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 and job title:	████████ (Open Innovation Manager) ████████ (Customer Experience Manager, Open Innovation) ████████ (Graduate, Open Innovation)	Date DPIA completed	25 September 2023
		Proposed launch date	Filming is expected to commence in 2023. Images are expected to go live in 2024.
Name and description of the project:	**Google Street View & Indoor Live View for Stations** Google are keen to develop a Street View solution for key TfL stations. This will give disabled customers and anyone who is unfamiliar with the TfL stations, e.g. tourists, the tools to pre-plan their journey. In addition, Google will use the Street View images to enhance the Google Maps product with augmented reality features (i.e. Indoor Live View) to help customers travel more easily around our stations. Indoor Live View has already been rolled out in selected cities and will shortly be live in other		

EVERY JOURNEY MATTERS

	cities. More information can be found here: https://blog.google/products/maps/redefining-what-map-can-be-new-information-and-ai/ **PLEASE NOTE: The primary purpose of this document is to assess any privacy risks relating to this project. However, it has been used as an opportunity to also record some non-privacy related risks and their assessment.**				
Personal Information Custodian (PIC) or band 5 lead	███████ (Chief Customer Officer)	Is PIC aware of this DPIA?	Y	Project Sponsor	███████ (Chief Customer Officer)

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.		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.	Y	Process personal data which could result in a risk of physical harm or psychological distress in the event of a data breach.		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.	Y	Process personal data on a large scale or as part of a major project.	Y	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.	Y	Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	Y
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.	Google Street View for Stations aims to provide the same Street View feature that Google Maps has offered for many years but for TfL stations. The Project team have liaised closely with IDAG (Independent Disability Advisory Group) who have approved the project and been clear that it will offer huge benefits for disabled users who like to pre-plan their journeys so they are less anxious about potential hurdles they may need to overcome on their route. There are more than one billion monthly active users of Google Maps services. TfL Go's number of active monthly users is around 715 thousand (July 2023). Google will carry out the work to enable Street View for stations in London at no material cost to TfL. The data collected by Google is topographical data related to the station layout and images of the customer facing areas of the stations. Each station will be filmed only once, but this may take place over several days, as filming is dependent on clear weather – Google's cameras must be calibrated outside the station at ground level and can't operate in poor visibility or rainy/humid conditions. It is anticipated that stations will be re-captured at appropriate intervals, and any privacy (or other) controls will need to be in place as outlined in this DPIA for any future filming. A trial was carried out in 2017 at Green Park station, but privacy implications were minimised during this by Google filming at night, without passengers present. Network Security have asked that we film at a time when the station is open as they would like to use this as an opportunity to demonstrate that our stations are secure. This means that customers and staff will be present in the images, and it is for this reason that we need to complete a DPIA.

	Whilst the filming will take place in publicly accessible parts of the TfL network, this data collection is not taking place in the public realm, given that stations are private property. We need to protect the interests of our customers, employees and other stakeholders throughout. The stations filmed will be in central London to begin with but progress to a wider network outside of that area including stations in outer London. All privacy considerations will remain the same.
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	1. Supports our Mayor's Transport Strategy objectives - (i) Accessibility **Policy 14:** *"The Mayor, through TfL and the boroughs, and working with stakeholders, will seek to enhance London's streets and public transport network to enable disabled and older people to more easily travel spontaneously and independently, making the transport system navigable and accessible to all and reducing the additional journey time that disabled and older users can experience"* **Proposal 53:** *"The Mayor, through TfL and working with transport operators, will enable spontaneous and independent travel for disabled and older people by:* *a) Improving journey planning tools, ensuring advances in technology make the tools more accessible and easier to use; and guiding people to the most accessible journey options.* (ii) Better information for customers **Policy 13:** *"The Mayor, through TfL and the boroughs, and working with stakeholders, will seek to make the public transport network easier and more pleasant to use, enabling customers to enjoy comfortable, confident, safe and secure, informed and stress-free travel."* 2. Allowing customers to use their channel of choice and reach a large number of users. - There are more than one billion monthly active users of Google Maps services. 3. Value for money.

	- The work will be completed at no material cost to TfL. 4. Enhances our own digital products. - Street View is already available in some of our digital customer products, e.g. TfL website, Journey Planner, and users of our own products will benefit from this new feature. It can also be used by our station staff to help provide additional guidance to our customers.
Will the processing directly affect the individuals concerned?	The processing affects the individuals concerned as they will be travelling (or working) on our network and images of them will be captured by a third party during this time. However, the effect of the processing is minimised as Google's blurring technology is designed to automatically blur identifiable faces before publishing. The blurring of images to protect the privacy of individuals is the responsibility of Google, as they are Controller for this processing. However, all images will also be checked by TfL staff before being made available in Google services for network security purposes (i.e. TfL will be able to add additional blurring where there are security concerns). Google will provide a platform which stores the images and provide TfL with training on how to blur additional images. Many station staff wear name badges, which could be visible in images – managers will be asked to tell staff they can remove name badges on the day of filming. This will be reiterated in staff briefing materials.

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).	
What is the source of the data?	Images will be collected by Google's contractor at selected TfL stations. Google and its contractors will adhere to the terms agreed in the contract between TfL and Google. Google will use special Street View cameras mounted on rucksacks to collect cartography and imagery data of TfL station interiors, and street level images of station entrances and exits. These images may include individuals that are present in the area during the imagery collection.
Will you be sharing data with anyone?	Google will collect and process the imagery, as Controller. Processed data (i.e. after blurring has been completed) will be shared as Street View imagery with Google Maps users. All potential personal information captured in images will be held by Google on their network. TfL will have temporary access to these images prior to release, but after the initial blurring of faces has taken place. TfL will not hold a copy of the images on

	our network. Further blurring will be carried out by TfL for network security purposes, such as redaction of certain infrastructure to ensure appropriate security measures have been undertaken.
Are you working with external partners or suppliers?	Yes, Google's contractor and Google. We also plan to work with Network Rail, but exact parameters are to be confirmed.
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	An agreement will be in place between TfL and Google before any filming takes place. TfL Legal, the Information Governance department and external legal counsel have been involved in the review and drafting of this agreement.
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?	Google are the Controller for any personal data processed as part of this activity and they are therefore not acting as TfL's Processor in terms of the UK GDPR definition of Processor. TfL have still ensured that there are adequate privacy contractual controls in place. Google have provided an explanation in relation to the security of the images at the point of data collection and when processed afterwards. They have also provided additional detail of what data is generated during filming of the imagery. ██████████████████████████████████████ The collected data includes imagery and cartography data. Audio is not collected. ███████████████

	████████████████████████████ ████████████████████████████ ██ ████████████ ████████████████ ████████████████
Will the data be combined with, or analysed alongside, other datasets? If so, which ones?	Alongside the images, Google will also collect cartography data from our stations. Before filming, we have provided them with station maps which include exits, entrances, toilets, etc. These will be used to enable Google to plan their routes through the stations, and identify and highlight points of interest such as lifts, etc.
Will AI or algorithms be used to make decisions? What will the effect of these decisions be?	Google's blurring technology is designed to automatically blur identifiable faces before publishing.
How and where will the data be stored?	██ ██ ██ ██ ████████████████████ Google will host the data on their network.
Will any data be processed overseas? Which countries?	Yes. Data will be processed in the EEA/Switzerland, in addition to the UK, and stored in data centres in the EEA/Switzerland and in the U.S. Once at the data centres, Google apply automatic blurring technology to all Google-owned Street View images after collection and prior to publishing.

	Google's Privacy & Terms website further describes their approach to EU data transfer obligations: • *https://policies.google.com/privacy?hl=en&gl=de#enforcement* • *https://policies.google.com/privacy/frameworks?hl=en-US* • *See also: https://safety.google/*
Are you planning to publish any of the data? Under what conditions?	Images will be published as part of Google Street View services.

Step 3: Describe the data	
Who does the data relate to?	The individuals who may be captured in the images include: • TfL customers and other members of the public • TfL station staff • TfL staff/contractors working in our stations at the time of filming e.g. cleaning operatives, engineers, etc • London Underground/Overground/Elizabeth line train drivers • British Transport Police (BTP) • Retailers and their staff who work from premises on the TfL network • Other dedicated space users e.g. buskers
How many individuals are affected?	On average, there are approximately the following number of passengers who use the relevant services each day of the week: Tube travel – 3.8 million, Network Rail/London Overground – 3.5 million, DLR – 200,000. 230,000 passengers use the Elizabeth line on an average mid-weekday.

	We plan to film at less busy times of the day - during off-peak hours (between 10am and 4pm). Network Security are keen to capture images that represent a usual day on the network.
	The figures quoted are pre-pandemic (2019) averages except for the Elizabeth line figures which are averaged from May to Oct 2022. Current ridership (Jan 23) sits around 80% of the pre-pandemic levels but fluctuates from week to week.
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	Potentially, if children or vulnerable groups are present in the station at the time of filming, but there is no specific intention to capture images of children or vulnerable groups.
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 convictions.	The collected data includes imagery and cartography data. Audio is not collected. The images will be time and date stamped to month and year. Collection timestamps are linked to the imagery. Once externally published to Google Maps, the Street View imagery only displays the month and the year the imagery was collected, without further details. There is no specific intention to collect any special category data, and Google does not plan to infer any special categories from the raw imagery.

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?	Images will be filmed within areas of TfL stations accessible to customers. As described above there are a variety of individuals to whom the data could relate should they be present at the point of filming, and the nature of our relationship with them is dependent on who they are. TfL customers could hold registered products with us, or be registered to use TfL services (e.g. Oyster card, Contactless payment card, Road User Charging, etc). However, there would be no way of linking an image back to an individual 'known' to TfL through any registered service use. TfL staff (including station staff and train drivers) hold a contractual relationship with London Underground or TfL through their employment contracts. Any contractors, whilst not holding a direct contractual relationship with TfL, are employed by a third party to be present at the station for employment purposes. BTP officers will also be there in an employment capacity. The BTP police Britain's railways, providing a service to rail operators such as TfL. Any retailers will have a commercial relationship with TfL. Advertisements will also potentially be captured within images – we hold a commercial relationship with advertisers. Yes, data will be limited to specific locations, i.e. to specific stations (exact order of stations still to be confirmed, but the rollout will begin with one phase of defined stations before moving onto a second phase).
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	Data minimisation has been considered and is a standard part of Google Street View already. The intention is for the data to be blurred before any public use to protect the privacy of individuals. Google's blurring technology is designed to automatically blur identifiable faces before publishing. Whilst Google will be responsible for carrying out the process of blurring the images to protect the privacy of individuals, TfL will be checking the images to identify any additional blurring required for network security purposes. TfL may use Google's online tools to request take-down or blurring of images after initial launch. A further method of data minimisation will be considered when setting a filming schedule - we will select stations that are not usually present in common journeys to be filmed on the same day to reduce the likelihood of an individual's complete/partial journey being identified from them being filmed more than once on the network. We will not film at the stations on the most popular routes on the same day. We will identify station pairs with a daily average of over 3000 passengers travelling between them or averaging over 1000 passengers travelling between them during the inter-peak hours (10:00 – 16:00) (using NUMBAT common origin/destination pairs). Any station pairs above these thresholds will not be filmed on the same day. We will use a pre-covid dataset so that customer journey numbers are above what we are seeing today. This means

	that there is no data for Elizabeth Line stations, as a result, we will not film any other station on the same day as an Elizabeth Line station.
	███
	More information on the Google Street View imagery policy can be found here: https://www.google.com/streetview/policy/ Anyone can report a problem with any of the images and request additional blurring directly from within Street View when viewing an image.
How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?	Where there are significant changes to the layout of a station, Google will try to accommodate a Street View imagery update. Timeline will depend on operational capacities. It is also possible to take down images of a station where the layout has changed significantly until a new set of images can be uploaded. Smaller changes such as updates to businesses can be requested at any time through the Google Business Profiles.
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?	Google will comply with its privacy policy (https://policies.google.com/privacy) in terms of its use of the data. As Controller, Google bears the responsibility for ensuring any use of their collected personal data is lawful. ██ TfL will not be responsible for retaining imagery and therefore does not need a documented disposal process. ██ There is also a Google-managed *Report A Problem* flow available for users to request additional blurring (e.g. full-body in published imagery). These blurs are also added to back-end copies of that imagery.

Step 4: Describe the context of the processing

Is there a statutory basis or requirement for this activity?	Yes, 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 (see earlier detail in step 1 as to how this supports objectives in the Mayor's Transport Strategy).
Is there any use of Artificial Intelligence or automated decision making?	Google's blurring technology is designed to automatically blur identifiable faces before publishing. In addition to the use of AI in Google's blurring technology, Google apply other technologies to improve the Google Maps product as described here https://ai.googleblog.com/2017/05/updating-google-maps-with-deep-learning.html
Will individuals have control over the use of their data? If so, how can they control it?	Yes – In the unlikely event that a face has not been blurred out, individuals can contact Google to request manual blurring, through the Google Report a Problem feature. For specific face blurring this link can support the answering of those changes. For example, they can ask for their entire body to be blurred out if desired. ██
Would they expect you to use their data in this way?	In many circumstances, yes – Street View is a well-established feature in Google Maps and some Network Rail stations have had detailed external Street View imagery since 2012. However, our customers might still not all expect it to feature within TfL stations, but a communication plan has been prepared (more detail below) to inform them of the planned work.
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?	We are developing a comprehensive communications campaign, (an excerpt can be seen below) to ensure that staff are aware of the filming, what the images will be used for and how to ask for further blurring. During filming customers will also be informed via posters and other communication methods, and where they ask via station staff, the Trekker operator, and our Contact Centre, of filming taking place, what the images will

be used for, and that faces will be blurred before publication. Station signage (posters) will also direct customers to the Street View website where they can access further information.

Part of our comprehensive communication plan will include a press release in advance of filming, internal comms to staff at affected stations, comms to relevant unions, web content, social media posts and in-station announcements and posters (including at interchanges).

The Open Innovation Team will ensure that provisions are in place for signage to be displayed to customers i.e. there are a sufficient number of posters and display boards at a station.

A TfL representative will also visit each station on the first day of filming and will be on hand to assist with introductions, ensure station staff are aware of what is required/expected and ensure in-station notices are clearly displayed before filming can start. The Google operative will also be provided with contact details for the TfL representative who will be on hand if there are any issues during filming (including if posters have been removed).

Google's contractors will also have a leaflet to give out to customers or staff who ask them on the spot questions.

Google's Policy for Street View

OI = TfL Open Innovation, CC = TfL Contact Centre

TfL Informing phase					
Date	What	Audience	Channel	Content created by	Delivered by
1 month before filming	TfL Teams Call: general area manager call (bi-weekly)	TfL Managers	Meetings	TfL OI Project team	TfL OI Project Team
1 month before filming	FAQ: prep for TfL station colleagues and rail industry partners	All affected station staff (TfL) CC teams (TfL) TOCs	Email / Document TfL Intranet Print	TfL OI Project team	TfL OI Project / Comms team
1 month before filming	TfL Briefing pack: time; prep for TfL station staff	All affected TfL station staff & CC teams	Emailing / Document / TfL Intranet site	TfL OI Project team	TfL OI Project / Comms team

		(Shared with TOCs)			
TFL Filming phase					
Date	**What**	**Audience**	**Channel**	**Content created by**	**Delivered by**
1 week before filming	**Posters** at appropriate TfL locations e.g. all interchanges/all entrances	All TfL passengers traveling through affected stations	Print	TfL OI Project team	TfL Station staff
1 week before filming	**Announcement** of planned date for TfL filming (script)	All TfL passengers traveling through affected stations	Loudspeaker	TfL OI Project team	TfL Station staff
1 week before filming	**Project Update**: info about filming, a link to more information on the TfL Google website. Will also reference/evidence TfL privacy due diligence	TfL Passengers	External TfL Innovation Website and Privacy & Cookies webpages	TfL OI Project team	TfL OI Project team
During filming days	**Posters** at appropriate TfL locations e.g. all interchanges/all entrances	All TfL passengers traveling through affected stations	Print	TfL OI Project team	TfL Station staff TfL OI Project Team will visit each station on the first day of filming and are contactable should there be any issues

						regarding signage
	During TfL filming days	**Announcement** of filming taking place (script)	All TfL passengers traveling through affected stations	Loudspeaker	TfL OI Project team	TfL Station staff or Control Centre staff (DLR)
	During TfL filming days	**Announcement** of filming taking place	All TfL social media follows	Twitter TikTok (TfL)	TfL OI Project team	Relevant TfL Social Media Teams
	During TfL filming days	**Passenger leaflet**	TfL Passengers who want to find out more	Print (in-person)	Google	Google Trekker operator

Are there prior concerns over this type of processing or security flaws?	There is a concern that some facial images may not be blurred. However, we are reassured from our discussions with Google as to the effectiveness of Street View blurring and its wide acceptance internationally. In addition, TfL staff will be reviewing all images to add further blurring for network security purposes. They will also inform Google if they spot any identifiable faces which have not been blurred.
Is it novel in any way, or are there examples of other organisations taking similar steps?	Street View is a long-standing feature in Google Maps. Street View for stations launched last year in Sydney and some international Airports. Network Rail images, captured in 2012 were processed as 2-d walk around maps but quickly became redundant and were not re-filmed with the increased features that the product can now hold.
What is the current state of technology in this area? Is this innovative or does it use existing products?	It uses existing products. The augmented reality (Indoor Live View) is innovative but already present in Google Maps for above ground journeys.
What security risks have you identified?	The security risks identified relate primarily to network security and not the security of personal data. A security risk is the capturing of security features in stations which could aid in the planning of a criminal act, for example. These will be blurred out with the support of Network Security.

	Network Security are following DfT Light Rail Security Programme (LRSP) advice to use Street View to promote the security of our stations, this is not a public document and therefore a link cannot be shared. ███████████████████████████████ ███████████████████████ ███████████████████████████████
Are there any current issues of public concern that you should factor in?	Our approach to this activity has kept areas of public concern as a focus. For example, concerns that an individual's personal data is being misused or is not transparently used, or that individuals are being tracked/monitored. There is currently a heightened profile for the role of data ethics in the implementation of personal data processing solutions, and in addressing issues of public concern we have kept ethical considerations to the fore.
Is the processing subject to any specific legislation, code of conduct or certification scheme?	As it will include images of the general public (and TfL staff and others working on the network), it will be subject to data protection legislation – including the UK GDPR and Data Protection Act 2018.
Will there be any additional training for employees?	Yes – Google will show relevant TfL staff how to blur out selected parts of images for network security purposes.
Does the processing actually achieve your purpose?	Yes – we do not need to show customers at all for the feature to be useful (as per the trial at Green Park). However, Network Security and DfT prefer to show the stations in use.
Is there another way to achieve the same outcome?	We continue to be open to other potential providers of similar products. Currently there does not appear to be a similar product, offering Indoor Live View navigation for free, and as well established as Google Street view.

Who will own this initiative and ensure there is no function creep without a review of this DPIA?	The Open Innovation Partnership Team owns the delivery of this project. Open Innovation will document relevant process flows and lessons learnt from this initial implementation phase. Once live, any future filming, updates or required security blurring, will be the responsibility of Customer Experience to manage.

Step 5: Consultation process	
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.	It has not been deemed necessary to directly consult with individuals whose data will be collected in regard to any decision to proceed with this activity, however we are developing a comprehensive communications plan with the Press Office and Operational colleagues from across the business, with involvement from the Privacy and Data Protection team also. This will include a press release in advance of filming, internal comms to staff at affected stations, comms to relevant unions, a web page to link to, social media posts and in station notices (including at interchanges). Google have advised that their contractors have a standard letter which they give out to anyone who asks them about the work they are doing.
Which business areas have been consulted within TfL?	Digital, Commercial Development, Customer Experience, Network Security, Legal, Open Innovation, Information Governance, IDAG, Contact Centre and Customer Services, Operations, Comms, including Press Office.
Have you discussed information security requirements with Cyber Security? If so, who is your contact in Cyber Security?	No, we believe that this isn't relevant as the ownership and hosting of the images is Google's responsibility.

Do you plan to consult with external stakeholders? If so, who?	Not consult but communicate to customers and trade unions. We have already consulted with IDAG to confirm that this project will be beneficial to disabled customers. We are also planning to work with Network Rail as Google plan to film both Network Rail and London Underground/TfL stations together where relevant.
	We have also consulted with our third-party operators KeolisAmey (DLR), Arriva Rail (LO), MTR (Elizabeth Line) and Heathrow Airport Holdings.
	Network Security will also inform BTP of planned filming so they know which stations are being filmed on which day.
	We will also communicate with City Hall on our plans and progress.
Who will undertake the consultation?	The Open Innovation Project Team is constructing a communication strategy plan with relevant stakeholders, e.g. London Underground / TfL operational staff, Google, and the TfL Press Office.
What views have been expressed by stakeholders?	**Network Security:** Supportive of the initiative. **Commercial Development:** Supportive. ████████████████████████████ **Digital:** Supportive. **Customer Experience:** Sponsoring the initiative and fully supportive of the value of this work for our disabled customers. ████████████████████████████

Step 6: Identify and assess risks (Privacy 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 = Less than 10%** **Possible = 10-50%** **Probable = Over 50%** (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?**
Person not being blurred out prior to live release	Possible	Significant	Medium	Y (but responsibility for blurring personal data is with Google)
Customer in images at two stations on the same day so their possible route could be identified	Remote	Minimal	Low	Y
Filming of non-customer areas of station	Remote	Significant	Low	Y
Agreement between Google and TfL does not restrict use of images to Street View / Live View, instead it refers to use of images in connection with Google products or services. The related risk is the potential	Possible	Significant	Medium	Y

for Google to use images captured for Street View in other Google products, not assessed in this DPIA – impacting customer privacy				

Step 6: Identify and assess risks (Non-privacy 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 = Less than 10% Possible = 10-50% Probable = Over 50% (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?
███████████████	██████	█████	██████	█
Security related assets not blurred out	Possible	Severe	High	Y
National security threat identified, and TfL advised by authorities to remove images	Possible	Severe	High	Y

████████████████	██████	█████	████	█

Step 7: Identify measures to reduce risk (Privacy risks)					
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8					
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?**
Person not being blurredout prior to live release	As controller Google uses its blurring technology, which is designed to automatically blur identifiable faces before publication, which technology is already widely used on other Street View images. After publication individuals can report concerns with the blurring directly to Google.	Reduced	Medium	Yes	Google

Customer in images at two stations on the same day so their possible route could be identified	We will not film at the stations on the most popular routes on the same day. We will identify station pairs with a daily average of over 3000 passengers travelling between them or averaging over 1000 passengers travelling between them during the inter-peak hours (10:00 – 16:00) (using NUMBAT common origin/destination pairs). Any station pairs above these thresholds will not be filmed on the same day.	Reduced	Low	Yes	Open Innovation & Google
Filming of non-customer areas of station	TfL will be able to remove entire panoramas from the images collected if Google contractors inadvertently film in staff only areas.	Reduced	Low	Yes	Open Innovation & Google
Agreement between Google and TfL does not restrict use of images to Street View / Live View, instead it refers to use of images in connection with Google products or services. The related risk is the potential for Google to use images	███████████ █ As Controller, Google bears the responsibility for ensuring any use of their collected personal data is lawful.	Accepted	Low	Yes	Customer Experience & Google

captured for Street View in other Google products, not assessed in this DPIA – impacting customer privacy					
Step 7: Identify measures to reduce risk (Non-privacy risks)					
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8					
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?**
■■■■■■	■■■■■■	■■■■	■■	■■	■■■■■
Security related assets not blurred out	TfL will be able to blur out security assets as required. TfL will be able to request additional blurring from Google post launch.	Reduced	Medium	Yes	Open Innovation, Network Security & Google

National security threat identified, and TfL advised by authorities to remove images	TfL can require Google to remove sensitive images.	Reduced	Medium	Yes	Network Security & Google
████████████ ████████ ██	██████████████ ██████████████ ████████████ ████████████ ████████	████████	████	████	██████████████ ████

To be completed by Privacy & Data Protection team	
What is the lawful basis for processing? Are there any Special Category or sensitive data?	The lawful basis for the collection of this data is not for TfL to decide as we are not the controller of the data Google are collecting. However, TfL will access the imagery collected for the purposes of reviewing for network security reasons. Whilst personal data (i.e. identifiable faces) should have been blurred by this stage, if any does remain, we will be accessing in accordance with Article 6(1)(e) of the GDPR – "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". 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. There is no specific intention to collect any special category data, and Google does not plan to infer any special categories from the raw imagery.
Is this use of personal data compatible with our original purposes for collecting the data?	Google are the controller of the data collected, but we understand the proposed use to be compatible, including our use to review for network security reasons.

Are changes to Privacy Notice required?	We will work with the business to ensure on-site signage is displayed during filming and we will review any content added to the Open Innovation section of the TfL website. We will also add content to our Privacy & Cookies suite of webpages. We should use these opportunities to link out to Google privacy content also.
How will data subjects exercise their rights?	Data subjects should exercise their rights directly with Google as controllers for this data.
How do we safeguard any international transfers? Is any data being processed outside the UK?	Data is being processed outside of the UK, but the responsibility for data protection compliance of any international transfers is with Google in their role as controller.
Could further data minimisation or pseudonymisation be applied?	We understand this has been fully considered.
Have appropriate security measures been considered, with Cyber Security involvement where necessary?	Given the role of TfL in this, limited involvement is needed from Cyber Security. However, we will ask the project to liaise with Cyber Security to ensure TfL's access to the Google platform is secure.
Are data sharing arrangements adequate? Do they require further documentation?	N/A
Is the data likely to be and remain adequate, accurate and up to date?	We understand that Google have processes in place to assist with this requirement – i.e. updating station images after layout changes, reporting functionality for individuals to request additional blurring, or remove images if changes are significant until new filming can be undertaken, etc.

The process which customers should follow to report an issue with images is illustrated below. |

1. When viewing a particular Street View image, you can report a problem with it using the "Report a problem" button in the bottom right corner:

2. A "Report a problem" form will open. You will need to fill in the requested details, and submit the form:

Report Inappropriate Street View

Street View: **5 Pancras Sq**

Image preview: *Adjust the view of the image so that it is focused on the part of the image you are reporting*

This box can be moved around to focus on the element to be removed

Why are you reporting this image? (Please choose from one set of options.)

Request blurring: What would you like us to blur?
- ⦿ A face
  Please include additional information that will help us identify the face that should be blurred.
  (Required)

  Characters Remaining: 1500

- ◯ My home
- ◯ My car / a license plate
- ◯ A different object

You can provide more information about your specific request

Report image quality: What is wrong with this image?
- ◯ Misplaced image or misaligned navigation arrows
- ◯ Overall poor image quality
- ◯ A place on the street has a wrong or misplaced icon

Email address:
(Required)

reCAPTCHA verification
(Required)

☐ I'm not a robot

Step 8: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by Privacy Team:	Head of Privacy and Data Protection, Privacy Advisor (25/09/2023)	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Head of Privacy and Data Protection, Privacy Advisor (25/09/2023)	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Head of Privacy and Data Protection, Privacy Advisor (25/09/2023)	Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	This DPIA is to be published on the TfL website, alongside some brief content describing the project.	
DPO Comments:	This DPIA is unusual in that it relates to processing of personal data by a controller other than TfL but it is valuable for documenting the impact on our customers and staff and ensuring that relevant risks and mitigations have been identified.	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):	Yes	If overruled, you must explain your reasons below.
Comments:		
This DPIA will kept under review by:	Customer Experience Open Innovation	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 Top of Form 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.
Pseudonymise d 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.