# 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: | Road User Charging (RUC) Head of Operational Delivery | Date DPIA completed | August 2023 |
| Job title: | RUC Head of Operational Delivery | Proposed launch date | 29 August 2023 (launch date of the London Wide ULEZ) |
| Name and description of the project: | The processing of personal data associated with the expansion of the Greater London Ultra Low Emission Zone (ULEZ) on 29 August 2023, and the continued operation of the London Low Emission Zone (LEZ) has been previously considered in a separate DPIA. This DPIA concerns the use of mobile vehicle mounted ANPR cameras (also referred to as Mobile Enforcement Vehicles) to support the expansion of the ULEZ to outer London which will operate on a London-wide basis, as well as its joint operation and enforcement with the LEZ.<br>This DPIA covers the following areas:<br>• the impacts and assessments for the use of electric powered vehicles ('mobile enforcement vehicles') with ANPR cameras affixed to the roof for the purpose of supporting the fixed ANPR cameras for the ULEZ and LEZ scheme;<br>• ensuring only vehicle data is captured; | | |

| | | | | | |
|---|---|---|---|---|---|
| | • back office/systems and infrastructure testing/development activities;<br>• the additional volumes of personal data (Vehicle Registration Marks -‘VRMs’) that would be processed;<br>• (To note, the ANPR cameras fitted to the vehicles will be the same camera type as those used to enforce the Congestion Charging, Low Emission Zone and also the Ultra-Low Emission Zone via the fixed, on-street infrastructure.) | | | | |
| 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 (Air quality, Environment and Technology). |

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

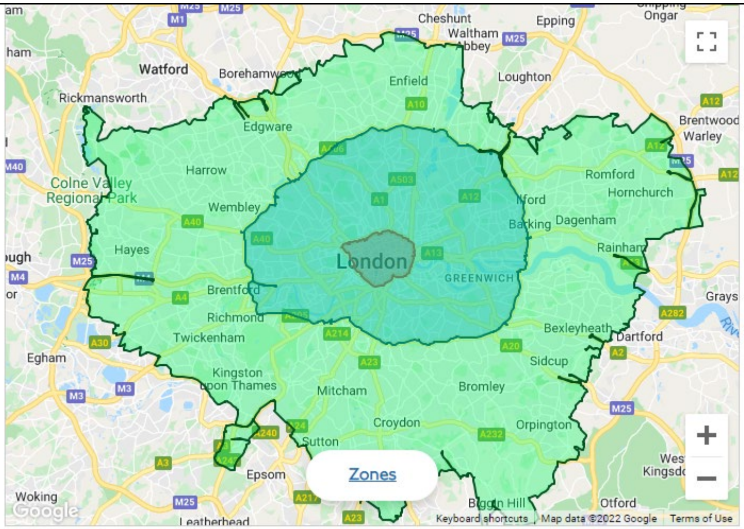
| | | | | | |
|---|---|---|---|---|---|
| Use profiling or automated decision-making to make decisions that will have a significant effect on people. Significant effects can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits. | **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. | **X** |
| 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.<br>You may find it helpful to refer or link to other documents, such as a project proposal.<br>Summarise why you identified the need for a DPIA. | **Project Aims**<br>The geographical area covered by the ULEZ is being expanded on 29 August 2023 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”).<br>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.<br>The current LEZ will also continue to apply and be enforced in the same way as the ULEZ within the same London-wide geographical area (for those larger/heavier vehicles that are affected by that scheme). An expanded ULEZ Scheme will be operated and enforced by the existing Road User Charging (RUC) 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:<br>https://tfl.gov.uk/ruc-cdn/static/cms/documents/ulez-boundary-map-main.pdf<br>and the extent of the expanded zone to cover the LEZ area can be seen here:<br>https://tfl.gov.uk/ruc-cdn/static/cms/documents/low-emission-zone-map.pdf<br>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 use of mobile ANPR camera vehicles for the purpose of plugging in the gaps where there are no fixed, on-street operational cameras installed or where there are ANPR camera that are  inoperative, particularly in terms of the following:<br>• The testing and development of mobile ANPR camera vehicles. The testing will be completed in various locations in London not covered by RUC ANPR cameras or non-operationally working cameras in general. The back office/systems and infrastructure testing/development activities require the use of an extract of real Vehicle Registration Mark (VRM) data and contextual images from the mobile ANPR camera vehicles;<br>• The use of multiple mobile ANPR camera vehicles to enforce scheme integrity inside the ULEZ where ANPR cameras have not been installed, or where there are gaps within the zone due to inoperative equipment. |

| | |
|---|---|
| | - The potential for the collection of increased volumes of personal data during the operation and enforcement of the expanded ULEZ, because of the mobile ANPR camera vehicles operating inside the expanded zone; |
| 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**<br>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.<br>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 or into 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.<br>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.<br>**Commercial benefits**<br>As with the existing RUC schemes, including the inner London ULEZ, LEZ and Congestion Charge, surplus revenue must be reinvested in public transport to support the delivery of the Mayor's Transport Strategy.<br>**Operational benefits**<br>Installation of the mobile ANPR vehicles is an agile solution which will allow TfL to effectively administer, operate and enforce the expanded ULEZ area in line with an (amended) Scheme Order in order to realise the anticipated benefits of the scheme – by facilitating camera coverage in areas not covered by fixed, on street ANPR camera infrastructure. |
| Will the processing directly affect the individuals concerned? | Yes. The broader intended effect on individuals of ULEZ and its expansion 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.<br>All those living and working in London will benefit from improved air quality as a result of reduced vehicle |

| | |
|---|---|
| | emissions.<br>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.<br>A greater proportion of vehicles driving into, out of or across London are likely to pass by a TfL ANPR camera and will have their VRM recorded than currently, due to the expanded camera network (though the VRM will be pseudonymised if the vehicle is known to be ULEZ-compliant – see Step 3). The period that that data will be stored will vary in line with the published RUC privacy notice 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**<br>The expanded ULEZ will 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.<br>The current camera network can be broken down into three different 'rings' -<br>There will be approximately 248 ANPR cameras principally used to enforce the congestion charge zone that can also capture vehicles liable for the LEZ and ULEZ ('central ring').<br>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').<br>Outside the current inner London ULEZ zone there will be (once an existing camera refresh programme is complete) approximately 119 cameras enforcing the LEZ only.<br>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).<br>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 will 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. Some of the approximate 2,750 enforcement cameras, will be deployed on mobile enforcement vans that will be used across London to ensure the scheme integrity on the boundaries and inner zone by being in locations where camera coverage is limited due to installation or camera operational issues.

There will be approximately 20 mobile camera vehicles that will operate and enforce inside the ULEZ area. It is anticipated that these vehicles will be agile in their locations and will operate across any boroughs on a day-to-day basis. The vehicles will have clear signage on the sides and rear of the vehicles for the public to clearly understand the purpose of these vehicles and who will operating them.

The camera locations will be determined to maximise the effectiveness and efficiency of the Scheme, chiefly by locating the mobile ANPR camera vehicles where ANPR cameras are not operationally working or have not been installed. The mobile ANPR camera vehicles’ locations will take into consideration safety and parking restrictions within the boundaries and inner area of the expanded Zone.

The mobile 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 vehicles are moved as described above, they will still be within the areas covered by on street 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.

Considerations around the number and density of the ANPR cameras required to enforce ULEZ has been described in previously published DPIAs.

The use of mobile camera vans will be reviewed continually by TfL to ensure data minimisation.

**Mobile cameras Performance and Capacity testing (phase 1)**

The testing activities for the mobile ANPR camera vehicles began in late July to ensure that back office systems currently used for road user charging can process the data from these mobile ANPR cameras, and to ensure that only the road space is captured. The testing is also to provide assurance that the additional volumes of data can be processed to the required standard and reliability for this scheme.

The testing will be achieved by using an extract of the evidential records (ER) captured by these mobile ANPR cameras installed on these vehicles, the volume of data used will be approximately 100k worth of ERs which will be unique to single VRMs. The data collected will be used for testing from late July until the end of December 2023, after this date the data will be destroyed. The rationale for keeping the data after go live is due to testing any future system upgrades and will be used only in the pre-production environment delivered by Capita under the current contract.

There will also be a subset of the original data used for testing from the first expansion of the ULEZ scheme in 2021. 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 from the mobile ANPR camera vehicles will be transferred via the ‘Business As Usual’

| | | |
|---|---|---|
| | encrypted route to Yunex's data centre (Yunex, formerly known as Siemens, are responsible for the installation and maintenance of all the ANPR cameras used for road user charging) and then onto Capita systems. Once processed, the images will be flowed into the pre-production environment to which testers will have access.<br>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 scheme go live date of 29 August. 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.<br>The risk of testing data being inadvertently used to affect a data subject or to make a 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.<br>**Mobile cameras Performance and Capacity testing #2**<br>The mobile ANPR camera vehicles are being tested from 24 July 2023 and throughout August 2023. It is intended that once the fleet of the mobile ANPR camera vehicles are operational, they will initially be used for testing and business planning purposes to ensure the concept works. Once the testing has been completed, they will be used to ensure scheme integrity and to ensure the cameras only capture vehicles driving on the roads entering/exiting or driving inside the ULEZ area.<br>**Pre-go-live traffic monitoring**<br>The mobile ANPR camera data will not be used for traffic monitoring.<br>**Compliance and Awareness campaign**<br>The mobile ANPR camera data will not be used in any advance awareness campaigns (pre go live). | |
| Will you be sharing data with | **Camera Sharing with Metropolitan Police Service (MPS)** | No |

| | | |
|---|---|---|
| anyone? | TfL does not intend to share the data from the mobile ANPR camera vehicles with any third parties, including the MPS. | |
| 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.<br>Yunex, (formerly known as Siemens), are responsible for the installation and maintenance of the cameras including the mobile ANPR 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 to ensure data is not being used unnecessarily.<br>Capita has overall responsibility for the camera (and associated systems) 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 Yunex 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.<br>Any new cameras, including those on the mobile enforcement vans, 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 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.<br>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 required to be shared with TfL.<br>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 | No |

| | | |
|---|---|---|
| | adequate.<br>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? | Not during testing but after go-live, 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 to, and use of, the data is subject to regular audit by the DVLA.<br>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 fixed, on street ANPR cameras at the roadside and from the mobile camera vans is transferred by Yunex to Capita using encrypted mobile 4G communications<br>The retention period for any personal data stored is subject to a local disposal schedule; data is stored for the minimum period possible for the purpose. | No |

| | | |
|---|---|---|
| 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.<br>Some testing activities take place using remote access to data from overseas locations. This includes locations within the EEA as well as Argentina, India, Israel. Where required, the appropriate International Data Transfer Assessments have been conducted as well as contractual provisions implemented. | 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:<br>• vehicles travelling on roads within Greater London,<br>• individuals who have an online account to pay a daily charge or to manage a discount<br>• where PCNs are issued, the Registered Keepers of those vehicles | No |
| How many individuals are affected? | As stated in previously published DPIAs for ULEZ:<br>On an average day, the number of unique vehicles currently captured and then processed for payment or enforcement purposes via the ANPR cameras within the existing ULEZ is in the region of 900k.<br>Although the proposed ULEZ expansion would cover a bigger geographical area, the volume of expected unique vehicles captured for payment/enforcement purposes will only increase slightly.<br>The reason for this is that in order to reduce unnecessary processing of data (and so adhere to the principle of data minimisation), only vehicles that are not ULEZ compliant will be further processed by the camera system (ie to confirm payment of a daily charge or issue a PCN) with data and images of any ULEZ compliant vehicles that enter the zone being filtered out.<br>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 with the required emissions standards. The filtering process minimises the volume of ANPR data and images that is required to be sent to Capita (who provide services to enforce road user charging schemes for TfL) and aims to only process VRMs that are required for road user charging purposes (ie to confirm payment of a daily charge or issue of a PCN).<br>Traffic Monitoring (as described in Step 2 above) will also take place using Road User Charging cameras. This activity will include all vehicles that pass by an ANPR camera (except for the mobile cameras).  However, it is important to note that individuals are not affected by this processing as data used by TfL for traffic monitoring is pseudonymised so that VRMs cannot be associated with | Yes |

| | | |
|---|---|---|
| | individual registered keepers.<br>. | |
| 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.<br>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 with a vehicle, 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 directed towards traffic (and further – to the number plate / bonnet area of vehicles rather than the windscreen.<br>To note also that all cameras (fixed and mobile) will only trigger a capture when a number plate enters the field of view and the number plate is in motion. Parked vehicles within the field of view will not be captured as they will not be in motion.<br>It is also important to note that ANPR cameras (including the mobile cameras) do not capture rolling video footage, and any imagery is in the form of still photographic images to enable the read of the Vehicle Registration Mark (VRM), to be confirmed against the recorded make, model and colour of a vehicle.<br>TfL would have no means of identifying any pedestrian inadvertently captured in a still photographic image, however the ANPR cameras will not be triggered by pedestrians crossing in the ANPR field of view.<br>During each set up of the mobile ANPR camera vehicles, the operator will ensure that no property is in the field of view of the camera or any other private or commercial property - and as far as possible minimise the scope for capturing images of pedestrians or other bystanders on pavements. | No |
| What is the nature of the data? (Specify data fields if possible; For *example, name, address,* | 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. This is the same | No |

| | | |
|---|---|---|
| *telephone number, device ID, location, journey history, etc.*)<br>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 | regardless of whether the camera is fixed on-street infrastructure or a mobile camera installed onto a vehicle.<br>Where enforcement of the ULEZ is necessary (i.e. when a charge is applicable but 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.<br>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. | |
| 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.).*<br>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.<br>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))<br>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.<br>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.<br>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 | No |

| | | |
|---|---|---|
| | compliant with the ULEZ standards. A camera is only triggered when a VRM enters its field of view and when the vehicle is in motion.<br>ANPR data is pseudonymised before being processed for the purposes of traffic monitoring and transport planning to reduce the risk of 'real world' identification.<br>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).<br>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. | |
| How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data? | The mobile ANPR cameras will work in the same manner as the rest of the RUC camera estate that enforce the Congestion Charge, Low Emission Zone and the Ultra Low Emission schemes. The only exception is that the mobile ANPR cameras will be affixed to a van roof and therefore may move locations throughout the day.<br>When the vans are in motion, the ANPR cameras will not capture any data, the only time the mobile ANPR cameras capture data will be when they are stationary/parked up legally and safely inside the ULEZ zone.<br>Before the mobile ANPR cameras capture any data, the operator will check to ensure the ANPR camera field of view is the road only to minimise capture of private or commercial property within the imagery. As referenced throughout this document, the ANPR camera will only detect vehicles that are in motion, this protects any vehicles that may be parked within the ANPR field of view.<br>The ANPR cameras are all tested to ensure that they work accurately in varying weather and light conditions.<br>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?<br>Who is responsible for this deletion process?<br>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.<br>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.<br>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).<br>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...<br>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.<br>The Act also states that TfL has a duty to 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. The current MTS (2018) has been revised to include a formal proposal to expand the ULEZ London-wide (Proposal 24.1). 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.<br>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 is implemented by a variation order that extends the area of that Zone to the boundary of the LEZ.<br>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 its capacity as the statutory charging authority for those schemes.<br>In addition, the Mayor of London has a legal responsibility to prepare an Air Quality Strategy (as part of his London Environment 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.<br>TfL's use of ANPR cameras for road user charging schemes is recognised in law for enforcement purposes, under regulations dating from 2001 – and an ANPR camera is a "prescribed device" under the Road User Charging (Enforcement and Adjudication) (London) Regulations 2001/ 2313 (as amended). | 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.<br>Individuals who have a RUC account will have control over the use of data for marketing purposes, via an 'opt in'.<br>No other Road User Charging customer will receive marketing from TfL.<br>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 | 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. | 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<br>PCNs will also include a privacy notice (as they currently do for road user charging and other traffic enforcement).<br>The online privacy notice for ULEZ has been updated to include reference to the use of mobile ANPR cameras.<br>All of the mobile ANPR vans will have clear signage identifying them as using ANPR cameras operated by TfL on both sides and the rear of the vans.<br>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. | No |

| | | |
|---|---|---|
| | In terms of the distribution of on-street signage, this will be placed on the boundary roads for the scheme (including in advance of the boundary) and supported with in-zone-repeater signs. Collectively, these signs will provide information to inform drivers that TfL is using cameras for the purpose of operating ULEZ. There are three key purposes of the signage –<br>• To advise drivers that they are in the Ultra Low Emission Zone;<br>• To advise drivers that there are enforcement cameras in operation in the area<br>• To help meet TfL's fair processing obligations under data protection legislation (alongside the information published online and on Penalty Charge Notices).<br>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. | |
| 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.<br>The use of mobile enforcement vehicles is commonplace amongst local authorities and other agencies responsible for roads and traffic compliance. | 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.<br>All mobile 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. | No |

| | | |
|---|---|---|
| Are there any current issues of public concern that you should factor in? | The expansion of ULEZ is a matter of current controversy and opposition to it has included physical attacks on camera infrastructure.<br>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.<br>Questions relating to privacy and data protection were included in the public consultation on the proposal to expand the ULEZ that took place between May-July 2022. More information can be found in Step 5 of this DPIA below. | 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<br>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).<br>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 training for employees? | Yes, the mobile ANPR camera operators will be trained to ensure that the ANPR camera field of view is only on the road to minimise any inadvertent capturing of private or commercial property. The process for reporting back locations will be included within the training.<br>Capita will complete a quality control over this process alongside TfL RUC Operations as part of the monthly monitoring process regime across the performance and quality of the Capita contract.<br>The expansion of the scheme will increase the overall scale and volume of processing and 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.<br>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 | No |

| | | |
|---|---|---|
| | statutory timescales. | |
| Does the processing actually achieve your purpose? | Yes – changes in vehicle numbers, type and emissions and air quality since the implementation of ULEZ are being monitored and show the scheme's objectives are being achieved. See the monitoring reports published at https://tfl.gov.uk/corporate/publications-and-reports/ultra-low-emission-zone#on-this-page-1<br>Please see the explanation below as to why 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 expanded 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.<br>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.<br>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 VRMs correctly | No |
| Who will own this initiative and ensure there is no function creep without a review of this DPIA? | RUC's Personal Information Custodian (PIC) will own the DPIA aspects of the camera systems, including the mobile cameras, and function creep will be monitored through the use of robust change control processes, together with a review of this DPIA in the event of a change to the intended use of mobile cameras 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:**<br>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 took place between May and July 2022, including on a variation order to amend the 2006 Scheme Order for that purpose.<br>The consultation materials included specific content on privacy (including a DPIA). This however was prior to the development of the current proposal to deploy mobile ANPR cameras. The consultation process, the privacy-related responses to it and TfL's response to those was described in the previous DPIA on the expansion. | No |
| 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 are 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? | No, not on the specific question of use of mobile enforcement cameras. | No |
| Who will undertake the consultation? | n/a | No |

| | | |
|---|---|---|
| What views have been expressed by stakeholders? | n/a | No |

## Step 6: Identify and assess risks (see also Step 7)

| **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**<br>**(Remote = Less than 10%,**<br>**Possible = 10-50%;**<br>**Probable = Over 50%)** | **Severity of harm**<br>**(Minimal, significant or severe)** | **Overall risk**<br>**(Low, medium or high)** | **Is this risk included in project or other risk register?** |
|---|---|---|---|---|
| **Proportionate processing and data minimisation:**<br>**Excessive or irrelevant data collection – for example parked vehicles, private residences, pedestrians/bystanders - meaning that there is a risk of i) PCNs are incorrectly issued and/or ii) vehicle images included within a PCN include personal data relating to third parties** | Possible | Significant | Medium | Yes |
| ***Proportionate processing (corporate risk:)***<br>**Public/ political concerns about the potential for police access (specifically) to the data collected by mobile enforcement** | Possible | Significant | Medium | Yes |

| | | | | |
|---|---|---|---|---|
| **vehicles - leading to legal challenge** | | | | |
| ***Data accuracy:***<br>**The accuracy of the cameras installed on the Mobile Enforcement Vehicles is not sufficiently robust, meaning that a VRM is incorrectly read and PCNs are incorrectly issued.** | Possible | Significant (distress) | Medium | Yes |
| ***Fair processing:***<br>**Risk of challenge that the Mobile Enforcement Vehicles are located/sited in such as way at the roadside that it could be considered 'covert'** | Possible | Significant (corporate risk relating to transparency and fair processing) | Medium | Yes |
| ***Fair processing:***<br>**Risk of challenge that the Mobile Enforcement Vehicles do not have adequate signage/branding that sufficiently indicates the purpose of their use, details of the operating organisation or contact details.** | Possible | Significant (corporate risk relating to transparency and fair processing) | Medium | Yes |

## 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:**<br>**Excessive or irrelevant data collection – for example parked vehicles, private residences, pedestrians/bystanders - meaning that there is a risk of i) PCNs are incorrectly issued and/or ii) vehicle images included within a PCN include personal data relating to third parties** | Carefully site the Mobile Enforcement Vehicles cameras in locations which maximise opportunity to achieve scheme benefits and avoid intrusion into the boundaries of private property or individuals. The focus of the camera must always be directed at the roadside.<br>Part of the camera set up is to check the field of view, the operators will be trained and checked to ensure they stick to the process Parked vehicles will not 'trigger' the cameras, and so those VRMs will not be captured. | Reduced | Low | Yes | RUC Operations / PPD implementation team |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| ***Proportionate processing (corporate risk):***<br>**Public/political/legal challenge that the use of Mobile Enforcement Vehicles is disproportionate, intrusive and therefore excessive for the intended purpose** | Conducting (and publishing) this DPIA; Regular review of the use of mobile enforcement vehicles to ensure minimum possible used for purpose and only in locations where their use is necessary for ULEZ compliance purposes<br>Transparency about rationale for camera deployment and use and benefits realisation | Reduced | Low | Yes | RUC Operations / PPD implementation team |
| ***Data accuracy:***<br>**The accuracy of the cameras installed on the Mobile Enforcement Vehicles is not sufficiently robust, meaning that a VRM is incorrectly read and PCNs are incorrectly issued.** | Levels of manual validation are 100% to ensure VRM matches against correct make, model and colour of vehicle before any PCN is issued.<br>The mobile enforcement cameras will also be subject to volume testing prior to go live to ensure the accuracy rates are as | Reduced | Low | Yes | RUC Ops |

| | | | | | |
|---|---|---|---|---|---|
| | expected and the cameras can cope with the volumes of data flowing through them | | | | |
| ***Fair processing:***<br>**Risk of challenge that the Mobile Enforcement Vehicles are located/sited in such as way at the roadside that it could be considered 'covert'** | The vans have clear signage on the sides and rear. The signage consists of a TfL, roundel along with Transport for London, a picture of camera and with ANPR cameras in operation. A TfL web address is also included.<br>The mobile enforcement vehicles can only be parked in areas where parking is permitted generally so there is no possibility of a vehicle being parked in such a way that it is obscured or hidden. | Reduced | Low | | RUC Operations / PPD implementation team |

| | | | | | |
|---|---|---|---|---|---|
| ***Fair processing:***<br>**Risk of challenge that the Mobile Enforcement Vehicles do not have adequate signage/branding that sufficiently indicates the purpose of their use, details of the operating organisation or contact details.** | As above | | | | |

| | **To be completed by Privacy & Data Protection team** | Could there be a privacy risk? |
|---|---|---|
| What is the lawful basis for processing?<br>Are there any Special Category or sensitive data? | The lawful basis for processing in this case is Article 6 (1) (e) of the GDPR –<br>"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."<br>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. | No |
| Are changes to Privacy Notice required? | Some amendments have already been made to the privacy notice to take account of the use of Mobile Enforcement Vehicles. The content will be revisited to ensure it remains update to date. However, there will be no other fundamental changes to current processing that will necessitate an update. | No |
| 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. | 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.<br>Safeguards on international transfers are achieved in different ways:<br>- via DVLA requirements in respect of data sourced from their databases<br>- through tender requirements issued by TfL to suppliers | No |

| | | |
|---|---|---|
| | - through data processor contractual clauses<br>- through appropriate due diligence and audits of suppliers<br>- Most camera testing will take place within EEA countries which currently have an Adequacy finding from the UK Government.<br>Other camera or systems testing that may be required for the expansion could include remote access to data from offshore locations, which comprise Argentina, India and Israel. These countries (with the exception of India) currently have an Adequacy finding from the UK Government.<br>In respect of any processing that takes place from India, this has been subject to an International Data Transfer Assessment as well as the inclusion of the appropriate contractual clauses. | |
| 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.<br>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? | There is no intention to share the mobile enforcement cameras with any third parties, including the MPS. (The current Mayoral Delegation relating to the sharing of the fixed, on-street infrastructure, can be found online: MD2977 Delegation to TfL to grant ANPRC data access to MPS.) | No |

| | | |
|---|---|---|
| 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.<br>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.  This check also helps to reduce the risk of a PCN being issued to vehicle that has had its VRM cloned. | No |

| Step 8: Sign off and record outcomes | | |
|---|---|---|
| **Item** | **Name/date** | **Notes** |
| Measures approved by Privacy Team: | Privacy Team Leader / August 2023 | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by Privacy Team: | Privacy Team Leader / August 2023 | If accepting any residual high risk, consult the ICO before going ahead. |
| Privacy & Data Protection team advice provided: | Privacy Team Leader / August 2023 | Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed. |
| Comments/recommendations from Privacy and Data Protection Team: | This DPIA to be published alongside the existing DPIAs for the expansion of the ULEZ<br>Consideration to be given as to whether any further updates should be made to the privacy notice – to expand on the existing content regarding the use of mobile enforcement vehicles. | |
| DPO Comments: | The data minimisation aspects of the operation of the mobile cameras should be reflected in a further update to the privacy notice. | |
| 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 Head of Operational Delivery | 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.<br>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.<br>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.<br>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.<br>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.<br>Data minimisation must be considered at every stage of the information lifecycle:<br>• when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary;<br>• when deciding what information to record, you must consider what information is required, what is relevant and whether any information is excessive;<br>• 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.<br>Disclosing too much information about an individual may be a personal data breach.<br>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:<br>• The right to be informed;<br>• The right of access;<br>• The right to rectification;<br>• The right to erasure;<br>• The right to restrict processing;<br>• The right to data portability;<br>• The right to object;<br>• 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*."<br>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”.<br>This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations.<br>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.<br>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).<br>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.<br>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.<br>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.<br>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.<br>TfL adopts a layered approach to privacy notices, with clear links to further information about:<br>• Whether the information will be transferred overseas;<br>• How long we intend to keep their personal information:<br>• The names of any other organisations we will share their personal information with;<br>• The consequences of not providing their personal information;<br>• The name and contact details of the Data Protection Officer; |

| | |
|---|---|
| | • The lawful basis of the processing;<br>• Their rights in respect of the processing;<br>• Their right to complain to the Information Commissioner;<br>• 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:<br>‘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.<br>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.<br>The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes.<br>Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability.<br>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:<br>• financial circumstances;<br>• health;<br>• safety;<br>• reputation;<br>• employment opportunities;<br>• behaviour; or<br>• choices |
| **Special Category data** | Special category data consists of information about identifiable individuals':<br>• racial or ethnic origin;<br>• political opinions;<br>• religious or philosophical beliefs;<br>• trade union membership;<br>• genetic data;<br>• biometric data (for the purpose of uniquely identifying an individual);<br>• data concerning health; or<br>• data concerning a person’s sex life or sexual orientation.<br>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.<br><br>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:<br>• Traffic signs<br>• Traffic control systems<br>• Road safety |

| | |
|---|---|
| | • Traffic reduction<br>We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs).<br>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.<br>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:<br>• Occurring according to a system<br>• Pre-arranged, organised or methodical<br>• Taking place as part of a general plan for data collection<br>• Carried out as part of a strategy<br>Examples of activities that may constitute a regular and systematic monitoring of data subjects include:<br>• operating a telecommunications network;<br>• providing telecommunications services;<br>• email retargeting;<br>• data-driven marketing activities;<br>• 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);<br>• location tracking, for example, by mobile apps;<br>• loyalty programs; behavioural advertising;<br>• monitoring of wellness,<br>• fitness and health data via wearable devices;<br>• closed circuit television;<br>• 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. |