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:		Date draft DPIA completed	April-May 2022
Job titles:	On street Infrastructure Co-ordination Manager; RUC Operations and Contract Manager	Proposed launch date	Summer 2023 (TBC)
Name and description of the project:	The processing of personal data associated with the proposed expansion of the Ultra Low Emission Zone (ULEZ) in 2023. The ULEZ was originally introduced on 8 April 2019 and covered the same geographical area as the Congestion Charge ("CC") in central London. It was then extended on 25 Oct 2021 to inner London cover a larger area bounded by the North and South Circular Roads. The ULEZ operates 24 hours a day, every day of the year except Christmas Day. It is proposed that the current ULEZ boundary be extended to cover most of Greater London and follow the same boundary as the existing Low Emission Zone (LEZ). A DPIA was produced in September 2020 to cover the testing, implementation and ongoing running of the inner London ULEZ at that time. This DPIA takes account of –		

	• the additions to the Automatic Number Plate Recognition (ANPR) camera infrastructure that would be required to allow enforcement of the new, further extended boundary area (in the region of 2750 cameras); • back office/systems and infrastructure testing/development activities; • the additional volumes of personal data that would be processed; • awareness campaign activities; and • the potential for camera sharing. NOTE: this is a DRAFT DPIA which will be reviewed and updated if necessary following public and stakeholder feedback from the statutory consultation on the London-wide ULEZ extension proposals due to take place in May 2022.				
Personal Information Custodian (PIC) or band 5 lead	General Manager, Road User Charging	Is PIC aware of this DPIA?	Y	Project Sponsor	Lead Sponsor, Investment Delivery Planning

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

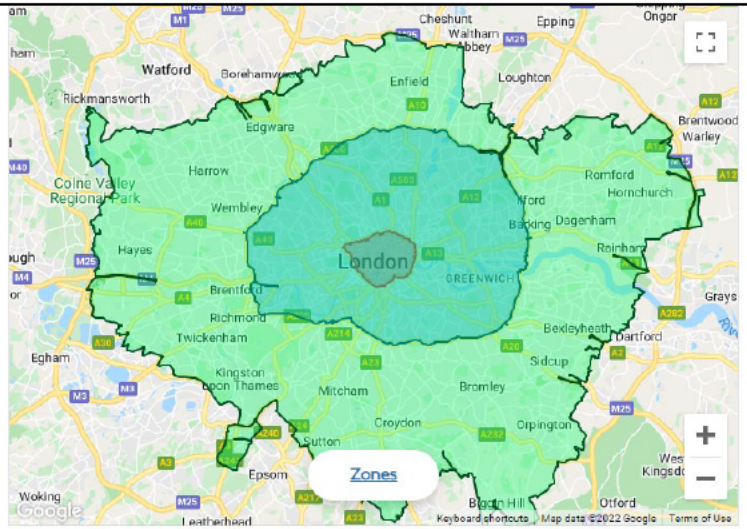
Use profiling or automated decision-making to make decisions that will have a significant effect on people. Significant effects can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits.	**X**	Process special category data (relating 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.	**X**
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.		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.	**X**	Process personal data in a way which involves tracking individuals' online or offline location or behaviour.	**X**	Match, compare or combine datasets, or have the potential to deny anonymity or re-identify people.	**X**
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.	**X**	Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	
Process biometric or genetic data in a new way.		Undertake systematic monitoring of individuals.	**X**	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.	**Project Aims** This project proposes an expansion of the geographical area covered by the ULEZ, from the current inner London boundary at the North/South Circular to the existing London Low Emission Zone (LEZ) boundary close to the Greater London boundary ("the expanded ULEZ zone"). The overall aim of the project is primarily to deliver even greater improvements to air quality within Greater London and the associated public health benefits this will provide, as well as secondary consequential carbon and traffic congestion reduction benefits. It will also help London to achieve net zero carbon emissions by 2030 and cut congestion. The current LEZ would also continue to apply within the same London-wide geographical area (for those larger/heavier vehicles that are affected by that scheme). An expanded ULEZ Scheme would be operated and enforced by the existing Road User Charging Systems, currently used to operate and enforce the current Congestion Charge, LEZ and (inner-London) ULEZ. The geographical locations for the current inner London ULEZ can be seen here: https://tfl.gov.uk/ruc-cdn/static/cms/documents/ulez-boundary-map-main.pdf and the extent of the expanded zone to cover the LEZ area can be seen here: https://tfl.gov.uk/ruc-cdn/static/cms/documents/low-emission-zone-map.pdf While TfL follows the principles of data minimisation and privacy by design across its work, a DPIA is required to establish whether there are any privacy issues connected specifically with the processing of personal data associated with the installation of new ANPR camera infrastructure for the purpose of the proposed expansion of the scheme, particularly in terms of the following: 1. The installation (and testing) of new ANPR camera infrastructure, in locations not currently covered by cameras, and the use of existing ANPR infrastructure not currently used for charging or enforcement purposes; 2. Back office/systems and infrastructure testing/development activities that requires the use of an extract of real Vehicle Registration Mark (VRM) data and contextual images;

	3. The potential for the collection of increased volumes of personal data during the operation and enforcement of the expanded ULEZ as a result of any increase in ANPR camera numbers and locations where they are installed or of extended use of the existing ANPR infrastructure; 4. The potential for further camera data sharing with the Metropolitan Police Service (MPS) from the additional ANPR cameras, with whom an agreement already exists in relation to ANPR cameras used for existing TfL Road User Charging Schemes (Congestion Charge, LEZ and inner London ULEZ); 5. Monitoring journeys made by vehicles in the expanded zone, for traffic analysis and transport planning purposes; and 6. Monitoring journeys made by vehicles that are non-compliant with ULEZ standards in order to contact their registered keepers in advance of the expansion go-live date, in order to raise awareness of the proposed scheme expansion and what to do to comply with the emissions standards.
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	**Benefits to TfL customers/employees/members of the public** The main objective of an expanded ULEZ is to improve air quality and reduce emissions in outer London. Therefore, the scheme aims to encourage frequent users of the zone who primarily travel using a non-compliant vehicle to switch to a sustainable mode or change to a compliant vehicle. For those who travel less frequently in, to and around the zone, it may not be cost effective to change their vehicle specifically to comply with the ULEZ standards. These users are more likely to 'stay and pay' the £12.50 charge for the small number of trips they make in the zone. Those who visit more frequently are more likely to change their vehicle. In both cases there will be a number of users unwilling to pay the ULEZ charge or change to a different vehicle and therefore will either choose to change route, change mode, change destination or not travel at all. As an indicator of this, such improvements were measured within the first month of the expansion of the ULEZ to the boundary of the North and South Circular roads in October 2021. **Commercial benefits** As with the existing road user charging (RUC) schemes, including the inner London ULEZ, LEZ and Congestion Charge, surplus revenue will be reinvested in public transport to support the delivery of the Mayor's Transport Strategy. **Operational benefits** Installation of additional cameras will allow TfL to effectively administer, operate and enforce an expanded ULEZ

	in line with an (amended) Scheme Order in order to realise the anticipated benefits of the scheme.
Will the processing directly affect the individuals concerned?	Yes. The broader intended effect on individuals is for them to reduce the emissions from their vehicles by encouraging use of vehicles that meet the required emissions standards or changing their behaviour and moving to more sustainable forms of transport such as walking, cycling and public transport. All those living and working in London will benefit from improved air quality as a result of reduced vehicle emissions. Those individuals whose vehicle is subject to the ULEZ charge or who are issued with a Penalty Charge Notice (PCN) will be directly affected by the processing. A greater proportion of vehicles driving into, out of or across London are likely to pass by a TfL ANPR camera and have their VRM recorded than currently, due to the expanded camera network. The period that that data will be stored will vary according to whether the vehicle is exempt, has paid the charge or is liable for a PCN.

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?	**Vehicle data sourced via on-street ANPR cameras** The proposed expansion of the ULEZ would work in exactly the same way as the existing road user charging schemes in London – which are described on the road user charging privacy notice. The current camera network can be broken down into three different 'rings' - There will be approximately 237 enforcement ANPR cameras (once an existing camera refresh programme is complete) principally used to enforce the congestion charge zone that can also capture vehicles liable for the LEZ and ULEZ ('central ring'). There are approximately 1156 cameras principally used to enforce ULEZ but can also be used for LEZ enforcement (these are outside the congestion charge zone but within the boundaries of the north and south circular roads - the 'middle ring'). Outside the current inner London ULEZ zone there will be (once an existing camera refresh programme is complete) approximately 106 cameras enforcing the LEZ only. The ANPR cameras operate 24 hours a day, all year, as their use for traffic monitoring purposes continues during times or days a scheme is not enforced (for example the Congestion Charge does not operate between Christmas and New Year and the ULEZ does not operate on Christmas Day). The expansion of the ULEZ will take it up to the same boundary of the LEZ zone, as shown on the map below.	Yes



It is anticipated that approximately 2,750 additional ANPR cameras may be needed to effectively administer, operate and enforce an enlarged ULEZ. Approximately 750 of these additional cameras would be placed at the new boundary sites with the remainder capturing intra-zone movements. All of these additional ANPR cameras will be in locations within the Greater London Boundary.

The camera locations will be determined in order to maximise the effectiveness and efficiency of the Scheme, chiefly by locating the cameras where they will cover the busiest roads and junctions, on the boundaries of the expanded Zone and within it.

The majority of these new cameras will use mobile communications which will mean that they can be quickly relocated, if necessary, as a result of road layout changes and/or intelligence that highlights undetected entry, exit or busy routes where a high volume of non-compliance is believed to be occurring. Where cameras are moved as described above, they will still be within the areas covered by signage ('in-zone repeater signs') that inform individuals they are within the ULEZ and LEZ and that cameras are in use. These are DfT-approved road signs (at the time of writing DfT approval is to be confirmed).

The number of up to 2750 additional ANPR cameras has been reached based on the geographical size of the expanded ULEZ zone and the objective of achieving as high a capture rate as possible to effectively influence customer behaviour and achieve the improvements in air quality desired whilst ensuring all drivers are treated equally by the enforcement process.

	The numbers of additional ANPR cameras (and their proposed locations) are considered proportionate because the geographical size of the area is increasing from 380 km^2 to 1572km^2 and TfL will be required to effectively administer, operate and enforce an (expanded) ULEZ scheme and treat everyone equally. An analysis of the camera density over the new geographical area of any expanded ULEZ will be included in a subsequent draft of this DPIA, in the light of final decisions on camera numbers and locations. Alongside the installation of new cameras, there will also be an assessment as to whether any existing cameras can be removed, in particular from the 'middle ring' shown on the map above. It may be possible to remove cameras in existing locations that are no longer needed because a vehicle can be captured on a road in the expanded zone. **Performance and Capacity testing (phase 1)** Testing activities will begin from an early stage of the project to ensure that back office systems currently used for road user charging can process additional volumes of data to the required standard and reliability. This will be achieved by using an extract of the evidential records captured by existing RUC cameras in April 2021, which was originally used for testing the first expansion of the ULEZ schemes. This data has been specifically retained for testing purposes and avoids the need for further extracts of live VRM data and contextual images to be captured and stored. (This data will continue to be retained for the purposes of testing any future system upgrades and will be used only in the pre-production environment delivered by Capita under the current contract.) This data is securely stored in Capita's pre-production environment, which is hosted in a Microsoft Azure Cloud solution physically located in a Microsoft Ireland datacentre, with a backup in the Netherlands. The data includes VRM and vehicle image, as well as the date/timestamp 'metadata' recorded by the cameras. Capita is TfL's primary service provider for the operation of all its road user charging schemes. There is a full contract in place with Capita which includes data processing clauses. The data will be transferred via dedicated secure FTP transfer. Once processed, the images will be flowed into the pre-production environment to which testers will have access. The data will be used to test the overall stability of the camera infrastructure as well as how it performs at different transaction volumes. Non-Functional Testing will include backup and restore, disaster recovery, patching and release process, monitoring and alerting. The testing will be	

	complete before the proposed scheme go live date. This time period will allow for the volume testing and other non-functional testing to be completed and ties in with the date that the new camera in-stations are intended to go live. The risk of testing data being inadvertently used to affect a data subject or to make decision about them (eg being sent a PCN in error) has been mitigated as the data used in testing will only be used in a pre-production environment which is not connected to the live system which obtains data from the DVLA for enforcement purposes. Due to this, there is no risk that the testing data will be processed in the live environment. In addition, the pre-production environment is not connected to any other live systems that require camera data such as those which are used to generate daily charges and Penalty Charge Notices. The VRM will therefore remain unlinked from any other personal data reducing any risk of impact on a data subject. **Performance and Capacity testing #2** The new ANPR cameras will begin to be installed from 2022 and this will be completed by mid 2023. It is intended that, once installed, the new cameras will initially be used for testing and business planning purposes (ie used to inform compliance rates, resourcing requirements, system capacity requirements and financial budgeting/forecasting). **Pre-go-live traffic monitoring** For a short period ahead of the go live, the new cameras will also be used for traffic monitoring and transport planning purposes using TfL's existing London Vehicle Analysis Tool (LVAT2), Real Time Origin and Destination (RODAT) and London Congestion Analysis Program (LCAP) systems. These use pseudonymised ANPR data and match it against pseudonymised DVLA vehicle types. In simple terms, we replace the VRM with an alternative random set of letters and numbers, as a way of distinguishing vehicles in a dataset by using a unique identifier that does not reveal its 'real world' identity. In addition, there is no possibility of making a link to DVLA Registered Keeper address details in this monitoring activity. Data is used to produce reports on vehicle type/fuel type, which helps to calculate the number and type of vehicles that do not meet the required emissions standards, journey time monitoring, which helps to manage the Transport for London Road Network (TLRN) and provides real time indication of emerging issues on the TLRN. This vehicle data specifically concerns the specification of the vehicle itself and excludes details of the registered keeper.	

	As the new camera infrastructure is to be used in this way before the proposed official launch of the expanded ULEZ, then appropriate transparency will also need to be in place in order help ensure the processing of the traffic monitoring data is fair and transparent. On street signage will not be in use across the *whole* area of the expanded scheme until the month prior to go live. However, the existing charging schemes, including LEZ, already have camera warning signs in place and these will continue to provide warning of camera capture throughout the lead up to the new scheme, and will be supplemented by additional transparency measures such as revisions to the Road User Charging privacy notice published online. This would replicate the processing that took place during the first expansion of the (inner London) ULEZ, during 2021. **Compliance and Awareness campaign** As with the previous phases of ULEZ, during the run-up to the go live date for expansion, it is proposed that from early 2023 TfL will contact the registered keepers of vehicles that are non-compliant with the ULEZ scheme, and which have been seen driving within what will be the expanded ULEZ. Registered keepers will be informed of the pending implementation of an expanded ULEZ Scheme and will be encouraged to visit TfL's website to find out further information. TfL has a responsibility to raise awareness of new (or changes to existing) road user charging schemes. The sources of the data used for this activity will be the VRMs of vehicles seen driving (via existing ANPR cameras) within Greater London from January 2023. TfL will then de-duplicate the VRM captures and identify which are non-compliant with the ULEZ Scheme using the existing TfL database used for the existing Ultra Low Emission Zone. Those VRMs that are non-compliant will then be checked against TfL's existing Road User Charging customers and if they are an existing customer with an approved communication channel (eg CC Autopay Customers who get monthly statements) then they will be contacted directly by TfL. A record of the remaining non-compliant VRMs will then be provided to the DVLA who will send an agreed letter to the registered keeper, where they have details in their database. The registered keeper details for these vehicles will not be shared by DVLA with TfL. The first iteration of the ULEZ awareness campaign (for the central zone in 2019) identified two issues of concern - • that the DVLA letters did not include details of the VRM that was 'seen' by the cameras, meaning owners of multiple vehicles (in particular) did not know which one was being referred to; and	

	• the lack of manual validation of the VRMs seen (as no images were captured) resulted in claims from individuals, who had received letters, stating they had never driven in London. This is essentially the result of a misread of a VRM which matches a VRM that is non-compliant and registered with the DVLA. The subsequent ULEZ Compliance and Awareness Campaign avoided these issues by: • including the VRM on the DVLA letter to inform the registered keeper which vehicle was observed and is non-compliant; and • validating the VRMs observed by TfL, which are matched against TfL's list of non-compliant vehicles, by removing VRMs observed less than twice on any day by an ANPR Camera, which will reduce the risk of registered keepers receiving letters for non-compliant vehicles that had not been driven within London. The measures will be implemented again for this campaign. The Road User Charge privacy notice currently includes information on how personal data has been used for previous iterations of ULEZ awareness campaigns. This will be updated as needed to ensure it remains accurate and is fully transparent going forward. The overarching concept of working with the DVLA to support TfL's awareness activities was the subject of a DPIA in 2018.	
Will you be sharing data with anyone?	**ULEZ expansion awareness campaign** As explained above, for any non-compliant vehicles that cannot be associated with an existing RUC account, those VRMs will be shared with the DVLA for the purpose of sending awareness correspondence on TfL's behalf. **Camera Sharing with Metropolitan Police Service (MPS)** TfL anticipates that personal data collected by some, or all, of any additional cameras would also be shared with the MPS, subject to meeting the appropriate data protection and information sharing principles. TfL will hold discussions with the MPS before agreeing to share any new information or give access to infrastructure. An updated Mayoral Delegation to TfL to enable it to share ANPR camera data with the MPS has been prepared in response to the inner London ULEZ expansion in 2021 and the proposed expansion to outer London. If approved by the Mayor it will provide for extended camera sharing in the future - subject to the MPS demonstrating their own obligations around conducting (or updating)	Yes

	DPIAs and other strategic assessments on necessity and proportionality. Should the MPS be given access to any additional cameras, they will act as a separate Controller for the processing they are responsible for. TfL is not responsible for any MPS' processing of ANPR data, including for criminal law enforcement purposes (ie their processing under Part 3 of the DPA 2018). Any information (or infrastructure) sharing will comply with data protection legislation.	
Are you working with external partners or suppliers?	TfL uses a third party supplier to administer the day-to-day operation of all of its Road User Charging Schemes, and this will include the expanded ULEZ. This supplier is currently Capita. Siemens, who are responsible for the installation and maintenance of the cameras, transfers the ANPR data and images to Capita. They also filter out ANPR data and images of VRMs loaded on to a compliance list from further processing. Capita has overall responsibility for the camera testing activity. If any particular issues are identified as a result of the testing, then it may be necessary to involve Capita subcontractors, specifically, Hitachi, Kapsch, Amdocs and Taranto to resolve these – and they then may have access to the testing data as a consequence of this. These sub-contractors undertake particular functions related to providing the cloud storage environment (Hitachi), interpreting the ANPR read (Kapsch) and Amdocs/Taranto whose systems use camera data for charging and enforcement purposes (ie produce daily charge data, and PCNs).	No
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	There is a full contract in place with both Capita and Siemens which includes data processing clauses. Capita has contracts in place with all of the sub-contractors named above and these contracts contain appropriate data processing clauses as required by Capita's own Agreement with TfL. Any new cameras installed to monitor/enforce the expanded ULEZ will utilise encrypted mobile 4G communications provided by O2, under contract with appropriate data protection clauses	No
What measures do you take to ensure suppliers processing personal data on our behalf provide adequate assurances about their ability to process this	All Road User Charging 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 carried out by in-house and third party auditors. The results of these audits are	No

data safely and lawfully?	required to be shared with TfL. In addition, regular monthly meetings are held between TfL and its RUC suppliers to specifically discuss cyber security and other data protection aspects. TfL's cyber security team and data governance experts are regularly involved in clarification discussions to confirm assurances are adequate. Following the Covid-19 pandemic there has been a permanent shift to flexible (home based) working by some Capita staff, meaning that they may be processing personal data on TfL's behalf at sites away from an office environment.	
Will the data be combined with, or analysed alongside, other datasets? If so, which ones?	As described above, VRM data will be shared with the DVLA - who will then match it against their own database of registered keepers - for the purpose of sending awareness letters. (The DVLA will not be provided with any date, time or location information associated with the VRMs capture on the ANPR network.) More generally, in respect of the overall operation of TfL's road user schemes, in order to issue a PCN to the Registered Keeper (where an applicable daily charge has not been paid) TfL obtains the name and address from the DVLA Database of Registered Keepers. TfL has a contract in place with DVLA that grants secure access for this purpose. TfL is required to abide by the DVLA Code of Connection and TfL's access and use of the data is subject to regular audit by the DVLA. TfL receives data on VRMs that are known to be compliant with ULEZ emissions standards. (This can be based on vehicle age, fuel type, make and model.) This is used to filter out known compliant vehicles from further processing (and is also used for TfL's online vehicle checker). This data is derived from a number of different sources, including the DVLA, Society of Motor Manufacturers and Traders (SMMT) and individual vehicle manufacturers. It does not currently include data on all UK registered compliant vehicles.	No
Will AI or algorithms be used to make decisions? What will the effect of these decisions be?	No	No
How and where will the data be stored?	The RUC Information technology system is a cloud based solution (hosted in a Microsoft Azure environment in Ireland and the Netherlands) The data captured by the ANPR cameras at the roadside is transferred by Siemens to Capita using encrypted mobile 4G or 5G communications The retention period for any personal data stored is subject to a local disposal schedule; data is	No

	stored for the minimum period possible for the purpose.	
Will any data be processed overseas? Which countries?	The RUC Information technology system (operated by Capita) is a cloud based Azure solution (hosted in Ireland and the Netherlands). Currently UK data protection law treats the EU and EEA Member States as having 'adequate' protection for personal data.	No
Are you planning to publish any of the data? Under what conditions?	No personal data will be published. Aggregated non-personal data derived from traffic monitoring activities, such as numbers of non-compliant vehicles, may be published to demonstrate the scheme effectiveness and meet statutory transparency requirements.	No

Step 3: Describe the data		Could there be a privacy risk?
Who does the data relate to?	The data captured will relate to: • vehicles travelling on roads within Greater London, • individuals who have an online account to pay a daily charge or to manage a discount • where PCNs are issued, the Registered Keepers of those vehicles	No
How many individuals are affected?	On an average day, the number of unique vehicles currently captured via the ANPR cameras within the existing ULEZ is in the region of 900k. Although the proposed ULEZ expansion would cover a bigger geographical area, current analysis suggests that the volume of unique vehicles that will be captured will remain the same due to expected increase in compliance and the filtering of compliant vehicles which means that they are not further processed (other than in a pseudonymised form for traffic monitoring). A list of known compliant VRMs is loaded within the camera in-station where it is used to discard any ANPR data and images of VRMs that are compliant. The filtering process minimises the volume of ANPR data and images that is required to be sent to Capita and aims to only process VRMs that are required for road user charging purposes (ie for payment of a daily charge or issue of a PCN).	Yes
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	None of the road user charging schemes, including the ULEZ is intended to capture data relating to children or vulnerable adults. Any enforcement of the schemes is directed to the registered keeper of the vehicle in each case. The cameras now used for Road User Charging have a wider range of view than those used previously (pre-2021) meaning that there is a slightly increased risk that images of individual people (eg pedestrians) could be captured unintentionally, together with the boundaries of private properties or other buildings that could be considered as 'sensitive', such as places of worship, health facilities, schools. This will be mitigated as far as possible by ensuring that the focus of the cameras is	No

	directed towards traffic (and further – to the number plate / bonnet area of vehicles rather than the windscreen.) It is also important to note that ANPR cameras do not capture rolling video footage, and any imagery is in the form of still photographic images to enable the make, model and colour of a vehicle to be confirmed. TfL would have no means of identifying any pedestrian inadvertently captured in a still photographic image.	
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 ANPR cameras capture an alpha-numeric reading of a vehicle's Vehicle Registration Mark (VRM) together with the date, time, unique camera reference and still photographic images. The cameras are not intended to capture images of vehicle occupants or pedestrians. Where enforcement of the ULEZ is necessary (ie when the required charge has not been paid), a Penalty Charge Notice (PCN) is sent to the registered keeper of the vehicle. The name and address of the registered keeper is obtained from the DVLA under a specific contractual agreement. The PCN includes a photographic image of the vehicle alongside the date, time and location the image was captured as well as the make, model and colour of the vehicle. There are no Special Category or sensitive personal data being processed. In addition, enforcement of road user charging schemes by TfL is a civil matter, not a criminal offence.	No

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 is the charging authority for the ULEZ (including when expanded to outer London), LEZ and CC schemes. TfL's relationship will be one of enforcing the payment of ULEZ charges by vehicles that do not meet ULEZ emissions standards detected driving in the expanded ULEZ. There will be a mix of those unregistered customers who pay a charge on an ad hoc basis, customers who have an online account to pay a regular charge and/or apply for a discount and those customers who have been issued with a PCN for non-payment of a daily charge. Data will relate to vehicle Keepers/Owners/Operators (or their nominated representatives). Their registered address may be anywhere within the UK, or overseas (though likely to be limited to countries within the European Economic Area (EEA)) The ULEZ itself will be geographically limited to Greater London within the current LEZ boundary.	No
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	TfL takes a number of steps to minimise the amount of personal data that is processed for the operation and management of all road user charging schemes, including the ULEZ. It is possible to pay the daily charge by providing only a payment card number and the VRM of the vehicle in question; it is not mandated to have an account or to provide a name and address. The ANPR data and images of those vehicles who are not required to pay the ULEZ charge (because they are already known to be compliant) or that have paid the charge within the required timeframe are deleted within 21 days. The filtering process within the camera in-stations also supports the principle of data minimisation as, aside from the filtering process itself, (and the pseudonymisation process for traffic monitoring purposes), it avoids the further processing of data relating to those vehicles that are known to be compliant with the ULEZ standards. ANPR data is pseudonymised before being processed for the purposes of traffic monitoring and transport planning to reduce the risk of 'real world identification. While it is possible to pay a daily charge with minimal personal data, it is not possible to enforce the Road User Charging schemes using anonymised or pseudonymised data, because Regulations dictate that the PCN needs to be issued to the Registered Keeper (the person liable to pay the PCN). The camera and systems performance testing activity required for the proposed expansion, needs to use 'real-life' VRMs and image captures because the technology cannot be adequately tested using dummy data. However, in this respect, a single dataset, originally extracted in 2021 is maintained for this purpose, which removes the need to repeatedly extract fresh data for testing.	No

How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?	The camera infrastructure includes a process of ground-truthing for cameras. This involves all cameras being manually checked for accurate reads by an operator before they are commissioned for live enforcement. In addition, there is requirement for ongoing sample ground truthing of existing cameras throughout their life cycle to ensure accuracy remains. The cameras are tested to ensure that they work accurately in varying weather and light conditions. The Capita process ensures every PCN is manually checked to ensure the camera read obtained matches the image on the PCN and that the vehicle type and colour match the records obtained from the DVLA. If there is no match, the data, including any keeper details obtained from DVLA, is deleted.	No
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?	Customer data will be retained in line with the existing Data Retention Policy for Road User Charging. ANPR data and images of those vehicles who are not required to pay the ULEZ charge or have paid the charge within the required timeframe other than via Autopay, will be deleted within 21 days. (ANPR data and images of vehicles known to be compliant with ULEZ standards are filtered out within the camera instations even sooner.) A summary of the core retention periods for RUC data is published within the RUC privacy notice. Registered Keeper data will be retained in line with the existing Data Retention periods relating to the Autopay Service and RUC enforcement. The retention period for the Autopay Service is 3 months after the monthly statement and the retention period for enforcement data is triggered by the date at which the PCN and any associated fees are paid or written off. The retention periods for all data processed across all road user charging schemes is defined by TfL in accordance with legitimate business needs and other legal or regulatory requirements (such as those relating to financial transactions or legal claims for example). In relation to the camera testing activity, some ANPR and image data will be retained within TfL systems for longer than its usual retention period – specifically that data that would normally be deleted after 21 days. This is explained to customers within the RUC privacy notice... Where that data is stored in systems on TfL's behalf by a service provider (currently Capita), they are instructed to delete data in accordance with TfL's instructions (and contractual requirements).	No

Step 4: Describe the context of the processing		Could there be a privacy risk?
Is there a statutory basis or requirement for this activity?	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 TfL has a duty implement the Mayor's Transport Strategy (MTS). 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, TfL regulates how the public uses highways and we are responsible for road safety and emissions from vehicles. Section 295 and Schedule 23 of the Act empowers TfL to make road user charging schemes concerning the payment of charges by vehicles driven or kept on public roads. If the Mayor approves the London-wide expansion of ULEZ the MTS will be revised to include policies and proposals for the expansion. TfL is the charging authority for the purposes of the Greater London Low Emission Zone Charging Order 2006, as amended, which includes the London Emission Zones Charging Scheme under which the LEZ and ULEZ are established. The expansion of the ULEZ to outer London will be implemented by a variation order that extends the area of that Zone to the boundary of the LEZ, which will only take effect if confirmed by the Mayor (with or without modifications). TfL will process data from the ANPR cameras used for the operation and enforcement of the CC, LEZ and ULEZ (including as expanded) schemes in aits capacity as the statutory charging authority for those schemes. In addition, the Mayor of London has a legal responsibility to prepare an Air Quality Strategy in order to improve air quality in London and achieve statutory air quality standards and objectives in London as soon and as effectively as possible. The implementation of the expanded ULEZ will continue to contribute to this objective.	No
Is there any use of Artificial Intelligence or automated decision making?	No	No

Will individuals have control over the use of their data? If so, how can they control it?	Individuals will have limited control over the capture by a camera of their vehicle as any vehicle that passes by a camera will be subject to an 'ANPR read' and will have a photographic image taken of it. Individuals who have a RUC account will have control over the use of data for marketing purposes, via an 'opt in'. No other Road User Charging customer will receive marketing from TfL. Individuals will be able to exercise their Information Rights under Articles 15-21 of the GDPR, and TfL will consider these requests on a case by cases basis, as per existing processes. All of these rights are publicised on the TfL website at Access Your Data and Your Information Rights In respect of any MPS processing for policing purposes, issues of transparency and data subject control and rights will be their own responsibility as a separate Controller This is unconnected to TfL's own processing.	Yes
Would they expect you to use their data in this way?	Yes; road user charging schemes and the use of ANPR cameras to enforce them, have been in operation in London since 2003. Camera sharing with the MPS began in 2007 (for national security purposes only), and was expanded in 2015, to include wider law enforcement purposes. TfL has always been transparent about this activity and included it within the fair processing information that TfL publishes online.	No
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?	Information is publicised on the TfL website at Access Your Data and Your Information Rights PCNs will also include a privacy notice (as they currently do for road user charging and other traffic enforcement). All TfL Road User Charging schemes are supported by on-street signage, the original design of which was approved by the ICO. Specific ULEZ signage has been designed and is already in place within the Central and Inner London ULEZ. This will be further rolled out across the expanded area. Examples of signage can be seen on the ULEZ Road Signs web page. Further consideration will be given to transparency of the exact camera locations, although this must be carefully considered against the risk of undermining the scheme and creating 'rat runs' as people actively seek to avoid being detected. The MPS will be responsible for any fair processing information provided to individuals about their own use of ANPR cameras for policing purposes.	No

Are there prior concerns over this type of processing or security flaws?	Please see the entries for security risks and issues of public concern below	No
Is it novel in any way, or are there examples of other organisations taking similar steps?	The approach being taken is consistent with existing Road User Charging and Vehicle Enforcement schemes operated by TfL which include the current Congestion Charge, LEZ Scheme and the ULEZ.	No
What is the current state of technology in this area? Is this innovative or does it use existing products?	Advanced - using digital, high definition cameras with Automatic Number Plate Recognition (ANPR) software.	No
What security risks have you identified?	Any security risks are anticipated to be low; the expanded zone will be enforced using the same technology and back office systems that are currently used for the operation and enforcement of TfL's road user charging schemes. All cameras have in-built security controls that detect any unauthorised access and automatically disable the camera and destroy any data held. Data collected by the cameras will be transmitted via an encrypted 4G or 5G network.	No
Are there any current issues of public concern that you should factor in?	It is possible that the introduction of further ANPR cameras within Greater London – particularly in areas not currently subject to TfL's CCTV or ANPR coverage - may contribute to concerns about excessive surveillance – by either TfL or the MPS (or both).	Yes
Is the processing subject to any specific legislation, code of conduct or certification scheme?	All of the road user charging schemes (including the ULEZ) are subject to UK legislation. Whilst not subject to VCA (Vehicle Certification Agency) and Home Office standards in relation to Vehicle Capture systems, the existing systems are built to these same standards Transport for London voluntarily complies with the Surveillance Camera Code of Practice issued by the Home Office (which applies to local authorities and police forces in England and Wales). Capita (TfL's current suppliers for operating the 'back office' of our road user charging schemes) is ISO27001 accredited and PCI DSS compliant.	No
Will there be any additional	The proposed expansion of the scheme will increase the overall scale and volume of processing and	Possibly.

training for employees?	more people will be required to help operate the scheme. These will all be provided training as per the Capita contract requirements and refresher training provided to existing staff as appropriate to ensure a full understanding of the new scheme characteristics and reinforce data protection principles. In addition there may be greater volumes of information rights requests – including subject access and right to erasure requests. All such requests will need to be handled correctly and within the relevant statutory timescales.	
Does the processing actually achieve your purpose?	Yes – please see the explanation below as to alternative processing methods cannot be considered in this particular case.	No
Is there another way to achieve the same outcome?	No - not to the extent that the proposed scheme is hoping to achieve. Alternatives have been considered but none offer the same potential for changing behaviour and reducing vehicle emissions. Drivers could, in theory, simply be 'asked' not to drive non-compliant vehicles into the (expanded) ULEZ. However, this would be highly unlikely to achieve the necessary air quality improvements required as there would be neither any incentive for complying nor consequence for driving a non-compliant vehicle. In addition, the use of cameras is the only known way to provide evidence of a vehicle's presence in a road user charging zone without the need for on board technology (eg GPS location data). Even with on board technology, a photograph would still be required for any PCN to be legitimately issued and for subsequent enforcement. In respect of the dataset used for the camera testing activity, the cameras need to be tested using real VRMs and vehicle images. The stability and performance of the systems cannot be effectively tested using dummy data because it will not have real life conditions that can impact on the camera ability to read the number plates correctly In respect of the awareness campaign; TfL has a statutory duty to undertake this. While more 'generic' methods will also be used (radio, social media, print media etc) directly contacting the keepers of vehicles actually seen driving in London prior to go live (and so have an increased likelihood of being affected) also forms an essential part of that campaign.	No
Who will own this initiative and ensure there is no function creep without a review of this DPIA?	RUC's PIC will own the DPIA aspects of the camera systems and function creep will be monitored through the use of robust change control processes, together with conducting further DPIAs whenever a change to the original purpose of the scheme is contemplated. TfL is also limited to only undertaking activities which are within its statutory powers which in itself places some limits on function creep.	No

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.	A full public and stakeholder consultation on the proposals to expand the ULEZ to outer London will take place in May 2022, including on a variation order to amend the 2006 Scheme Order for that purpose. The consultation materials will include specific content on privacy (including this document) and the responses will be used to inform any potential privacy enhancing measures that could be taken. This draft DPIA will be further updated once the outcomes to the consultation are known. TfL will liaise as required with the Information Commissioner's Office and the Surveillance Camera Commissioner. TfL will need to consider whether it is appropriate/necessary to consult further with other stakeholders on the specific issue of privacy intrusion. TfL will also work with the MPS specifically on the issue of sharing the additional cameras, including TfL's view on whether the MPS should conduct a DPIA of its own and whether it should conduct a further round of public consultation before access to the cameras is enabled.	Yes
Which business areas have been consulted within TfL?	All relevant departments/team within TfL are involved with the project to expand the ULEZ, including City Planning, Projects and Planning Directorate (PPD) Cyber Security, TfL Legal, the Consultations team and the Privacy and Data Protection team.	No
Have you discussed information security requirements with Cyber Security? If so, who is your contact?	Cyber Security will be fully involved in the development of the expanded scheme. The key contact is currently a Senior Cyber Security Analyst.	No
Do you plan to consult with external stakeholders? If so, who?	Yes. The public and stakeholder consultation on the London-wide ULEZ expansion proposals is a fully comprehensive and active consultation process seeking views from individuals, stakeholders and other organisations to inform the report to the Mayor and his final decision making about whether to	Possibly

	confirm the consultation proposals (with or without modifications). As above, this will include specific content on privacy and the responses will be used to inform any potential privacy enhancing measures that could be taken. This draft DPIA will be further updated once the outcomes to the consultation are known.	
Who will undertake the consultation?	The TfL Consultation team will undertake this work. The consultation will be widely publicised and available online via TfL's 'Have Your Say' portal.	No
What views have been expressed by stakeholders?	This draft DPIA will be further updated once the outcomes to the consultation are known.	Possibly

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 = Less than 10%,** **Possible = 10-50%;** **Probable = Over 50%)**	**Severity of harm** **(Minimal, significant or severe)**	**Overall risk** **(Low, medium or high)**	**Is this risk included in project or other risk register?**
Proportionate processing and data minimisation: **Excessive data collection resulting from additional ANPR camera infrastructure**	Possible	Significant	Medium	Yes
Proportionate processing (corporate risk): **Public/political/legal challenge that camera numbers are disproportionate**	Possible	Significant	Medium	Yes
Proportionate processing (corporate risk): **Public concerns about police access (specifically) to a greater number of surveillance cameras; leading to legal challenge**	Possible	Significant	Medium	Yes

Proportionate processing: **Possibility that the ULEZ scheme is subsequently scrapped or suspended meaning cameras continue to capture data even though TfL's original purpose no longer applies**	Remote	Severe	Medium	Yes
Data accuracy: **The accuracy of the cameras is not sufficiently robust, meaning that the VRM is incorrectly read and PCNs are incorrectly issued to the wrong recipients**	Possible	Significant (distress)	Medium	Yes
Fair processing: **New cameras are installed and are used for monitoring purposes before the scheme go-live and without appropriate transparency.**	Possible	Significant (corporate compliance risk relating to transparency and fair processing)	Medium	Yes
Data retention: **Long term retention of live VRM data and images for ongoing testing purposes results is excessive, lacks transparency and/or could result in function creep. Compatibility concerns with the principle of data minimisation.**	Possible	Moderate	Medium	Yes
Data security: **Shift to greater home working by service provider and or TfL staff may create additional level of risk with regard to handling personal data away from a more 'controlled'**	Possible	Moderate	Medium	Yes

or 'supervised' office environment (general risk across all RUC processing - not specific to this ULEZ expansion)				

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 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?**
Proportionate processing and data minimisation: **Excessive data collection resulting from additional ANPR camera infrastructure**	Ensure appropriate retention periods are implemented so that data is deleted once it is no longer required (those vehicles which are not liable for a PCN - eg exempt, have paid the charge). Carefully site cameras in locations which maximise opportunity to achieve scheme benefits and avoid intrusion into the boundaries of private property or other buildings. The focus of the camera must always be directed at the road. Extent of compliance with the scheme and need to improve London's air quality to be regularly reviewed to determine continuing need for, and size of, camera network. Only retain non-pseudonymised data of non-compliant vehicles (estimated	Reduced	Low	Yes	RUC Operations / PPD implementation team

	to be 25% of all vehicles). ie- Based on the ANPR read the vehicle is checked for its compliance with the ULEZ Scheme. If it is known to be ULEZ compliant, the VRM will not be retained for any longer than necessary to verify this. If it is not ULEZ compliant or its compliance status is unknown, then it will be sent for further verification and possible enforcement.				
Proportionate processing (corporate risk): **Public/political/legal challenge that camera numbers are disproportionate**	Conducting (and publishing) a DPIA; Analysis of camera numbers required) to demonstrate that the camera numbers are needed to enforce the scheme (and deliver air quality benefits); Regular review of camera numbers to ensure minimum possible used for purpose Transparency about rationale for camera deployment and use and benefits realisation	Reduced	Low	Yes	RUC Operations / PPD implementation team
Proportionate processing (corporate risk: **Public concerns about police access (specifically) to greater number of surveillance cameras; leading to legal challenge**	To be addressed by a MPS DPIA and/or other strategic assessment which will establish whether access is necessary and proportionate.	Reduced	Low	Yes	Information Governance / RUC Ops (in liaison with MPS)

Proportionate processing: **Possibility that the ULEZ scheme is subsequently scrapped or suspended meaning cameras continue to capture data even though TfL's original purpose no longer applies**	TfL will pseudonymise the data from the expanded ULEZ cameras completely; re-purpose them (eg for monitoring of traffic volumes and congestion), with appropriate transparency and after a DPIA has been completed; or hand over sole control to the MPS so that they can continue using the cameras for law enforcement/policing purposes	Reduced	Low	Yes	RUC Ops
Data accuracy: **The accuracy of the cameras is not sufficiently robust, meaning that the VRM is incorrectly read and PCNs are incorrectly issued to the wrong recipients**	Levels of manual validation are 100% to ensure VRM matches against correct make, model and colour of vehicle before any PCN is issued. The new camera infrastructure will also be subject to volume testing prior to go live to ensure the accuracy rates are as expected and the cameras can cope with the volumes of data flowing through them	Reduced	Low	Yes	RUC Ops
Fair processing: **New cameras are installed and are used for monitoring purposes before the scheme go-live and without appropriate transparency and signage being installed**	Ensure that only pseudonymised data is used for monitoring purposes Make fair processing information prominently available on ULEZ pages on the TfL website as well as the RUC privacy page of the TfL website Publish DPIA Signage will be installed and	Reduced	Low	Yes	RUC Ops

	visible in the preceding month before the expanded ULEZ goes live (ie from mid-2023)				
Data retention*:* **Long term retention of live VRM data and images for ongoing testing purposes results is excessive, lacks transparency and/or could result in function creep. Compatibility concerns with the principle of data minimisation.**	The data is securely stored in a ring-fenced pre-production environment with restricted, role based access permissions. The data will not be used in conjunction with any other data available to TfL in order to identify an individual (eg the DVLA database of registered keepers). The data will not be used to inform any decision making about an individual. The RUC privacy notice was updated (Mar 2022) to aid fairness and transparency to data subjects. The dataset dates from April 2021, which means that its 'value' to a malicious or motivated intruder or the level of harm caused by any potential misuse diminishes with time. The longer term retention of a	Reduced	Low	Yes	RUC Ops

	single dataset that can be re-used for testing purposes in many respects supports data minimisation in the sense that subsequent, multiple new extracts of bulk data are not required.				
Data security: **Shift to greater home working by service provider and or TfL staff may create additional level of risk with regard to handling personal data away from a more 'controlled' or 'supervised' office environment (general risk across all RUC processing - not specific to this ULEZ expansion)**	**TfL:** Staff using privately owned devices to log on to TfL systems are required to use multi- factor authentication (MFA) – or Staff may also work from TfL owned devices that are protected with corporate level cyber security measures. Printing is disabled away from the office. All existing information governance, employee conduct and information security policies apply to home working (including requirement for annual data protection training). There is a specific TfL Procedure implemented for Information Governance and Hybrid Working. **Capita:** Staff only permitted to work	Reduced	Low	Yes	TfL RUC Ops; TfL Information Governance TfL Cyber Security Capita TfL Security Team

	on Capita owned devices that are protected with corporate level cyber security measures. Printing is disabled; website/internet restrictions in place All existing Capita information governance, employee conduct and information security policies apply to home working. All customer service agents required to complete data protection training. Endpoint DLP tools on laptops, blocking of removable media, laptop encryption and mobile device management solution.				

	To be completed by Privacy & Data Protection team	Could there be a privacy risk?
What is the lawful basis for processing? Are there any Special Category or sensitive data?	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." No special category (or crime-related) personal data will be processed by TfL as a result of an expanded camera network.	No
Is this use of personal data compatible with our original purposes for collecting the data?	Yes. The purpose of the processing remains the same as for the current road user charging schemes. Only the geographical area covered by the ULEZ would be changed under the proposal.	No
Are changes to Privacy Notice required?	There may be some minor amendments required to the privacy notice to take account of the expanded ULEX area and/or the associated awareness campaign. However, there will be no other fundamental changes to current processing that will necessitate an update.	tbc
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, Road User Charging and Your Information Rights. The MPS will be responsible for managing data subject rights in relation to their own processing of ANPR camera data as a separate controller. Information on how to do this will be available on their own website.	No
How do we safeguard any international transfers? Is any data being processed outside the UK?	The 'back office' systems for road user charging are cloud based and hosted within the EEA., which currently has an Adequacy finding from the UK Government. Safeguards on international transfers are achieved in different ways:	No

	- via DVLA requirements in respect of data sourced from their databases - through tender requirements issued by TfL to suppliers - through data processor contractual clauses - through appropriate due diligence and audits of suppliers - camera testing will take place within the EU (Ireland) which currently has an Adequacy finding from the UK Government.	
Could further data minimisation or pseudonymisation be applied?	Data minimisation principles are already applied in line with the existing road user charging schemes and have been described elsewhere in this DPIA. In order to enforce all road user charging schemes, it is necessary to use personal data, as opposed to pseudonymised data. The ability to pay the daily charge for the congestion charge / LEZ / ULEZ zones without providing a name and address has always existed and will continue to do so. (Except where required by banks or card providers in order to validate payment card transactions, eg '3D Secure'.)	No
Have appropriate security measures been considered, with Cyber Security involvement where necessary?	Cyber Security is fully involved with the project and advising on appropriate security measures (noting that existing road user charging systems will be used).	No
Are data sharing arrangements adequate? Do they require further documentation?	Any camera sharing with the MPS will require a formal data sharing agreement (in addition to the Mayoral Decision and Delegation of powers to TfL to share the cameras).	Yes
Is the data likely to be and remain adequate, accurate and up to date?	In terms of data quality, the cameras operating the scheme have an 95% read (accuracy) rate in respect of number plate recognition. The cameras also operate in accordance with the National ANPR standards used by the various police forces and is the benchmark for cameras. To mitigate against the risk of a PCN being issued against a vehicle whose number has been misread by the cameras, the ANPR read of every PCN is subject to an automated confidence check, followed by a manual, visual check prior to being issued. This also checks that the VRM links to the correct make model and colour of the vehicle as recorded in the DVLA database.	No

	This check also helps to reduce the risk of a PCN being issued to vehicle that has had its number plates cloned. The VRM read and make and model checks are not undertaken for the awareness campaign as no images are captured for this purpose. In previous campaigns, this resulted in a small number of complaints from individuals who have received letters saying that their vehicle had been seen in London, when they have not travelled there. Mitigations to prevent this occurring again have already been put in place and are described elsewhere in this DPIA.	

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Privacy Team Leader 10/05/2022	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Privacy Team Leader 10/05/2022	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Privacy Team Leader 10/05/2022	Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	This draft DPIA to be published DPIA to be updated and published once results/outcomes of the public consultation are known Subsequent expansion planning to take account of public and stakeholder responses in relation to privacy wherever possible and where they cannot be accommodated, any revised DPIA should provide an explanation for this Include analysis of proposed camera density when DPIA is updated as described above Information Sharing Agreement to be put in place with MPS in the event additional cameras are shared by TfL	
DPO Comments:	In addition to implementation of the recommendations above, consideration of the possibility of removing existing cameras (as referred to on page 9) must involve input from the Privacy and Data Protection Team.	
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:	RUC Operations and Contract Manager	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 cannot 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 person's: • 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.