022
Job title:	Principal Privacy Adviser	Proposed launch date	Data transfer anticipated to take place from 13 January 2022

Name and description of the project:	The technology systems and vehicle licensing services for TfL Taxi and Private Hire (TPH) underwent a competitive re-let exercise during 2020, and a contract was awarded in Spring 2021. Lot 1 was for the '*Provision Of An End To End Information Technology System'* which includes the main taxi and private hire licensing database. This contract was awarded to TCS. Systems and development and testing work is now underway prior to the go live of the solution in 2023. For the internal testing of the systems prior to go live, TCS needs a copy of the entire database from incumbent supplier Marston. Marston will supply (live) production data to TCS (via their subcontractors Civica and Centrality). Upon receiving such data from Marston, TCS has been requested to mask any personal data before it is used for development and testing. No live TPH personal data (in its original raw format) will be used in the development / build of the TPH information technology

	system – ie for system development, unit testing, factory testing, User Acceptance Testing (UAT), System Integration Testing (SIT) or any other form of testing during the system development and testing phase. This DPIA covers the privacy risks associated with the data migration and the data masking solution that has been proposed in order to protect the personal data processed during this testing activity.				
Personal Information Custodian (PIC) or band 5 lead	Graham Robinson – TPH General Manager	Is PIC aware of this DPIA?	Y	Project Sponsor	Rouadi Hanane

A DPIA is **mandatory** in certain circumstances. Please tick each box where it likely that the proposal will meet the criteria:

Use profiling or automated decision-making to make decisions that will have a significant effect on people. Significant effects can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits.		Process special category data (relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life or sexual orientation) or criminal offence data on a large scale.	**X**	Make changes to processes and systems that are likely to result in significantly more employees having access to other peoples' personal data, or keeping personal data for longer than the agreed period.	
Use data concerning children or vulnerable people. A person with vulnerability is usually described as someone who is at a higher risk of harm than others.		Process personal data which could result in a risk of physical harm or psychological distress in the event of a data breach.	**X**	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.	
Systematically monitor a publicly accessible place on a large scale – e.g. through the use of CCTV or Wi-Fi tracking.		Process personal data in a way which involves tracking individuals' online or offline location or behaviour.		Match, compare or combine datasets, or have the potential to deny anonymity or re-identify people.	

Use new technologies or make novel use of existing technologies.		Process personal data on a large scale or as part of a major project.	**X**	Process personal data without providing a privacy notice directly to the individual.	
Use personal data in a way likely to result in objections from the individuals concerned.		Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	**X**
Process biometric or genetic data in a new way.		Undertake systematic monitoring of individuals.		Prevent individuals from exercising a right or using a service or contract.	

Step 1 – Identify the need for a DPIA	
Explain broadly what your project aims to achieve and what type of data and processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	TfL has a statutory responsibility for regulating all taxi and private hire services that operate in London. This includes taxi drivers and vehicles (ie 'black cabs') and private hire vehicles, drivers and operators This aspect of the TPH contract mobilisation work involves testing of the TCS solution designed for the administration/operation of the End To End Information Technology System. The TPH information technology system is essentially a database consisting of the records of prospective, current and previous taxi and private hire drivers, vehicles and operator licensees. It includes information provided by licensees when they apply for or renew a licence together with information sourced from a number of third parties, including but not limited to, the DVLA. Some of the personal data is special category data about medical conditions. There may also be data relating to allegations of committing crime and/or criminal convictions. The migrated data will be stored in a segregated, cloud based service hosted by AWS with the servers physically located in Ireland with back up servers (for disaster recovery etc) hosted in Germany. The current supplier for this system is unable to provide a copy of 'dummy' or pre-masked personal data fields to TCS for testing purposes. Therefore, a copy of the live (production) data has to be migrated to TCS, with subsequent masking of personal data fields applied. For clarity this data includes that which is currently used for the day to day operation/administration of TPH services, as well as 'historical' (static) data which resides in an archive database. TCS has produced a '*production data masking approach'* document which describes the activity in more detail. This DPIA is required due to – • the volume of personal data involved • some of the personal data being special category data (health, criminal convictions/allegations data) • live production data being copied and migrated (and subsequently masked)
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	It is essential that robust testing takes place in order that when the solution moves into 'business as usual,' it is fit for purpose and the data is appropriately protected.

Will the processing directly affect the individuals concerned?	This migration and testing activity (including the data masking) is not intended to have any effect on individuals, - other than to ultimately ensure the security and integrity of the personal data that TfL processes about them.

Step 2: Describe the nature of the processing (You might find it useful to refer to a flow diagram or other description of data flows).		Could there be a privacy risk?
What is the source of the data?	The immediate source of the data for this migration/testing activity is TfL's current supplier Marston. They will be supplying the data via their subcontractors, Civica and Centrality. (The original sources of data from individuals and other third parties is described in Step 1 above.) Marston will be transferring the data in its 'raw' format, with masking subsequently applied by TCS.	Y
Will you be sharing data with anyone?	The data will not be shared with anyone other than TfL's designated Processor (TCS).	N
Are you working with external partners or suppliers?	Yes. TCS is the designated Processor for this migration/masking/testing activity. The cloud solution itself is provided by AWS. The incumbent supplier, Marston, and their subcontractors, Civica and Centrality.	Y
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	Yes. All TfL contracts for services that include personal data processing include privacy and data protection clauses as well as clauses relating to the requirement for regular security and data protection audits. TCS has a contract with their supplier AWS containing EU approved clauses for data protection.	N
What measures do you take to ensure suppliers processing personal data on our behalf provide adequate assurances about their ability to process this data safely and lawfully?	All Taxi and Private Hire tender exercises include privacy and data protection questions at ITT stage and which are evaluated and scored as part of each bidder's tender submission. All TfL contracts for services that include personal data processing include privacy and data protection clauses as well as clauses relating to the requirement for regular security and data protection audits. TCS has a contract with their supplier AWS containing EU approved clauses for data protection.	N

Will the data be combined with, or analysed alongside, other datasets? If so, which ones?	The data will not be combined with or analysed alongside any other datasets as part of the services provided by TCS.	N
Will AI or algorithms be used to make decisions? What will the effect of these decisions be?	This data masking activity may use an algorithm to apply the masking to the personal data fields. The logic used will be subject to TfL approval prior to deployment to ensure that it is robust. There will not be any decisions made about data subjects as a result of this use.	N
How and where will the data be stored?	The data will be stored in a segregated S3 bucket on AWS servers (physically located in Ireland, with disaster recovery/back up servers hosted in Germany). There are essentially four phases to this activity: 1 Transfer of (a copy of) live production data from Marston (via Civica/Centrality) to TCS 2 Data masking applied to personal data fields by TCS 3 Once masking has been validated, TCS' copy of the original production data is deleted 4 Masked data used for testing purposes by TCS The associated security measures are described later in this DPIA and within the TCS Approach document.	Y
Will any data be processed overseas? Which countries?	The TPH Information technology system will be a cloud based solution (hosted by AWS) with the physical servers located in Ireland and Germany (both countries within the EEA). The UK government has stated that transfers of data from the UK to the EEA are currently permitted under UK data protection legislation. The TCS Security Operations Centre for this activity will be deployed from India. Only onshore, UK based staff will be involved in the masking and testing activity itself.	N
Are you planning to publish any of the data? Under what conditions?	Not applicable to this DPIA	N

Step 3: Describe the data		Could there be a privacy risk?
Who does the data relate to?	The data relates to TfL taxi and private hire licensees – past, current and prospective.	Y
How many individuals are affected?	There are a significant number of data subjects; as an illustration, for the year 2020-21, there were 21,000 licensed taxi drivers, 105,000 private hire drivers and in the region of 91,000 licensed vehicles.	Y
Does it involve children or vulnerable groups? If children's personal data is processed, how old are they? Consider the ICO Age Appropriate Design Code	The data does not involve children or other vulnerable groups	N
What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*) Are there any Special Category or sensitive data (list all): Race or ethnicity; Physical or mental health, Political opinions; Religious or philosophical beliefs; Trade Union membership; Using genetic or biometric data to identify someone; Sex life or sexual orientation; Criminal allegations or	The core data fields comprise (including special category data in red text): Name (including previous names) / Contact details (postal address, telephone number, email address, etc) / Date of birth / DVLA or European driving licence details / Photographs / Referees' details / Certificate of good conduct / Employment history / Proof of identity /Country of origin and/or nationality / Proof of right to work in UK / National Insurance Number / Knowledge of London, topographical, driver skills and English language assessments/qualifications / Completed medical forms and any supporting medical information / Vehicle Registration Marks and Vehicle Identification Numbers / Outcomes of DBS checks / Outcomes of Motor Insurers' Bureau (MIB) checks / Details of traffic contraventions, including unpaid Penalty Charge Notices / Details of unpaid PCNs for the Congestion Charge, Low Emission Zone and/or Ultra Low Emission Zone / Details of criminal offences, and/or allegations of criminal offences / Information used to assess fitness to hold a taxi or	Y

convictions	private hire vehicle licence / Complaints made about drivers or operators / Dismissals from working with a private hire operator / The licence and/or badge number issued to a driver/operator or a vehicle by TfL / Bankruptcy status of directors of private hire operators / Details of which operator(s) a private hire driver and/or vehicle has been available to work for / Correspondence (including social media posts) / Licensing decisions from other authorities	
What is the nature of TfL's relationship with the individuals? *(For example, the individual has an oyster card and an online contactless and oyster account.).* Is the data limited to a specific location, group of individuals or geographical area?	TfL's relationship with taxi and private hire licensees is that of Regulator. TfL holds individual records about each prospective, current or past licensee (subject to the local retention / disposal schedule). The data is limited to taxi and private hire licensees as described elsewhere in this DPIA.	N
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	The current supplier (Marston) is unable to provide a copy of 'dummy' data or supply data that has been 'pre-masked' to TCS. The solution includes a data masking solution in order to pseudonymise the data, and which in itself is a data minimisation technique. The copy of the live production data will be deleted once the masking process has been validated by both TCS and TfL. It is anticipated that the copy of the transferred production data will need to be available for a period up to 10 March 2022 to allow for the data to be first validated and then for the masking process itself to be tested/completed/validated.	Y
How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?	After data is loaded in the database from Civica, verification scripts will run which will identify all the records received in files are loaded into database. Once Verification is completed, execution of data masking scripts will be started. TCS has created a table of all the personal data fields that will be migrated and which requires masking. This has been shared with TfL (including the Privacy and Data Protection team). TfL will approve / instruct on all the personal data fields that must be subject to masking.	N

How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process? Do you have a documented disposal process?	The live production data as provided by Civica/Centrality (on behalf of Marston) will be deleted once the data masking process has been validated. The masked data subsequently used for testing purposes will be deleted once the testing activity has been completed and validated / verified. This may include a period after the solution has gone live for continued bug fixing and testing purposes – in the event that any defects are subsequently identified. TCS will delete the data on instruction from TfL – with documentary evidence provided to TfL that the deletion has taken place.	Y

Step 4: Describe the context of the processing		Could there be a privacy risk?
Is there a statutory basis or requirement for this activity?	This data migration and testing activity will help to maintain the effective administration of TfL's taxi and private hire licensing function as it switches to a new supplier in 2023. As such it forms part of TfL statutory function as the Regulator of Taxi and Private Hire services in London under the following: • Greater London Authority Act 1999 • Private Hire Vehicles (London) Act 1998 • Private Hire Vehicles (London PHV Driver's Licences) Regulations 2003 • London Cab Order 1934	N
Is there any use of Artificial Intelligence or automated decision making?	No – but the data masking solution may use an algorithm as part of the data masking process. There will be no automated decision making that will affect data subjects.	N
Will individuals have control over the use of their data? If so, how can they control it?	Data subjects will have limited control over how their data is used for this purpose, but TfL maintains a strong level of transparency, via the TPH privacy notice, about how and why licensing data is processed. All data subjects will be able to exercise all the data subject rights found in Articles 15-21 of the UK GDPR.	N
Would they expect you to use their data in this way?	The data subjects would expect TfL to maintain a licensing record about them. Data subjects would expect this information to be kept securely and this migration and testing activity helps achieve this. The use of live production data for testing purposes would fall outside the specified purposes of	N

	processing described in the taxi and private hire privacy notice. The data masking solution ensures that the personal data is protected and therefore the testing activity would not be considered incompatible.	
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?	Through public facing information on the existing TfL Privacy page for Taxi and Private Hire. The privacy notice is comprehensive – and could be updated to include publication of this DPIA.	N
Are there prior concerns over this type of processing or security flaws?	As described elsewhere, the use of live or production personal data should always be avoided for testing purposes where possible. This is mitigated in this instance through the use of the data masking solution. In terms of the data transfer - Examples of masking logic for personal data fields are below. TfL will have oversight and approval of the logic used within the data masking solution before it is deployed by TCS. • **Masking the First Name, Middle Name and Surname –** Customer Name will be replaced with some random names (from list of 3000 Names). This will be purely on random basis and reverse decoding is not possible. • **Date of Birth –** Value of date and month will be changed to random numbers keeping the year the same as there are business rules which work on customer age • **Mobile Number –** This will be replaced with random numbers • **Email Address –** Email address will be anonymised by replacing first 4-5 characters with xxxxx for all Email Addresses • **Customer address –** This also can be anonymised following the same process as with Customer Names • **Data Masking of Documents –** As per discussion with Civica, Civica will provide metadata of the documents and their linking to application record in extraction files. These extraction files will contain the location of Documents. These documents will be replaced with dummy files of the same type on the location which is present in metadata.	Y

	• It is necessary to retain the TPH licence/application number in its original format as this is required in order to maintain the overall 'structure' of the records and forms part of the validation that none of the other (masked) data fields have been lost during migration.	
Is it novel in any way, or are there examples of other organisations taking similar steps?	Data masking/ scrambling solutions are widely used in order to protect personal data processed for testing purposes.	N
What is the current state of technology in this area? Is this innovative or does it use existing products?	Static masking will be used by TCS. Static data masking - also sometimes called data obfuscation replaces ('masks') sensitive data by altering the data at rest. It is used to provide high quality (realistic) data for development and testing of applications TCS will be using their proprietary 'Mastercraft Data Plus' product as the solution for masking the data. TfL will be required to approve the logic used prior to its deployment (as per the TCS Data Masking Approach document).	Y
What security risks have you identified?	There may be concerns about effectively maintaining the overall security of this activity, including the potential for misuse of any personal data (particularly during the period it is stored in its original unmasked format). The following measures are in place to mitigate these risks. Contractual obligations on the supplier to – 1) Only process personal data in accordance with their role as Processor and under specific instruction from TfL as Controller 2) Implement a monitoring strategy to include monitoring for instances of misuse and attempts of misuse by supplier (and TfL) personnel, malicious software in supplier systems, access to and movement of all TfL Restricted data. 3) Report any actual or suspected data breaches or security incidents to TfL within 24 hours of becoming aware. Technical measures: 4) Data will be encrypted to AES 256 standard 5) Access permissions will be limited to onshore, UK based staff authorised to work on the	Y

masking and testing activity

6) In terms of the data transfer itself – The initial transfer of the production data from Civica to TCS will be handled via a secure VPN. Data will be encrypted using AES 256 / SHA-2

7) Once the data is transferred to the SFTP folder, TCS will not be able to open these encrypted files (Data files encryption to be done by Civica) until the key is shared by TfL (provided by Civica/Centrality) to TCS. TCS will only request the key once the SOC is set up.

8) This data will be stored in a segregated S3 bucket which TCS has verified is not exposed to the public internet. Change control and monitoring by the SOC will ensure this remains the case. Only TCS resources in the UK can access the S3 bucket, using VPN.

9) Access permissions will prevent the copying of data to any local drives.

10) The AWS CloudTrail product will be utilised to enable governance, compliance, operational auditing, and risk auditing for the AWS Environment deployed for TfL

11) AWS CloudWatch will also be used to monitor infrastructure events and performance. It provides a dashboard view of all servers and services hosted by AWS and alerts on any server/service failures or degradation. CloudWatch collects logs, metrics and events to provide a view of all AWS resources applications and services.

12) Personal data will be masked as described elsewhere in this DPIA. This is also included in the Security Management Plan agreed between TfL and TCS. The anonymisation will ensure that re-identification of data subjects is not possible; the techniques used mean that once masked, the data cannot be reinstated to its original form in the non-production environment.

Organisational measures:

13) The supplier will appoint (or already have in place) a Data Protection Officer, and a Security Manager dedicated to the TPH service.

14) All supplier staff –will be subject to pre employment screening and vetting including DBS check. Annual confirmation must be supplied that this is accurate and up to date.

15) All staff will have completed security awareness training to include (amongst other topics) privacy/data handling, incident reporting, data protection legislation and security policies. Such training must be ongoing throughout the term of the contract.

16) The TCS Security Operations Centre will be ‘stood up’ - and shall perform 24x7 security

	monitoring and incident response for the Service System hosted on AWS. TCS will be responsible for providing security incident management, including 24x7 monitoring of logs and events, alerting, detection, response, and final remediation Industry best practice and accreditations 17) The supplier has accreditation to the following standards a. Information Security Management Standard ISO/IEC 27001: :2013 including requirements of ISO 27017:2015 and ISO 27018:2019 for Cloud Security and Privacy standards b. ISO 22301:2019 for Business Continuity Management System Standard	
Are there any current issues of public concern that you should factor in?	None identified.	N
Is the processing subject to any specific legislation, code of conduct or certification scheme?	The migration/masking/testing activity itself is not subject to specific legislation or certification; however, TCS adheres to the industry standards specified above.	N
Will there be any additional training for employees?	The need for any additional training over and above that outlined above will be discussed and agreed between TfL and TCS. In addition, TCS staff will be required to sign a non-disclosure agreement to cover this activity.	N
Does the processing actually achieve your purpose?	Yes. The migration of data is required to effectively test new systems, software and applications that will be used to administer taxi and private hire services from 2023. Both TfL and TCS are aware that the use of ‘live’ personal data should be avoided for testing purposes; the data masking solution applied will help to significantly reduce the associated risks.	N
Is there another way to achieve the same outcome?	The incumbent supplier was requested to provide data for testing purposes in either a ‘dummy’ format or otherwise already masked/scrambled. It has not been possible for the supplier to do this. As such there no alternative but for TCS to	Y

	receive a copy of the live production data and then subsequently apply masking to protect the data during testing.	
Who will own this initiative and ensure there is no function creep without a review of this DPIA?	This migration/masking/testing work is very much a 'ringfenced' activity and in itself, should have little, if any, bearing on the possibility that function creep will occur. More generally, function creep will be prevented through the use of robust change control processes, together with conducting further DPIAs whenever any changes to the testing process are contemplated. TfL is also limited to only undertaking activities which are within its statutory powers which in itself places some limits on function creep.	N

Step 5: Consultation process		Could there be a privacy risk?
Consider how to consult with relevant stakeholders: Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.	TfL does not intend to consult with the taxi and private hire trades on this activity, as there will be no impact or effect on individuals as a result of the testing activity. TfL ensures transparency on the processing of taxi and private hire personal data, with the issue being directly addressed within the privacy notice. This DPIA can also be published.	N
Which business areas have been consulted within TfL?	PPD are project-managing the contract mobilisation activities following contract award. Cyber Security are involved in the security aspects of all of the Lot 1 solution. They have completed an initial review of the supplier masking proposals and have raised no concerns.	N
Have you discussed information security requirements with CSIRT? If so, who is your contact in CSIRT?	As above	N
Do you plan to consult with external stakeholders? If so, who?	There are no plans to consult with external stakeholders	N

Who will undertake the consultation?	N/A	N
What views have been expressed by stakeholders?	N/A	N

Step 6: Identify and assess risks				
Describe source of risk and nature of potential impact on individuals. Include risks of damage or distress as well as associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Is this risk included in project or other risk register?**
The transfer process between Marston (Civica/Centrality) is not secure and leads to loss/unauthorised access to the live production data	Possible	Severe	High	
The scope and volume of production data may be more vulnerable to third party malicious activity during its storage prior to masking	Possible	Severe	High	
Masking solution is not robust and can be reversed	Possible	Significant	Medium	
Not all relevant fields of personal data are masked	Possible	Significant	Medium	

Unauthorised Access / disclosure / alteration / corruption/ deletion / breach of personal data by TCS staff.	Possible	Severe	High	

Step 7: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6

Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated, reduced or accepted)	**Residual risk** (Low, medium or high)	**Measure approved** (Yes/no)	**Who is responsible for implementation?**
The transfer process between Marston (Civica/Centrality) is not secure or compromised which leads to loss/unauthorised access to the live production data	The suggested transfer process has been provided by Civica to TCS and in turn submitted to TfL for approval. Data will be encrypted to an acceptable standard during transit and use SFTP via VPN.	Reduced	Low	Yes	TCS responsible for implementation – TfL is also required to review transfer process and approve
The scope and volume of production data may be more vulnerable (attractive) to third party malicious activity during its storage prior to masking	The transferred/migrated data will be stored in a segregated S3 bucket ringfenced from any other data processed by TCS. TCS has verified that the S3 bucket is configured so that it is not accessible to the public via the internet. Change control and monitoring by TCS will ensure this remains the case throughout the lifetime of the activities. The data will be encrypted; the keys will not be shared	Reduced	Low	Yes	TCS

	until masking is ready to commence. TCS Security operations Centre will be monitoring activity on a 24/7 basis. In addition, AWS monitoring tools will also be utilised. The storage period for this data will be limited to the minimum possible and in any event, not after 10 March 2022.				
Masking solution is not robust and can be reversed	For Static Data Masking on non production, data scrambling or replacement technique will be used. Once data is masked, it cannot be reinstated in the environment. The logic to be deployed will be shared with TfL prior to its use to demonstrate that this is the case.	Reduced	Low	Yes	TCS – with oversight and approval of the masking solution by TfL.
Not all relevant fields of personal data are masked	TfL will have the opportunity to specify which fields of personal data must be masked prior to the testing activity taking place; TCS will perform quality check by taking random sample records and verify manually that all the personal data fields are masked properly. Reports of this activity will be prepared	Reduced	Low	Yes – subject to the level of random sampling (ie by percentage of data) being confirmed by TCS	TfL and TCS

	manually and shared with TfL				
Unauthorised Access / disclosure / alteration / corruption/ deletion / breach of personal data by TCS staff.	TCS has proposed Static Data masking to mitigate the risk of breach of Data. Access to personal data will be managed by Application access and controls. TCS Security operation Centre will monitor for unusual / suspect activity and report promptly	Reduced	Low	Yes	TCS

What is the lawful basis for processing? Are there any Special Category or sensitive data?	**To be completed by Privacy & Data Protection team** The lawful basis for processing in this case is Article 6 (1) (e) of the GDPR – “The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.” The migration and testing activity supports the delivery and operation of TfL’s regulation of taxi and private hire services in London. The categories of data are described elsewhere in this DPIA.	Could there be a privacy risk?
Is this use of personal data compatible with our original purposes for collecting the data?	The use of live production data would not be compatible with the listed purposes for processing. This is mitigated by the masking of personal data fields prior to any testing work taking place. The masking solution cannot be reversed once completed.	N
Are changes to Privacy Notice required?	Whilst the privacy notice is comprehensive, further transparency could be achieved by including a summary description of the testing work (and associated masking).	N

How will data subjects exercise their rights?	Data subjects will continue to be able to exercise their information rights with TfL in accordance with existing processes, which are published on our website on various pages, including; Access your data, Taxi and private Hire and Your Information Rights.	N
How do we safeguard any international transfers? Is any data being processed outside the UK?	The TCS solution will involve an international transfer in respect of the cloud hosting (albeit within the EU/EEA region – Ireland and Germany). Currently UK data protection law treats the EU and EEA Member States as having 'adequate' protection for personal data. The UK is currently the subject of an adequacy decision from the EU in respect of its data protection laws. This took effect in June 2021 and is for a period of four years. TfL will need to implement additional safeguards if the UK does not receive a renewed adequacy decision at the end of this period. This could include the EC Model Clauses (or ICO-approved equivalent clauses), together with a further assessment of the data protection and security measures applied to the data. In respect of the remote access to personal data by TCS support staff in India, the EC Model clauses have been appended to the TfL/TCS contract for services from the outset. (Although this is not anticipated within this activity, with the exception of the Security Operations Centre).	N
Could further data minimisation or pseudonymisation be applied?	Masking techniques are being deployed to help mitigate the risks of unauthorised or unlawful processing.	N
Have appropriate security measures been considered, with Cyber Security involvement where necessary?	Cyber Security is actively involved in this project and are assessing any associated cyber risks	N
Are data sharing arrangements adequate? Do they require further documentation?	No data sharing (other than that involving TCS and their sub-processor, AWS) is intended as part of this activity. Processor activities by TCS are covered by data processing contractual arrangements. The TCS Agreement with AWS includes EC approved clauses as standard.	N
Is the data likely to be and remain adequate, accurate and up to date?	This activity will involve a 'snapshot' of data that will be accurate at the time it is captured and transferred(migrated) for testing purposes. As the testing work involves masked data, it is not necessary to keep it up to date in a pre-production environment.	N

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Principal Privacy Adviser 13 January 2022	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Principal Privacy Adviser 13 January 2022	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Principal Privacy Adviser 13 January 2022	Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	**Privacy Notice to be updated to describe testing activity and security measures in place.** **While the TPH licence number is being retained in its original format, the Principal Privacy Adviser has reviewed all the other data fields to be masked and has agreed that it is robust enough to avoid any inadvertent access/viewing/disclosure.** **TfL must ensure that it exercises all sign off / approval tasks as described in Section 6 of the TCS Approach document** **The process described in this DPIA may be repeated in the event future transfers/testing activity is required. Any changes to this existing process must be subject to a further/revised DPIA.** **TCS to confirm the level of sampling that will take place to ensure the integrity of the masking solution** **If the date (10 March 2022) that the raw data is required to be stored changes (ie a longer time period is needed), prior consultation with the Privacy and Data Protection team must take place, specifying the reasons for any extension.**	
DPO Comments:	In addition to the points above, evidence of completion of the two deletion activities (of the live data and then the masked data) referred to in step 3 must be provided to the Principal Privacy Adviser. I recommend that this DPIA is published, alongside the updated Privacy Notice. I am content that the risks involved in this processing have been sufficiently mitigated.	
PDP Team / DPO advice accepted or overruled by (this should usually	Accepted	If overruled, you must explain your reasons below.

be the Project Sponsor):		
Comments:		
This DPIA will kept under review by:	Joshi Kiran	The DPO may also review ongoing compliance with DPIA.

Glossary of terms

Anonymised data	Anonymised data is information held in a form that does not identify and cannot be attributed to individuals. Anonymous information is not subject to the GDPR, and, where possible and appropriate, should be used in place of identifiable or pseudonymised personal data, particularly where sharing information with third parties or contemplating publication of data. Anonymised data will often take the form of statistics. If you are reporting statistics on a small number of individuals, or there is a level of granularity that allows reporting on small groups of individuals within the overall data set, you must exercise caution to avoid inadvertently allowing the information to be linked to an individual. If information can be linked to an identifiable individual the data is not anonymous and you must treat it as personal data.
Automated Decision Making	Automated Decision Making involves making a decision solely by automated means without any meaningful human involvement. Automated Decision Making is restricted and subject to safeguards under the GDPR. You should consult with the Privacy and Data Protection team before rolling out a process involving Automated Decision Making based on personal data.
Biometric data	Biometric data is a general term used to refer to any computer data that is created during a biometric process. This includes test samples, fingerprints, voice recognition profiles, identifiers based on mouse movements or keystroke dynamics and verification or identification data excluding the individual's name and demographics. Biometric data is subject to additional safeguards under the GDPR when it is processed for the purpose of identifying individuals.
Data breaches	A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored or otherwise processed. Personal data breaches must be reported immediately to DPO@tfl.gov.uk.
Data minimisation	Data minimisation means using the minimum amount of personal data necessary, and asking whether personal data is even required. Data minimisation must be considered at every stage of the information lifecycle: • when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary; • when deciding what information to record, you must consider what information is required, what is relevant and whether any information is excessive; • when deciding whether to share or make use of information, you must consider whether using all information held about an individual is necessary for the purpose.

	Disclosing too much information about an individual may be a personal data breach. When deciding how long to keep information, you must consider what records you will need, and whether some personal data can be deleted or anonymised.
Data Protection Rights	The GDPR provides the following rights for individuals: • The right to be informed; • The right of access; • The right to rectification; • The right to erasure; • The right to restrict processing; • The right to data portability; • The right to object; • Rights in relation to automated decision making and profiling.
Data quality	The GDPR requires that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*." This means you must take steps to ensure that the data you use is sufficiently accurate, up to date and comprehensive for your purposes, and that you take steps to effectively mitigate any detriment to individuals that is likely to result from inadequate data.
Function creep	Function creep describes the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Review and update your DPIA, or undertake a new DPIA to reflect changes in the purpose or the means by which you process personal data.
Genetic data	Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
Marketing	Direct marketing is “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations. Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects

	details to use in future marketing campaigns, the survey is for direct marketing purposes and the privacy regulations apply. Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the privacy regulations apply.
Personal data	Personal data is information, in any format, which relates to an identifiable living individual. Personal data means any information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The definition can also include pseudonymised data (where we hold data that has had the personal identifiers replaced with codenames); depending on how difficult it would be to re-identify the individual.
PIC (Personal Information Custodian)	Personal Information Custodians are senior managers, who are responsible for the Processing of Personal Data within their assigned area of control.
Privacy notice	A privacy notice must let people know who we are, what we intend to do with their personal information, for what purpose and who it will be shared with or disclosed to. TfL adopts a layered approach to privacy notices, with clear links to further information about: • Whether the information will be transferred overseas; • How long we intend to keep their personal information: • The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information; • The name and contact details of the Data Protection Officer;

	• The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner; • The details of the existence of automated decision-making, including profiling (if applicable).
Processing	Doing almost anything with personal data. The GDPR provides the following definition: ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Profiling is the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymised data	Pseudonymisation separates data held about an individual from information that identifies the individual. This can be achieved by encrypting (hashing) the individuals name, MAC address or ID code, masking an individual’s exact location or changing an image to make an individual unrecognisable. TfL can hold the same data in identifiable and anonymous form, provided appropriate controls are in place to prevent re-identification of the pseudonymised data. The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes. Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability. Pseudonymisation is an important security measure and must be considered as part of Privacy by Design and Default approach. If you use pseudonymised data you must ensure that an individual can not be re-identified with reasonable effort. The risk of re-identification is higher when information about the same individual is combined. For example, whilst a post code, a person’s gender or a person’s date of birth would be very unlikely to identify an individual if considered without other reference data, the combination of these three pieces of information would be likely to enable a motivated individual to re-identify a specific individual in most circumstances.

	If you use a "key" to encrypt or hide their identity you must ensure it is sufficiently protected to prevent the individual being re-identified. A Data Protection Impact Assessment can help you assess whether pseudonymisation is reversible in a given scenario.
Significant effects	A DPIA will be required for processing relating to an individual, or group of individuals that has an effect on their legal status or legal rights, or will otherwise affect them in a significant way. These effects may relate to a persons: • financial circumstances; • health; • safety; • reputation; • employment opportunities; • behaviour; or • choices
Special Category data	Special category data consists of information about identifiable individuals': • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data (for the purpose of uniquely identifying an individual); • data concerning health; or • data concerning a person's sex life or sexual orientation. Information about criminal convictions and offences are given similar protections to special category data under the Law Enforcement Directive.
Statutory basis for processing	TfL is a statutory body created by the Greater London Authority (GLA) Act 1999. This Act gives the Mayor of London a general duty to develop and apply policies to promote and encourage safe, integrated, efficient and economic transport facilities and services to, from and within London. The Act also states that we have a duty to help the Mayor complete his duties and implement the Mayor's Transport Strategy. In particular, we are required to provide or secure the provision of public passenger transport services, to, from or within Greater London. As a highway and traffic authority for GLA roads, we regulate how the public uses highways and we are responsible for: • Traffic signs • Traffic control systems • Road safety

	• Traffic reduction We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs). The GLA Act contains specific powers to provide information to the public to help them to decide how to make use of public passenger transport services and to provide or secure the provision of public passenger transport, as well as a broadly scoped power to do such things and enter into such transactions as are calculated to facilitate, or are conducive or incidental to, the discharge of any of its functions. Further miscellaneous powers are set out in Schedule 11of the Act. Activities may have a statutory basis related to other legislation, for instance the requirements to publish information under the Local Government Transparency Code.
Systematic processing or monitoring	Systematic processing should be interpreted as meaning one or more of the following: • Occurring according to a system • Pre-arranged, organised or methodical • Taking place as part of a general plan for data collection • Carried out as part of a strategy Examples of activities that may constitute a regular and systematic monitoring of data subjects include: • operating a telecommunications network; • providing telecommunications services; • email retargeting; • data-driven marketing activities; • profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); • location tracking, for example, by mobile apps; • loyalty programs; behavioural advertising; • monitoring of wellness, • fitness and health data via wearable devices; • closed circuit television; • connected devices e.g. smart meters, smart cars, home automation, etc.
Vulnerable people	A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or others from harm or exploitation. All children are considered vulnerable by virtue of their age and immaturity.