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:	John Clarke	Date DPIA completed	Original DPIA: 29/09/2020; This updated version 29/03/2022
Job title:	On street Infrastructure Co-ordination Manager	Proposed launch date	25 October 2021

Name and description of the project:	The processing of personal data associated with the installation of new ANPR camera infrastructure, for the purpose of the expansion of the Ultra Low Emission Zone (ULEZ). The ULEZ was originally introduced on 8 April 2019 and covered the same geographical area as the Congestion Charge. The ULEZ operates 24 hours a day, every day of the year, in the same way as the current Low Emission Zone, which began operating in 2008. From 25 October 2021, the ULEZ boundary will be extended to create a single larger zone bounded by the North and South Circular Roads.

	This is a further update to the original DPIA that was completed in September 2020 and revised in April 2021, to take account of changes to the retention period for the data used for camera and evidential record testing purposes and to explain the rationale for these changes.				
Personal Information Custodian (PIC)	John Clarke	Is PIC aware of this DPIA?	Y	Project Sponsor	Hayley Fails

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** The expansion of the geographical area covered by the ULEZ, from the current Congestion Charging Zone boundary to the North/South Circular which is 18 times the size of the current ULEZ. It will be used to increase the emission standards of vehicles driving in Greater London and thereby improve air quality within Greater London. The current LEZ will continue to apply from the boundary of the North/South Circular Road outwards covering the rest of the Greater London area. The expanded ULEZ Scheme will be operated and enforced by the existing Road User Charging Systems, currently used to operate and enforce the current Congestion Charge, Low Emission Zone and the first phase of ULEZ (central London). The geographical locations for the current and proposed ULEZ can be seen here: http://lruc.content.tfl.gov.uk/ulez-boundary-map-from-25-october-2021.pdf The complete ULEZ zone will cover all of London within the boundaries of both the North and South Circular roads 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 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. 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 camera numbers and locations where they are installed or of extended use of the existing ANPR infrastructure; 3. The potential for further camera sharing with the Metropolitan Police (MPS), with whom an agreement already exists in relation to the Congestion Charge Zone and Low Emission Zone cameras; and 4. Monitoring vehicles and contacting drivers in advance of the expansion go-live date, in order to raise awareness of the scheme expansion and what to do to comply with the emissions standards.

Step 2: Describe the nature of the processing	
How will you collect, use, and delete data? What is the source of the data? Will you be sharing data with anyone? Are you working with external partners or suppliers? Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.) Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones? How and where will the data be stored? Will any data be processed overseas? You might find it useful to refer to a flow diagram or other way of describing data flows.	**Collection, use and deletion** On Street The expansion of the ULEZ will work in exactly the same way as the existing road user charging schemes in London – which is described on the road user charging privacy web page. There are currently 647 ANPR cameras across 198 sites used to enforce the congestion charge zone and central London ULEZ and a further 334 ANPR Cameras across 81 sites, used to enforce the Low Emission Zone, to give a total of 981 ANPR Cameras across 279 sites. These cameras operate 24 hours a day, all year. It is anticipated that approximately 1050 additional ANPR cameras may be needed to effectively administer, operate and enforce the enlarged ULEZ. Approximately one quarter of these additional cameras are existing ANPR infrastructure which are currently solely used for traffic monitoring purposes. The other three quarters (circa 750) of these additional cameras will be new cameras installed on the boundary, to capture vehicles entering and exiting the ULEZ zone, and within the zone to capture vehicle movements within the ULEZ zone. All of these additional ANPR cameras will be in locations outside the Congestion Charging Zone boundary and within the North/South Circular roads. The camera locations have been 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 are 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 that cameras are in use. These are DfT-approved road signs. Any additional cameras will also operate 24 hours a day, every day of the year – which represents no change from the existing Low Emission Zone (which has operated on this basis since 2008) and the central London ULEZ. The number of up to 1,050 additional ANPR cameras was reached based on the use/re-use of existing ANPR infrastructure, 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.

	The new cameras will begin to be installed from August 2020 and this will be completed by July 2021. 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). This testing will require the use of ANPR data and images captured by existing camera infrastructure as follows: A copy / extract of the evidential records captured by existing RUC cameras from 6 days during April 2021 will be transferred by Siemens to Capita's pre-production environment, which is hosted in Dublin. The dataset will comprise approximately 7.5million records. The data will include VRM and 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. Siemens is the service provider responsible for the installation and maintenance of the camera infrastructure. There is a full contract in place with both Capita and Siemens which includes data processing clauses. The data will be transferred via a dedicated secure FTP transfer which only one Capita user will have access to download this data. Once processed, the images will be flowed into the pre-production environment to which all testers will have access. The data will be used to test the 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 by the end of August 2021. at which point it was originally intended that the data would be securely deleted. It has subsequently been identified that there is a need for further testing from time to time, for example to test subsequent camera system updates or patches, or to test the performance/capacity of infrastructure and back office systems in response to proposed scheme changes. As a result there is value in retaining the data extract for this purpose, and it was not deleted at the end of August 2021 as originally planned. It has been identified that there is less risk in retaining an existing bulk dataset rather than creating a new bulk download on each occasion that it might be required. As this dataset dates from April 2021, there is also a decreasing risk of any potential harm or detriment being caused as the data ages over time. The need to use real VRMs and vehicle images for any 'business as usual' testing will be documented and assessed in a separate DPIA. The risk of testing data being inadvertently used to affect a data subject or to make decision about them (eg 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 Amdocs or Taranto which are used to generate daily charges and Penalty Charge Notices. From June 2021 the cameras will be used for traffic monitoring purposes using TfL's existing London Vehicle Analysis Tool (LVAT), 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 data 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 official launch of the expanded ULEZ in October 2021, 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 until the month prior to go live (ie during September 2021), therefore other measures will be required. Steps to mitigate this risk are described in section 9 below. It is not intended that any camera data from the new ULEZ cameras will be shared with the MPS during this time, before the ULEZ expansion goes live. Use of the cameras for enforcement purposes will commence 25 October 2021. (This will include enforcement of ULEZ, LEZ and the Direct Vision Standard for heavy goods vehicles.) <u>Compliance and Awareness campaign</u> As with the central London phase of ULEZ, during the run-up to the go live date for expansion, it is intended that from January 2021 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 the expanded ULEZ Scheme in October 2021 and will be encouraged to visit TfL's website to find out further information. The activity will capture VRMs of vehicles seen driving within Greater London from October 2020. 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 central Ultra Low Emission Zone. Those VRMs that are non-compliant will then be checked against TfL's existing 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.

	The remaining non-compliant VRMs will then be sent 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 detailed privacy issues connected with a similarly designed awareness campaign were considered and mitigated in a DPIA for the launch of the central London ULEZ. As a result of that campaign, the following two issues were identified • 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 • no 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. <u>The expanded ULEZ Compliance and Awareness Campaign will avoid these issues by:</u> • including the VRM on the DVLA letter to inform the registered keeper which vehicle was observed and is non-compliant; and • validate 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. <u>Camera Sharing</u> There is currently a working assumption at an operational level that any new cameras installed will be added to those Congestion Charge Zone and Low Emission Zone cameras already shared with the MPS. This sharing is subject to a Mayoral Delegation from January 2015. TfL held initial discussions with the MPS in February 2020 and has sought appropriate advice as to whether this assumption is valid and whether an updated Mayoral Delegation should be sought from the current Mayor. It has now been confirmed that an updated Mayoral Delegation will be required before the commencement of any additional camera sharing with the MPS. Under the previous DPA 1998, data from the cameras was shared on a 'data controllers in common' basis. This concept does not exist under the GDPR or DPA 2018, therefore since May 2018 TfL and the MPS act as separate 'controllers' for the processing they are each responsible for.

	In addition, the MPS as a 'competent authority' for criminal law enforcement purposes is subject to Part 3 (and Schedule 8) of the DPA 2018 that incorporates the EU Law Enforcement Directive. TfL is not a competent authority in its processing of personal data for Road User Charging purposes. At present, the MPS access to ANPR data is limited to the alpha-numeric feed of VRM data and does not include the photographic images of vehicles. Going forward, if a decision is taken to share the camera network in the expanded Zone, and as the camera infrastructure is replaced and updated, the photographic images will be provided to the MPS through inclusion of these images in a file sent directly from the ANPR Cameras to the MPS systems. This DPIA will not further consider the MPS use of any ANPR data, other than the issue of whether TfL needs a revised Mayoral Delegation in order to make the sharing of data / infrastructure lawful (ie within TfL's statutory functions). <u>External Suppliers</u> 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, will transfer the data to Capita. Capita has overall responsibility for the camera testing activity. If 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). 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. In order to issue a PCN to the Registered Keeper (where a 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 audit by the DVLA.

	Any new cameras installed to monitor/enforce the ULEZ will utilise encrypted mobile 4G communications provided by O2, under contract with appropriate data protection clauses All data is stored either in the UK or in the European Economic Area (EEA).

Step 3: Describe the scope of the processing	
Who does the data relate to? How many individuals are affected? Does it involve children or vulnerable groups? If children's data is collected and used, are they aged under 13? What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*) Specify which special category data or criminal offence data are to be processed? Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data? How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process? Is the data limited to a specific location, group of individuals or geographical area?	**Who does the data relate to?** The data captured will relate to vehicles travelling on roads within Greater London. **How many individuals are affected?** Pre-coronavirus, on an average day, the number of unique vehicles captured via the ANPR cameras within the Central ULEZ was 115,000. Current analysis (without accounting for any effects of coronavirus) suggests that the volume of unique vehicles that will be captured across the expanded ULEZ will increase by 500% to approximately 575,000 vehicles, of which 25% are not compliant with the ULEZ emission standards. **Does it involve children or vulnerable groups?** None of the road user charging schemes, including the ULEZ is intended to capture data of children or vulnerable adults. Any enforcement of the schemes is directed to the registered keeper of the vehicle in each case. It is possible that data may be processed which indirectly enables locations to be inferred for children or vulnerable adults (by associating a vehicle known to contain them with the site of a particular camera). The cameras installed will have a wider range of view than previously, 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. **What is the nature of the data?** On street 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 5 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. The data currently accessible by the MPS is limited to the alpha numeric feed of the VRM only; they do not receive still photographic images of the vehicles. New camera infrastructure will allow the photographic images to be shared with MPS alongside the ANPR data.

	Specify which special category data or criminal offence data are to be processed? None. In addition, enforcement of road user charging schemes by TfL is a civil matter, not a criminal offence. TfL is not responsible for the MPS' processing of ANPR data for criminal law enforcement purposes (ie their processing under Part 3 of the DPA 2018). **Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?** The minimum personal data possible is processed for the enforcement 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. However, it is not possible to enforce the scheme using anonymised or pseudonymised data, because the PCN needs to be issued to the Registered Keeper (the person liable to pay the PCN). The camera testing activity needs to use 'real-life' VRMs and image captures because the technology cannot be adequately tested using dummy data. **How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion 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 Evidential Record data (comprising ANPR data, photographic image and date/time/location) and 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 (as described in Step 2) will be retained within TfL systems for longer than its usual retention period – specifically that data that would normally be deleted after 21 days. Since the completion of the original DPIA, it has subsequently been identified that there would be a benefit in retaining this same data in the longer term so it could also be re-used in cases where there is a need

	for further 'business as usual' testing from time to time, for example to test subsequent camera system updates or patches, or to test the performance/capacity of infrastructure and back office systems. No data held in these circumstances will be used for any other purpose than testing and proving system changes. Retaining a single bulk dataset for this purpose represents a lower risk than creating multiple ad hoc downloads of new data each time a need is identified. 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). At such a time that TfL requests deletion of this dataset, Capita will provide evidence to TfL when it has been completed. **Is the data limited to a specific location, group of individuals or geographical area?** Data will be related to vehicle Keepers/Owners/Operators. 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 is geographically limited to London, within the boundaries of the North and South Circular roads.

Step 4: Describe the context of the processing	
Is there a statutory basis or requirement for this activity? 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.)* How much control will individuals have over the use of their data? Would they expect you to use their data in this way? Are there prior concerns over this type of processing or security flaws? Is it novel in any way, or are there examples of other organisations taking similar steps? What is the current state of technology in this area? Are there any security risks? Are there any current issues of public concern that you should factor in? Are you or your delivery partner signed up to any code of conduct or certification scheme?	**Is there a statutory basis 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 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 Road safety and emissions from vehicles. The introduction (and expansion) of the ULEZ is covered by a Scheme Order contained as a schedule to the Greater London Low Emission Zone Charging Order 2006, as amended, together with a number of Variation Orders. In addition, the Mayor of London has a legal responsibility to prepare an Air Quality Strategy in order to improve air quality in London. The implementation of the ULEZ will contribute to this **How much control will individuals have over the use of their data?** 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 the MPS processing, this would be covered in their own DPIA, and subsequent processes they would put in place. These are unconnected to TfL's own processing. **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 TfL publishes online. **Are their prior concerns over the type of processing or security flaws?** Possibly; please see the entries for security risks and issues of public concern below. **Is it a novel approach or are there examples of other projects or 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 in central London. **What is the current state of technology in this area?** Advanced - using digital, high definition cameras with Automatic Number Plate Recognition (ANPR) software **Are there any security risks?** 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 network. **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). **Are you or your delivery partners signed up to any code of conduct or certain certification scheme?** All of the road user charging schemes (including the ULEZ) are subject to UK and European 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.

Step 5: Describe the purposes of the processing	
What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for TfL, for other external stakeholders, for the individuals concerned and for society in general?	**What do you want to achieve?** The ULEZ is an amendment to the existing LEZ Scheme which was introduced in 2007 to reduce the amount of harmful emissions from HGVs, buses and coaches. With the implementation of the Central Ultra Low Emission Zone (ULEZ) on 8 April 2019 and the extension of the ULEZ to the North/South Circular roads from October 2021, amendments to the existing LEZ Scheme have been confirmed to further reduce the harmful emissions from vehicles that are driven within the ULEZ – and so improve air quality. **What is the intended effect on individuals?** The 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. **What are the benefits of the processing** **- Commercial benefits** TfL's revenue from those who pay the daily ULEZ charge will be reinvested directly into improving the transport network in London. Non-compliant vehicles which drive within the ULEZ and do not pay the appropriate daily charge will be subject to targeted enforcement, with Penalty Charge Notices issued. These penalty charges, like other penalty charges for similar schemes in London (CC/LEZ etc.) will also bring revenue to TfL, with the money reinvested. . **- Operational benefits** Installation of additional cameras will allow TfL to effectively administer, operate and enforce the expanded ULEZ in line with the Scheme Order in order to realise the anticipated benefits of the scheme **- Benefits to TfL customers/employees** A reduction in the volume of harmful emissions emitted by vehicles driving within the ULEZ and a potential improvement in air quality within Greater London – which offers substantial health benefits.

Step 6: 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. Who else do you need to involve within TfL? Have you discussed information security requirements with CSIRT? Do you plan to consult with external stakeholders? If so, who? Who will undertake the consultation? What views have been expressed by stakeholders?	A number of consultations have taken place on the introduction of the ULEZ and its expansion, between 2014 and 2016. (However, data protection and/or privacy concerns were not specifically addressed by these consultations.) Details of these have all been published on the TfL website here: https://tfl.gov.uk/corporate/publications-and-reports/ultra-low-emission-zone 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. All relevant departments/team within TfL are involved with the project to expand the ULEZ, including where, necessary, CSIRT. To date (September 2020) there has been some public commentary on the expansion of the ULEZ, in particular on the need to install additional cameras and the MPS access to these cameras; see Mayorwatch comments from September 2018. Privacy related concerns have also been expressed by individual London Assembly member(s) to the Mayor, on the potential for increased intrusion from additional ANPR cameras and the volumes of additional data that will be collected as a result of the expanded zone. In addition, the Conservative Mayoral candidate for the (delayed) election, now due to be held in 2021 has expressed opposition to the expansion of ULEZ and privacy related concerns about the scheme may feature in the Mayoral election campaign.

Step 7: Assess necessity and proportionality	
Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals about how their data is used? 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?	The numbers of additional ANPR cameras (and their proposed locations) are considered proportionate because the geographical size of the area is increasing from 21km^2 to 379km^2 and TfL are required to effectively administer, operate and enforce the ULEZ scheme and treat everyone equally. As a comparison, the Congestion Charging/Ultra Low Emission Zone has a camera density of a camera every 0.1 square kilometres whereas the expanded Ultra Low Emission Zone is proposed to have a camera density of a camera every 0.25 square kilometres. The number of additional cameras in the expanded Zone has been assessed as adequate to provide confidence that compliance with the Scheme will be such that its objectives will be achieved, without capturing every vehicle movement in the Zone. **Does the processing actually achieve your purpose**? Yes **Is there another way to achieve the same outcome?** No - not to the extent that the 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 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 are the only known way to provide evidence of a vehicle's presence in a road user charging zone without the need of 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. In terms of ANPR camera sharing with the MPS, and whether this is proportionate; TfL was directed by the then Mayor in 2012 to share its camera infrastructure. TfL will share any new infrastructure depending on the outcome of the MPS's own DPIA (and public consultation if deemed necessary) on the privacy issues; together with a revised/updated Mayoral Delegation. The necessity and proportionality of the camera sharing will be

	assessed through that process. It could be argued that sharing access to an existing camera network actually reduces the numbers of cameras surveilling public spaces, as it means the MPS (in this case) does not have to install further cameras of its own. **How will you prevent function creep?** 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. **How will you ensure data quality and data minimisation?** Through internal quality controls. The current Road User Charging schemes already operate on the basis of using the minimum personal data possible for the purpose, and the ULEZ scheme is the same. The ability to pay the daily charge to enter the Congestion Charge / LEZ / ULEZ zones without providing 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'). In order to enforce all road user charging schemes (ie where the daily charge has not been paid), it is necessary to use personal data, as opposed to pseudonymised data. Data Minimisation is also achieved in the following ways: Once TfL has verified the vehicle is ULEZ compliant, then the vehicle data captured by the cameras is deleted within 21 days as there is no further business need to retain that data. Where the vehicle is identified as exempt from the ULEZ requirements, then the vehicle data captured by the cameras is deleted within 21 days as there is no further business need to retain that data Where the daily charge has been paid (and the payment verified), then the vehicle data captured by the camera is deleted within 21 days, (or within 90 days for auto pay account holders who receive a monthly statement) - as there is no further business need to retain that data. The only exception to this is where ANPR data and images are required for camera testing purposes (and also subsequent, longer term 'business as usual' testing purposes), where data that would have ordinarily been deleted within 21 days will be kept for longer. However the re-use of a single dataset captured for this purpose will in effect, minimise the amount of data that is required for testing purposes – as opposed to requiring a new extract of live data on each occasion that testing is required. . The testing will not have any effect or impact on any individual.

	In terms of data quality, both old and new cameras operating the scheme have an 95% read (accuracy) rate in respect of number plate recognition. However the new cameras will have trigger rate of 98% of vehicles passing which is also in accordance with the National ANPR standards used by the various police forces and is the benchmark for cameras. The difference between the old and new cameras is the field of view in so far as the old camera does this on a 2m wide section of the road (hence TfL require multiple cameras in CCR/LEZ installations to capture the full road width) whereas the new camera does this on up to 3 lanes of traffic up to 9.5m wide. 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 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. 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. In the previous campaign, 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 are described in Step 2 above **What information will you give individuals about how their data is used?** Through public facing information on the existing TfL Privacy pages and the Road User Charging scheme pages of the TfL website. 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 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.

To be completed by Privacy & Data Protection team	
What is the lawful basis for processing? How will data subjects exercise their rights? How do we safeguard any international transfers? Could data minimisation or pseudonymisation be applied? Are data sharing arrangements adequate?	**Are suppliers processing personal data safely and lawfully?** 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 **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." **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 is responsible for managing data subject rights in relation to their own processing of ANPR camera data as a separate controller. We expect this to be included in their own DPIA on accessing the expanded camera network. **Safeguards on international transfers** are achieved in different ways: - 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. **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 to enter 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'.) **Data sharing - DVLA** Data sharing arrangements between TfL and DVLA will need to be in place in respect of the VRM data passed to them for any awareness letter campaign. This would replicate what was undertaken for the Central ULEZ, and for which a DPIA has already been completed. In line with principles of data minimisation, TfL does not share any data with the DVLA that identifies exactly where or on what date a vehicle has been seen. **Data Sharing - MPS** TfL has had a camera infrastructure sharing arrangement in place since 2015 with the Metropolitan Police Service (MPS) in respect of ANPR cameras used for the Congestion Charge, and Low Emission Zone (the same cameras are currently also used for the central London phase of the ULEZ). The MPS and TfL in effect share the cameras, each being a data controller in respect of the purposes each partner uses the cameras for. This relationship is the result of a Mayoral manifesto commitment in 2012 to instruct TfL to give the Metropolitan Police Service (MPS) direct real time access to its Automatic Number Plate Recognition (ANPR) cameras used to enforce our Road User Charging schemes, for the purposes of preventing and detecting crime – and is the subject of a Mayoral Delegation and Direction to TfL The original proposal for TfL to give access to its camera infrastructure was subject to both a public consultation and a Privacy Impact Assessment (PIA – as it was then called)) completed by the MPS. The results of both are available via the hyperlink above. The completion of a new DPIA by the MPS will be required on the subject of their extended access to surveillance cameras on London's road network and any privacy implications associated with this. Consideration will also need to be given by the MPS as to whether there should be further public consultation regarding privacy in respect of the MPS's access to additional cameras. As stated elsewhere in this DPIA, the current working assumption (at an operational level) is that any new ANPR cameras installed by TfL for road user charging schemes will be included in those available to the MPS for the purpose of preventing and detecting crime. The existing Mayoral Delegation and Direction will also require updating to specifically reference any additional cameras installed for the ULEZ expansion prior to access be given.

Step 8 – 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, moderate or significant)**	**Overall risk** **(Low, medium or high)**
Proportionate processing and data minimisation: **Excessive data collection resulting from additional ANPR camera infrastructure**	Possible	Significant	Medium
Proportionate processing (corporate risk): **Public/political/legal challenge that camera numbers are disproportionate**	Possible	Moderate	Medium
Proportionate processing (corporate risk): **Public concerns about police access (specifically) to greater number of surveillance cameras; leading to legal challenge**	Possible	Moderate	Medium
Proportionate processing:	Remote	Significant	Medium

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			
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	Moderate (distress)	Medium
Fair processing: **New cameras are installed and are used for monitoring purposes before the scheme go-live and without appropriate transparency.**	Possible	Moderate (corporate compliance risk relating to transparency and fair processing)	Medium
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. Not compatible with the principle of data minimisation.**	Possible	Moderate	Medium

Step 9: 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)**
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 had the charge paid). 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 to be 25% of all vehicles).	**Reduced**	**Low**	**Yes**

	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 (value management exercise) 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**
Proportionate processing (corporate risk): **Public concerns about police access (specifically) to greater number of**	To be addressed by MPS DPIA; Camera sharing with the MPS not to commence until MPS DPIA (and public consultation	**Reduced**	**Low**	**Yes**

surveillance cameras; leading to legal challenge	completed if deemed necessary) with a positive outcome and Mayoral Delegation issued			
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**
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**

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 visible in the preceding month before the expanded ULEZ goes live (ie from mid-September 2021)	**Reduced**	**Low**	**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. Not compatible 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. A DPIA will be completed in respect of the data's longer term use for testing, and function creep will also be addressed within that.	**Reduced**	**Low**	**Yes**

	The RUC privacy notice has been 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/motivated intruder or the level of harm caused by any potential misuse diminishes with time. The longer term retention of a 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.			

Step 10: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Lizzie Meadows 06/04/2022	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Lizzie Meadows 06/04/2022	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Lizzie Meadows 06/04/2022	Privacy & Data Protection team should advise on compliance, Step 9 measures and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	The number and locations of the ANPR cameras used to enforce and monitor the expanded ULEZ should be regularly reviewed to ensure they remain in proportionate numbers and locations Privacy and Data Protection to ensure that relevant fair processing content is added to the Road User Charging website by 1st October 2020 - when the public awareness campaign for the expanded zone is due to commence. (COMPLETE) Project Team to confirm to Privacy and Data protection team when the camera testing work is complete and the ANPR/image test data has been permanently deleted. RUC/PPD to advise Privacy and Data Protection team when further requests for live testing data are received. ***New:*** RUC privacy web page further updated in April 2022 to take account of the revised retention requirements for testing data.	
DPO Comments:	Confirmation is required from the project team and PIC that all the measures described in Step 9 above to reduce or eliminate risks are accepted	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):	**Accepted by Hayley Fails; Lead sponsor 28/09/20**	If overruled, you must explain your reasons below.
Comments:		
Consultation responses reviewed by:	n/a	If your decision departs from individuals' views, you must explain your reasons.

Comments: n/a		
This DPIA will kept under review by:	Road User Charging Directorate	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.
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 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.