

# TfL Management System

F7526 A3

## Data Protection Impact Assessment (DPIA) Checklist

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

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

Your details			
Name:	██████████ ██████████████████ ██████████	Date DPIA completed	15/12/2019 Continuous review to 08/09/2023
Job title:	Project Manager Product Manager Change Design Manager	Proposed launch date	23/12/2019

Printed copies of this document are uncontrolled



Name and description of the project:	Body Worn Video – Pan TfL Deployment				
Personal Information Custodian (PIC)	████████████████████ ████████████████████ ████████████████████	Is PIC aware of this DPIA?	Y	Project Sponsor	████████████████████ ████████████████████

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

Use <a href="#">profiling</a> or <a href="#">automated decision-making</a> to make decisions that will have a significant effect on people. <a href="#">Significant effects</a> can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits.		Process <a href="#">special category data</a> (relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; <a href="#">genetic</a> or <a href="#">biometric</a> 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' <a href="#">personal data</a> , or keeping personal data for longer than the agreed period.	
Use data concerning children or <a href="#">vulnerable</a> people. A person with vulnerability is usually described as someone who is at a higher risk of harm than others.	X	Process <a href="#">personal data</a> which could result in a risk of physical harm or psychological distress in the event of a <a href="#">data breach</a> .	X	Process children's <a href="#">personal data</a> for <a href="#">profiling</a> or <a href="#">automated decision-making</a> or for <a href="#">marketing</a> purposes, or offer online services directly to them.	
<a href="#">Systematically monitor</a> a publicly accessible place on a large scale – e.g. through the use of CCTV or Wi-Fi tracking.	X	Process <a href="#">personal data</a> in a way which involves tracking individuals' online or offline location or behaviour.		Match, compare or combine datasets, or have the potential to deny anonymity or re-identify people.	
Use new technologies or make novel use of existing technologies.		Process <a href="#">personal data</a> on a large scale or as part of a major project.		Process <a href="#">personal data</a> without providing a <a href="#">privacy notice</a> directly to the individual.	X

Use <a href="#">personal data</a> in a way likely to result in objections from the individuals concerned.	X	Apply evaluation or scoring to <a href="#">personal data</a> , or <a href="#">profile</a> individuals on a large scale.	Use innovative technological or organisational solutions.
Process <a href="#">biometric</a> or <a href="#">genetic</a> data in a new way.		Undertake <a href="#">systematic</a> monitoring of individuals.	Prevent individuals from exercising a right or using a service or contract.

Step 1 – Identify the need for a DPIA	
<p>Explain broadly what your project aims to achieve and what type of data and <a href="#">processing</a> it involves.</p> <p>You may find it helpful to refer or link to other documents, such as a project proposal.</p>	<p>The Body Worn Video Camera project forms part of the wider Operational Workplace Violence Programme. The project will roll out bodyworn cameras which capture video images and audio of incidents where our Operational Staff and Contractors feel at risk as a result of actions of either TfL customers and / or members of the public, require evidence of unlawful activity to support a prosecution, or consider the use of BWV will help to safeguard a vulnerable person during an interaction. This includes verbal abuse or threat, physical abuse or Hate Crime. The data captured will be transferred from the device to a secure AWS cloud provided by a third party (this has been reviewed and approved for use by TfL Cyber Security). The footage will be retained for 365 days and then automatically deleted, although it may be exported as evidence for a prosecution and held elsewhere for a longer period in connection with this purpose.</p> <p>The footage will only be shared once approval has been provided by the Data Disclosure Unit and only to authorised personnel internal and external to TfL. This will be the MET Police, BTP, CCTV Data Manager, TfL Investigation, Appeal and Prosecution team (for TfL private prosecutions of offenders), members of the Data Disclosure Unit and on a permission only basis subject to the JAPAN principles by TfL Senior management for the purposes of Safety investigations or in all circumstances for CPOS staff where a physical intervention with a member of the public is required in line with TfL Policy on physical interventions. In addition, footage may be shared for the purposes of Taxi Private Hire licencing decisions (that may include suspension / revocation of a licence and subsequent court proceedings) if the staff member is assaulted (verbal or physical) by a TfL Licenced driver whilst carry out their inspection duties.</p> <p>This DPIA focusses on the main roll out of the Body worn cameras incorporating the Stratford tech test of the technology, Interims stations roll out at Kings Cross, Walthamstow, Tottenham Hale, Victoria, Hammersmith Bus stations and CPOS and wider roll out of cameras to all front line Stations and EC roles in LU, station staff within London Buses, and all front line</p>

roles in CPOS. Northern line extension, Woolwich Ferry, River Services, LUCC, Dial A Ride, Engineering, Public Transport Service Planning, Commercial Development and Property Management, Investment Delivery Planning and LU Stations hosting Elizabeth Line Stations are all now users.

Contractors installing ULEZ cameras were offered BWV on 08/09/2023 following reported incidents of work place violence and aggression whilst on site delivering the ULEZ cameras. (See Appendix A for further details)

Training cameras: In April 2021, BWVC Phase 2 project was started to roll out more cameras to additional users across Pan-TfL users. Apart from the roll out of cameras, the project also had requirements to enhance current BWVC system and Business processes. Providing cameras for TfL Training teams was one of the Phase 2 requirements. Currently training teams do not have dedicated cameras to train new joiners. So, they must rely on experienced staff to train new users on the job. T&D recommended a dedicated training environment for this requirement after analysing various options. Operations of training cameras in training environment will be similar to how LIVE cameras are operated in LIVE environment. In addition, the officers will also have an ability to view the footage of recordings in the training environment. This feature of viewing footage is not available for officers in the LIVE environment. Its only the DDU team who has the privilege in LIVE environment. TfL trainers strongly felt that the inability to know what's recorded is one of the main deterrent for officers to take out cameras. Adding this feature to training environment to view the recorded footage during training was requested as an important step to encourage usage of cameras.

A condensed training session is being offered to ULEZ camera contractors on 08/09/2023 covering:

- do a brief demo,
- share the process should an incident occur (the tagging template and email address)
- share a one-pager on how to use the Camera,
- provide a Card that enables the de-docking of the Camera and
- associated accessories.

<p>Summarise why you identified the need for a DPIA</p>	<p>It was identified that a DPIA was required due to the nature of the data being captured and the need for TfL to adhere to national Data Protection and GDPR legislation, as outlined by TfL's Information Governance team</p>
---------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Step 2: Describe the nature of the [processing](#)

<p>How will you collect, use, and delete data? What is the source of the data?</p>	<p>BWVC will only be used to capture incidents (video images and audio) where TfL staff (and contractors) feel threatened or at risk whilst carrying out their designated roles by TfL Customers and / or members of the public, Taxi Private Hire drivers and operators or commercial vehicle operators when the vehicle is entering a TfL premises and may be subject to vehicle safety checks , dealing with vulnerable members of the public and enforcement of by-laws by CPOS staff. This includes verbal abuse or threat, physical abuse or Hate Crime. The footage from the BWVC will be uploaded to the Video Manager. The Video Manager will store the following information:</p> <ul style="list-style-type: none"><li>- Employee data*<ul style="list-style-type: none"><li>○ User ID</li><li>○ SAP Employee No.</li><li>○ First Name</li><li>○ Family Name</li><li>○ RFID code of staff oyster card</li><li>○ Assigned camera ID</li><li>○ Date time assigned</li><li>○ CPOS Badge ID</li></ul></li><li>- Incident/Footage Data<ul style="list-style-type: none"><li>○ Date and Time</li><li>○ Unique Reference of the footage</li><li>○ Video</li><li>○ Sound</li><li>○ Camera ID</li><li>○ Video Quality</li><li>○ User ID taking recording</li><li>○ Doc Controller Location</li><li>○ Evidence Type</li></ul></li></ul>
----------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

If Workplace Violence & Aggression

- Verbal
- Physical
- Hate Crime

If Crime Prevention & Detection

- Violence
- Robbery
- Theft
- Drugs
- Criminal damage
- Sexual offences
- Other Crime Type – Please Detail

If Safeguarding

- Dealing with/supporting child
- Dealing with/supporting vulnerable adult
- Dealing with/supporting intoxicated person

If Byelaws

- Byelaws

- Hate Crime
- Crime Reference Number
- GPS Location of where video was recorded (Subject to signed off testing, approval and training material)
- Audit log of footage viewed
- Incident Status
- Subject Access Request reference
- 60 second pre-record buffer data - the camera will be continuously recording and overwriting, the buffer data is only permanently saved after manual activation.

On limited occasions it may be necessary for HR issues relating to a specific incident that data may be required for the purposes of safety fact finding. It will not be accessed without reference to a specific incident or otherwise used for “fishing expeditions” and only permitted if there is clear evidence that a video or data stored within the solution can validate or not validate a safety issue. Any request

for this data will be made via HR Services to CPOS. If this request is authorised as valid (in-line with existing TFL processes and procedures for management of staff), a copy of the relevant data will be supplied to the Investigating Manager.

In circumstances where CPOS staff have had cause for a physical intervention (in line with TfL Policy) with a member of the public / TfL customer, footage will be viewed by a Senior Manager for the purposes of safety review and ensuring the policy and training was adhered to. The findings may be used to improve training for CPOS staff.

On limited occasions where, during a routine inspection of a Taxi, Private hire driver, vehicle or operator, the BWC may be activated for personal safety reasons. This footage may be disclosed to Police or to the licencing authority for review of the licencing conditions that may involve civil action in relation to a licencing decision.

The Pan-TfL technical test and Rollout made some minor alterations to the arrangements described here, and will increase the usage of devices to include all on-duty staff who opt to use the devices.

Recording: No Change

Device Check in/out: Rather than manually checking in/out devices, an RFID reader will be used to register staff using their Staff Pass. This will record the device issued to each staff member and will link any recorded footage to the employee number

Transfer of footage: This will now take place at all LU and Bus Stations as well as TfLs Hub office at Palestra. There will no longer be a requirement to transport cameras and footage to Baker Street for this element of the process.

Upload of footage: Cameras will be docked in the way described above, with footage being uploaded to the AWS cloud environment owned by Edesix over the internet. This process will be protected by firewalls between TfL's network and the AWS interface and footage is encrypted end-to-end during the transfer process.

Ongoing back-office process: No change

Training cameras: Different from the LIVE cameras that are used in public places, training cameras will be used only in training rooms to record footage of trainers and trainees demonstrating the usage of cameras. The new training environment will enable the trainers to access the recorded footage and do a show & tell. The scope does not include usage of recorded footage for any other purposes except show & tell. E.g. Download, Link to incident, Export, sharing with 3rd parties etc., There will be no change to the design of how the data will be transferred securely to the back office video manager system. There will be a change in where the cameras will be located compared to LIVE cameras. Because the training cannot happen in the same room every time, it could happen in a general meeting room that's accessible to other TfL employees apart from the trainers. The trainers will own the management of setting up the kit before the training, disassembling them after the training and locking them in a secure location.

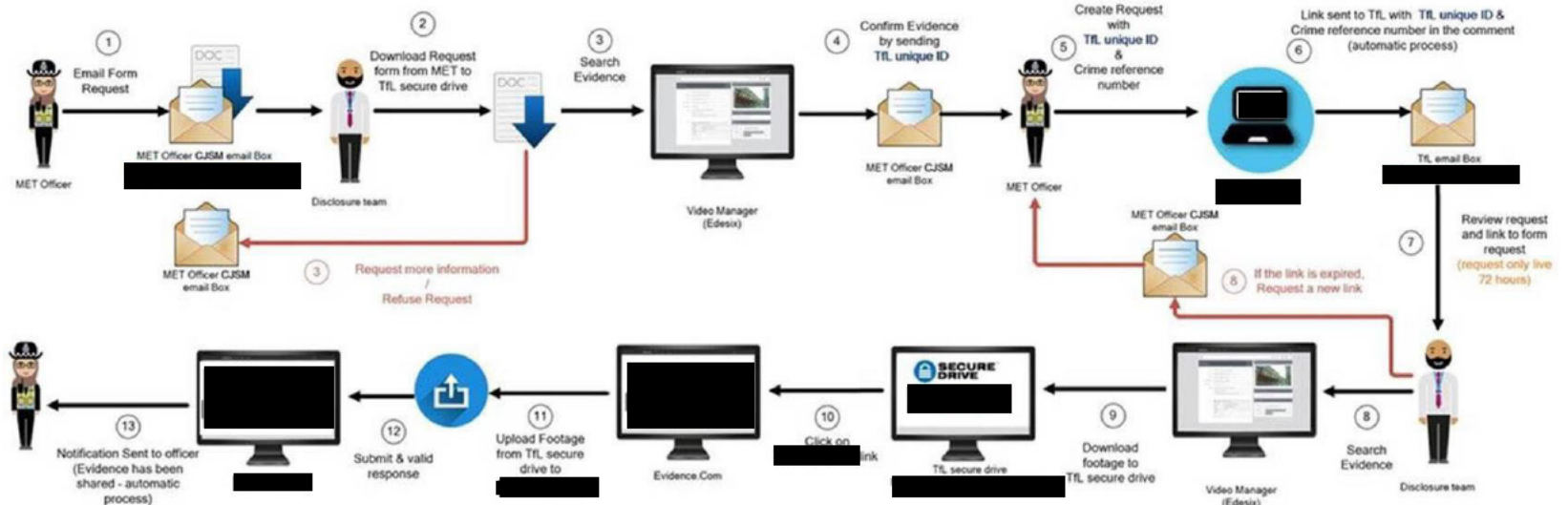


There will be no change to the security safeguards of the Video Manager system. i.e., A TSO process will be set up to maintain login accounts for new users. Leaver process will remain the same as LIVE environment. There will be no change to how footage will be uploaded to cloud There will be a change to retention policy in footages captured for training compared to the policy in place for LIVE footages. In LIVE, the retention configuration 365 days whereas in the training environment the configuration will be reduced to 7 days. At occasions trainers are required to take training cameras to another training room in a different TfL office to do basic operations demonstration. During such occasions, trainers require more time to dock in those cameras, upload footage and then to organize meetings for the show & tell. Due to this reason the retention configuration for the footage has been kept at 7 days than the same day. A new "Trainer" role will be created in the backend Video Manager system so the user control does not risk the LIVE system user roles.

Will you be sharing data with anyone?

Data will only be disclosed externally to our Policing Partners as part of a criminal investigation by the Data Disclosure Unit, and by the CCTV Data Manager for purpose of SAR requests made by or on behalf of Data Subjects. A member of the public can make a subject access request for the data, this will be processed as per the technology test SAR process.

TfL Cyber Security have approved the processes for sharing data with the Met Police and the BTP



	<p>The diagram illustrates a 12-step process for handling a request for footage:</p> <ol style="list-style-type: none"> <li><b>Request Footage</b> (1): BTP Officer initiates the request.</li> <li><b>Send request Footage (automatic process)</b> (2): Request is sent to TFL email Box.</li> <li><b>Check Request</b> (3): Disclosure team reviews the request.</li> <li><b>Connect to &amp; Select request</b> (4): Disclosure team connects to the system and selects the request.</li> <li><b>Download BTP form from [redacted] to TFL secure drive</b> (5): BTP form is downloaded to the secure drive.</li> <li><b>Search Evidence</b> (6): Evidence is searched. A red arrow labeled "Request more information/Refuse Request" loops back to step 1.</li> <li><b>Download footage to TFL secure drive</b> (7): Footage is downloaded to the secure drive.</li> <li><b>Connect to &amp; Select request</b> (8): System is connected and request is selected.</li> <li><b>Upload Footage from Tfl secure drive to [redacted]</b> (9): Footage is uploaded to the system.</li> <li><b>Save [redacted] Request to Tfl secure drive</b> (10): Request is saved to the secure drive.</li> <li><b>Submit &amp; valid response</b> (11): Response is submitted.</li> <li><b>Notification Sent to officer (Evidence has been shared - automatic process)</b> (12): Officer is notified.</li> </ol>
<p>Are you working with external partners or suppliers?</p>	<p>Edesix will provide the BWVC and the Cloud Hosted solution for the storage of the data. Edesix meet Home Office supplier standards.</p>
<p>Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)</p>	<p>A contract is in place with Edesix</p>

<p>Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?</p>	<p>Yes, data will be combined with electronic ticketing information, station/on bus CCTV in DDU process. In addition to Driver licensing details where the offence involves a TfL Licensed taxi or Private hire driver / operator</p>
<p>How and where will the data be stored?</p>	<p>The Data will be stored in Amazon Web Services Cloud Hosted solution provided by Edesix. The data storage is located in Belfast. TfL standard security requirements for technology have been applied and has been agreed by the TfL Cyber Security team as being secure for the purpose of the Technology Test. The Solution Architecture has been reviewed and approved by T&amp;D Architecture Review Board to ensure compliance</p>
<p>Will any data be processed overseas?</p>	<p>The data will not be processed outside the UK.</p>
<p>You might find it useful to refer to a flow diagram or other way of describing data flows.</p>	

<p><b>Step 3: Describe the scope of the processing</b></p>	
<p>Who does the data relate to?</p>	<p>Data relates to TfL Staff, TfL Customers, licenced taxi and Private hire drivers and operators and members of the public.</p>

<p>How many individuals are affected?</p>	<p>There will be circa 4500 devices rolled out to TfL Staff Members during rollout. The number of TfL Customer and / or members of the public cannot be quantified due to the unknown volume of future incidents that may be captured as part of the devices use on TfL's front lines.</p>
<p>Does it involve children or <a href="#">vulnerable</a> groups?</p>	<p>It is possible a child / young person / member of a vulnerable group could be captured on the BWVC either because of committing a potential offence against a staff member or passing an incident at the time a BWVC is in use (verbal or physical assault). Following feedback from users in the technology test it was established that a camera was activated when a child was abusive and hit a TfL employee. Cameras were also used when dealing with sleeping intoxicated passengers, to retain evidence when a vulnerable person fell and while assisting a sight impaired person to find and board a bus.</p>
<p>If children's data is collected and used, are they aged under 13</p>	<p>It is possible the recording could involve a child could be aged under 13, whether with an adult who is the subject of the recording or as the subject themselves. Interactions with unaccompanied children may also be recorded and tagged for safeguarding reasons.</p> <p>The circumstances and frequency that children are recorded on the cameras was reviewed during the trial. 1 instance was identified by camera users (described above).</p>
<p>What is the nature of the data? (Specify data fields if possible; For example, name, address, telephone number, device ID, location, journey history, etc.)</p>	<ul style="list-style-type: none"> <li>- Audio and video recordings.</li> </ul>

<p>Specify which <a href="#">special category data</a> or criminal offence data are to be processed?</p>	<p>The footage will be categorised as ‘Confidential’ under TfL’s <a href="#">Information Security Classification Standards</a> and the associated handling rules will apply.</p> <p>Requests from the police or other statutory law enforcement agencies for visual/audio recordings to assist the prevention or detection of crime will be subject to existing data sharing agreements between TfL and the Met Police. Footage may also be used by TFL Investigation Appeals and Prosecutions team for civil action against member of the public where Police take no action or there is a section 4 or 5 public order offence</p>
<p>Can the objectives be achieved with less <a href="#">personal data</a>, or by using <a href="#">anonymised</a> or <a href="#">pseudonymised data</a>?</p>	<p>The camera will only be activated where there is a clear reason to record footage. Due to the nature of the BWVC it is not possible to achieve the Project and System objectives with less data.</p> <p>Only a very small proportion (&lt;1%) of footage is currently tagged, but this is expected to increase with the rollout of the safeguarding and bylaws tagging categories.</p>
<p>How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?</p>	<p>Data will be stored initially for 365 days from the date that footage is recorded.</p> <p>Footage tagged as subject access request will be retained for 2 years from the date that the subject access request has been fulfilled.</p>
<p>Is the data limited to a specific location, group of individuals or geographical area?</p>	<p>Once footage has been captured and the request for retaining the footage due to a Crime Reference number being provided by our Policing Partners the footage will only be accessed by the following roles:</p> <ul style="list-style-type: none"> <li>• Crime and Anti-Social Behaviour Investigations Manager in Data Disclosures Unit</li> </ul>

**Step 4: Describe the context of the processing**

<p>Is there a <a href="#">statutory basis</a> or requirement for this activity?</p>	<p>See lawful basis of processing in Step 7.</p>
<p>What is the nature of TfL's relationship with the individuals? <i>(For example, the individual has an oyster card and an online contactless and oyster account.)</i></p>	<p>TfL's relationship with the individuals captured as part of the use of BWVC are as either customers of the Transport Network, (therefore they may have either an Oyster Card or Contactless Account), members of the public, Licensed Taxi / Private Hire drivers and operators and other TfL Staff Members.</p>
<p>How much control will individuals have over the use of their data?</p>	<p>Individuals captured on footage will be informed (where practical and safe to do so) that for safety purpose the camera user will audio and video record them at the time of the device being activated, in addition to this, posters about the use of body worn camera will be put up in stations with a link to TfL's Privacy and cookie page for further information about how TfL handles personal data and how to exercise their data subject rights. See more details in Step 7. Individuals are able to exercise their GDPR rights with guidance published on tfl.gov.uk and the web address given on posters.</p>
<p>Would they expect you to use their data in this way?</p>	<p>Yes. TfL are adopting the standard use of the BWVC devices and have used the national professional practice guidance from the College of Policing, BTP, MPS, Prison Service, ICO issued guidance to inform the use of BWVC.</p>
<p>Are there prior concerns over this type of <a href="#">processing</a> or security flaws?</p>	<p>There are no known concerns of this type of data processing or security flaws. However, use of mobile CCTV is considered as being particularly intrusive by the Information Commissioner's Office and there are campaign groups more generally concerned about surveillance and the use of CCTV in public spaces. The addition of audio recording may be considered as increasing the intrusive nature of body worn video devices. The justification for using audio recordings as well as visual recordings is to have clear evidence of any incident involving verbal communication. This may include evidence of a crime, such as threats or racial abuse, or other relevant information that may provide appropriate context to the recorded images.</p>

<p>Is it novel in any way, or are there examples of other organisations taking similar steps?</p>	<p>The use of body worn camera is also on the increase in the transportation industry. For example, following a pilot scheme, Virgin Trains has rolled out 275 cameras by February 2018, helping assaults on Virgin Trains staff to reduce each month, from 20 in March 2018 to six in September. Network Rail and British Transport Police are also users of this technology- Details of the PIAs and DPIAs carried out by several other public authorities are also publicly available via the internet and are likely to be a useful source of best practice and benchmarking.</p>
<p>What is the current state of technology in this area?</p>	<p>BWVC is not novel technology though its widescale use is new within TfL, and it is being used as standard in many transport organisations (Virgin, London North Western, TfL Rail, London Overground), Local Authorities for Parking Attendants and Supermarkets. The technology test will store and process data on the cloud and will also launch the GPS and Bluetooth functionality as future phases of BWC rollout.</p>
<p>Are there any security risks</p>	<p>There are no known security risks to technology being used by TfL and to ensure the BWVC devices and the Video Manager system meet TfL Security requirements as part of the Technology Test three Penetrations Tests were conducted, these are:</p> <ul style="list-style-type: none"> <li>- Penetration of the BWVC Device</li> <li>- Penetration of the Video Manager System</li> <li>- Penetration of GPS and Bluetooth functionalities</li> <li>- Playback, edit and download are strictly controlled and limited to a specific number of individuals, system access controls will set up so that only LU CCTV Data manager and Crime and Anti-Social Behaviour Investigations Manager in Data Disclosures Unit will be authorised to do so. It is not possible to view or playback footage within the camera itself; there is no removable media and no ability to plug in other devices such as USB sticks, so footage cannot be copied or shared.</li> </ul> <p>The processes for transfer of evidence to BTP and Metropolitan Police have been reviewed and agreed by TfL Cyber Security.</p>
<p>Are there any current issues of public concern that you should factor in?</p>	<p>In the past there have been concerns about the encryption of the cameras, storage of data on commercial clouds, the inclusion of Wi-Fi and Bluetooth capabilities in devices and poor technology (e.g. Failure to record, recording all the time even if not activated).</p> <p>Data will be stored and processed in the AWS cloud environment and TfL Cyber Security has assessed and given approval for the technology, There will be a support model for the duration of the Product Delivery and operation in and from Phase 1 utilizing project team and existing T&amp;D Processes.</p>



	<p>Users will be able to log calls via 1555 to our T&amp;D remedy solution and this will be then forwarded to project team resources to review and resolve including any engagement with 3<sup>rd</sup> party supplier or other T&amp;D Teams. This process is part of the training guidance provided and available on the training portal all users have been provided access to.</p> <p>Training cameras: After the roll out of BWVC in Phase 1, the usage of cameras had remained low. Though there were many reasons behind the low usage, one of the key reasons raised by the trainers was the inability for officers to see what's been recorded and how. Providing a set of dedicated cameras for training, dedicated training environment and an opportunity to view the footages will benefit the officers to gain more confidence of using the cameras. This could potentially help to improve the usage and thereby more safety to officers.</p>
<p>Are you or your delivery partner signed up to any code of conduct or certification scheme?</p>	<p>TfL complies with data protection code of practice for surveillance cameras and personal information and voluntarily adopts the surveillance camera code of practice issued by the Surveillance Camera Commissioner.</p> <p>Edesix solutions conform to Home Office standards for BWV equipment.</p>

Step 5: Describe the purposes of the processing	
<p>What do you want to achieve?</p>	<p>The BWVC Roll out aims to improve Staff Safety and outcomes from incidents of Work Place Violence with regards to staff morale, perceived safety and order on the network, compliance with laws and bylaws and rates of prosecution for aggression towards TfL's front line staff by the police and TfL's own internal prosecution's unit</p> <p>BWV supports frontline staff dealing with vulnerable people and protects vulnerable people themselves. Specific tags have been created to support:</p> <ul style="list-style-type: none"> <li>• <b>Dealing with/supporting child</b></li> <li>• <b>Dealing with/supporting vulnerable adult</b></li> <li>• <b>Dealing with/supporting intoxicated person</b></li> </ul>
<p>What is the intended effect on individuals?</p>	<p>The Technology is intended to serve as a deterrent to violence, aggression, hate crime and anti social behavior towards TfL staff on the part of Customers and members of the public, and provide reassurance to passengers on the TfL Transport network</p>

	<p>The focus of each recording will be the individual interacting with the staff member at the time. The cameras will not be used to capture images or conversations of the public going about their day-to-day business. Specific guidance will be provided to all users on this issue in the local procedure.</p>
<p>What are the benefits of the <a href="#">processing</a> – for TfL, for other external stakeholders, for the individuals concerned and for society in general?</p>	<p><b>Operational Benefits:</b></p> <ul style="list-style-type: none"> <li>• Use of body worn video is intended to improve the health &amp; safety of employees who undertake public facing roles across multiple locations.</li> <li>• The use of BWVC demonstrates TfL is serious about dealing with criminal and other antisocial behaviour and maintaining a safe transport network for all customers and employees.</li> <li>• Will support police and TfL private prosecutions for assault or other anti-social behavior across TfL network, and cases of By-Law prosecution / dispute</li> <li>• Will support investigations and complaints relating to interactions with vulnerable individuals (safeguarding).</li> </ul> <p><b>Benefits to TfL customers/employees:</b></p> <ul style="list-style-type: none"> <li>• Use of body worn video is intended to improve the health and safety of employees, and order on the network for customers.</li> <li>• A recording will provide a record of events that could support both customers and employees</li> <li>• Helps create and maintain a safer travel environment for customers</li> <li>• Could help improve the confidence and security of employees who may be working alone</li> <li>• May promote responsible behaviour and encourage considerate behaviour amongst users of TfL’s transport services</li> </ul>

**Step 6: Consultation process**

<p><b>Consider how to consult with relevant stakeholders:</b></p> <p>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.</p>	<p>TfL Senior Managers, Operational Managers and Trade Unions have been consulted during the initial phases of this project. Privacy and data protection, CPOS audit and compliance manager, CPOS data disclosure unit, LU CCTV data manager have also been consulted in body worn camera workshops. Views from all parties have been factored in to ensure no disagreements exist on the use and configuration of the BWVC device. Any changes will be discussed in the agreed stakeholder meetings and will result in this DPIA document being updated.</p> <p>BWV deployment has been discussed with representatives of the ICO and SCC.</p>
<p>Who else do you need to involve within TfL?</p>	<p>No further stakeholders within TfL are required at this time. Any changes to this position will result in this DPIA being updated.</p> <p>Training cameras: With regards to the requirements for training cameras, project team has consulted the following stakeholders · CPOS Business owner responsible for Phase 2 · Project sponsor · Cyber security analyst (T&amp;D) · Project forum senior stakeholders (LU, Bus Operations, Finance and Sponsorship)</p>
<p>Have you discussed information security requirements with TfL Cyber Security?</p>	<p>For developing the Solution Architecture, configuration of the BWVC Device, AWS Server and the VMS the following persons have been consulted with and / or significantly engaged with the project.</p> <ul style="list-style-type: none"> <li>• Cyber Security Lead</li> <li>• Solution Architects</li> <li>• Infrastructure Architects</li> <li>• Network Engineers</li> <li>• Commercial Manager</li> <li>• Commercial Assistant</li> <li>• LU Technology Improvement Lead</li> <li>• Product Manager</li> <li>• Senior Product Manager</li> <li>• Heads of T&amp;D (Surface &amp; LU)</li> </ul>

<p>Do you plan to consult with external stakeholders? If so, who?</p>	<p>For the BWVC Technology Test and main roll out, there were discussions with Policing Partners on their experiences on BWV and also notification of the fact that there will be BWC available via CPOS's police partnerships. Current processes using DVD to provide CCTV footage are being adopted in providing this video.</p> <p>The deployment was also discussed between the ICO and Privacy and Data Protection on 23 September 2020</p>
<p>Who will undertake the consultation?</p>	<p>The Unions will be informed about the compulsory issue of cameras and will be given opportunity to respond.</p>
<p>What views have been expressed by stakeholders?</p>	<p>Stakeholders engaged have expressed a number of views, the most relevant are captured below:</p> <ul style="list-style-type: none"> <li>• Security around the data captured</li> <li>• Access to the data captured needs to suitably controlled</li> <li>• Sharing of the data within TfL and external to TfL needs to be approved by the DDU in the first instance</li> <li>• Subject Access Requests are to be processed as per TfL's CCTV policy</li> </ul> <p>The primary focus of the BWVC is to promote the safety of Operational Staff and be provided in response to requests made by Operational Staff</p>

<p><b>Step 7: Assess necessity and proportionality</b></p>	
<p><b>Describe compliance and proportionality measures, in particular:</b></p> <p>Does the <a href="#">processing</a> actually achieve your purpose?</p>	<p>The processing achieves the purpose and there is no alternative way to achieve the same outcome. For Operational Staff based in either Underground or Bus Stations the option of Station, CCTV has been considered an alternative, however, it has limited coverage and there is no audio recording for incidents such as racist abuse and verbal abuse. Whilst for those Operational Staff who work away from stations as part of their designated tasks this is not an option and their current LoneWorker Device does not provide visual images and there are areas geographically where this technology does not work.</p>

<p>Is there another way to achieve the same outcome?</p>	<p>From the analysis completed it has been recommended and accepted that there is no other way to achieve the same outcome of providing sufficient visual and audio data to promote the safety of TfL Operational Staff through deterrence and ensure evidential quality data for pursuing and supporting criminal prosecutions.</p>
<p>How will you prevent <a href="#">function creep</a>?</p>	<p>The project will put in place clear controls of access for police, other TfL areas such as Taxi Private hire Licensing, Investigations, Appeals and Prosecution teams requests and Subject Access Requests. There will be no changes to configuration of the functionality of the devices and access control without agreement from the WVA Steering Group. Any changes to BWVC Device functionality will be documented and consulted on with stakeholders as required before being applied.</p>
<p>How will you ensure <a href="#">data quality</a> and data <a href="#">minimisation</a>?</p>	<p>Data quality and data minimization is covered in step 2</p>
<p>What information will you give individuals about how their data is used?</p>	<p>The ICO recommends that mobile CCTV devices should clearly indicate when they are in active use via a clearly visible flashing light. There will be a beeping sound and a front facing red light will be turned on when the camera is in active use, we also require that staff wear body worn camera in visible locations and each user verbally announce that 'For my safety I'm going to audio and video record you' where safe and practical on each occasion the camera is activated.. CCTV signage is in place in LU and Bus stations and on trains, Posters about the use of body worn cameras will be put up near station entrances and inside stations, TfL's CCTV &amp; surveillance cameras privacy page will also be updated</p> <p>If required, staff using a body worn camera must be prepared to explain how TfL is processing personal data captured by body worn cameras or direct the requester to TfL's CCTV &amp; surveillance cameras privacy webpage for more information. To enable this requirements for taking TfL's Data protection courses and briefings on the Data protection obligations on staff are included within the product's training materials. It has been decided that Subject Access / Deletion requesters should be directed to the website, because the specific circumstances in which BWV will be switched on are not conducive to asking the data subject for their name and address in order to fulfil the SAR or to respond to the deletion request.</p> <p>The project team needs to ensure that policy, processes and training are provided to staff at the same time as they are provided with the body worn cameras and that they are actively promoted.</p> <p>Contractors fitting ULEZ cameras are instructed to refer individuals to the TfL Website privacy pages for information</p>

	<p>about data subject rights.</p>
<p>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?</p>	<p>TfL has undertaken this DPIA Assessment of the current configuration and functionality to ensure that the solution processes personal data safely and lawfully. In addition TfL Cyber Security has engaged with the solution supplier to ensure that the solution delivered has the controls and security in place for the solution to ensure that the data is stored safely and securely.</p> <p>The contract which encompasses the technology solution and equipment in addition to the future extended use of the solution pan TfL and the additional equipment needed. This contact has specific obligations on the supplier regarding processing of data safely and securely.</p>
<p><b>To be completed by Privacy &amp; Data Protection team</b></p> <p>What is the lawful basis for processing?</p> <p>How will data subjects exercise their <a href="#">rights</a>?</p> <p>How do we safeguard any international transfers?</p> <p>Could data <a href="#">minimisation</a> or <a href="#">pseudonymisation</a> be applied?</p> <p>Are data sharing arrangements adequate?</p>	<p>The lawful basis for processing is that the information processed 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 (Article 6(1)(e) of the General Data Protection Regulation),</p> <p>The performance of a task carried out in the public interest or the official authority vested in TfL above includes:</p> <ul style="list-style-type: none"> <li>• The Mayor has a duty under section 141(1) of the Greater London Authority Act 1999 (GLA Act) to develop and implement policies for, ‘... <i>the promotion and encouragement of safe... transport facilities and services to, from and within Greater London</i>’ (the General Transport Duty). This duty has been delegated to TfL under section 154(3)(b) of the GLA Act.</li> <li>• TfL (including LUL) has a duty under section 17 of the Crime and Disorder Act 1998 to exercise their functions with due regard to the likely effect on, and the need to all that it reasonably can to prevent, crime and disorder in their respective areas.</li> </ul> <p>In respect of processing of any special category personal data and personal data relating to criminal convictions and offences, the lawful basis is that</p> <ul style="list-style-type: none"> <li>• the information processed is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and</li> </ul>

	<p>provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject (Article 9 (2)(g) of the General Data Protection Regulation).</p> <ul style="list-style-type: none"><li>• The information processed is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (Article 9(2)(f) of the General Data Protection Regulation)</li></ul> <p>The following conditions of Schedule 1, Part 2 of the Data Protection Act 2018 will apply where the information processed is:</p> <ul style="list-style-type: none"><li>• Necessary for the exercise of a function conferred on a person by an enactment or rule of law (Data Protection Act 2018, Schedule 1, Part 2, s 6 (1) and (2))</li><li>• Necessary for the purpose of the prevention or detection of an unlawful act (Data Protection Act 2018, Schedule 1, Part 2, s10(1) and (2))</li></ul> <p><b>Can TfL justify its interference with Article 8 Human Rights Act?</b></p> <p>i) the interference must be for a legitimate aim (see the lawful basis of processing above)</p> <p>ii) the interference is proportionate to support that legitimate aim:</p> <ul style="list-style-type: none"><li>• The use of body worn cameras will offer protection/reassurance for employees, citizens and the police</li><li>• The cameras will only be switched on in response to specific events. The cameras are continuously recording and overwriting, the 60 second pre-record buffer data will only be permanently saved after manual activation of the camera.</li><li>• The cameras will not be used to capture images or conversations of the general public going about their day-to-day business</li><li>• The use of body worn cameras is fully overt, devices are clearly marked as video/audio recording devices with a warning and camera icon. It's also made clear when the camera is in active use via a beeping sound, a front facing red light and the camera user's verbal announcement.</li><li>• There are clear retention/disposal rules and security measures for recorded footage</li><li>• The use of body worn cameras will follow guidance found in the <a href="#">ICO Code of Practice for CCTV</a> and the <a href="#">Surveillance Commissioners Code of Practice</a></li></ul> <p>iii) the interference is necessary in a democratic society:</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- Preventing and detecting crime, enforcing laws and maintaining public safety (including the safety of vulnerable persons) is an activity necessary to a democratic society.

How will data subjects exercise their rights? Individuals are provided with fair processing information as stated above. Information is published on the TfL website, which is displayed on CCTV posters and signage

Individuals can contact the LU CCTV Data Manager via TfL's Access your data webpage to exercise the right to access their personal data captured by LU CCTV cameras, a new section has been created for body worn camera footage captured by LU, CPOS and bus station staff. Individuals may also contact the Privacy and Data Protection team to submit SARs related to LU CCTV and the Privacy and Data Protection team will forward these SARs to the Data Disclosure Unit to process. This will be kept under review in the event that non LU SARs become the majority of requests

The LU CCTV Data Manager (for LU) and the Data Disclosure Unit (for non-LU) will manage SARs from start to finish, including maintaining a log for these SARs, disclosing the personal data to the individuals (via postal delivery or offering pick-up in person to the individuals) and reporting statistics to the Privacy and Data Protection team.

The body worn cameras include date/time stamps in each piece of footage, as well as linking it to the assigned user of the device. VideoManager allows simple search of footage using these parameters, so that body worn camera data can be organised, searched and retrieved. Long recordings may be split into more than one files, VideoManager automatically groups long recordings into multiple shorter clips, this is visually clear to the user and Video Manager enables users to collect and present the long recordings as a single recording.

Individuals can contact Privacy and Data Protection team to exercise the right to erasure. Privacy and Data Protection team will liaise with the designated staff who manages Video Manager who will carry out a search on the Video Manager system to locate the relevant footage and the Privacy and Data Protection will provide a bespoke response to the individual. Individuals can also contact the Privacy and Data Protection team to exercise their right of rectification, right to restriction of processing and right to object.

No international transfer of personal data is involved as the solution will consist of equipment used with London and the data storage will be located in AWS in Belfast. The Data Disclosure Unit will review each request received for footage from our Policing Partners and confirm if the footage will be disclosed.



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, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
Members of the public may have questions about the use of the cameras, and how to exercise their rights, that the camera operator is unable to answer at that time	Possible	Significant	Medium
Camera operators may be uncertain whether to record incidents where the primary concern is the safeguarding of the individual	Possible	Minimal	Low
There is a lack of clarity for camera operators about whether footage may be considered by HR investigating alleged misconduct. The footage may, in some scenarios, be obtained by a customer who	Probable	Minimal	Medium


makes a SAR and then submits the footage in support of a complaint			
There is no data to assess the likelihood that children aged 13 or less will be recorded using BWV. This affects the efficacy of the DPIA	Probable	Minimal	Medium
Untrained users of equipment risk data breaches or ineffective recordings	Probable	Significant	Medium
Volume of Subject Access requests may affect ability to answer them on time	Remote	Medium	Medium

**Step 9: Identify measures to reduce risk**

<b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8</b>				
<b>Risk</b>	<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b> Eliminated, reduced or accepted	<b>Residual risk</b> Low, medium or high	<b>Measure approved</b> Yes/no
Members of the public may have questions about the use of the cameras, and how to exercise their rights, that the camera operator is unable to answer at that time	Effective training on Privacy, both using TfL e-learning and camera specific training	reduced	low	Training is agreed.
Camera operators may be uncertain whether to record incidents where the primary concern is the safeguarding of the individual themselves	Develop further guidance for recording incidents where the purpose is to safeguard the interests of the individual being recorded.	Accepted whilst in tech test phase. Reduced thereafter	low	Safeguarding planned for Spring rollout
There is a lack of clarity for camera operators about whether footage may be considered by HR investigating alleged misconduct. The footage may, in some scenarios, be obtained by a customer who makes a SAR and then submits the footage in support of a complaint, or cameras may be used to record interactions between TfL employees	Such instances might be considered on a case by case basis, in the same way that other CCTV footage would be considered. Access will be restricted by request to the DDU subject to JAPAN principles.	Accepted whilst in tech test phase. Reduced thereafter	low	
The DPIA stated that there was no contract in place with Edesix, who are	A contract has been drafted and the security of the cloud environment has	Resolved		Issue closed

responsible for the provision of the cameras, and are acting as a data processor through provision of the data cloud. This is in breach of the GDPR	been reviewed by TfL Cyber Security. The contact has been signed			
There is no data to assess the likelihood that children aged 13 or less will be recorded using BWV. This affects the efficacy of the DPIA	Schedule interviews with users during the tech test to establish whether specific training or privacy information is required regarding children – Survey carried out in Autumn	Accepted whilst in tech test phase. Resolved thereafter		
Untrained users of equipment risk data breaches or ineffective recordings	Project board to receive report on training records	Resolved		
Volume of Subject Access requests may affect ability to answer them on time	DDU to advise Privacy team when first requests are received	Reduced	Low	

Step 10: Sign off and record outcomes		
Item	Name/date	Notes
Measures approved by Privacy Team:	██████ 22/07/2020 Latest review 20/06/2023	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	██████ 20/06/2023	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:		Privacy & Data Protection team should advise on compliance, Step 9 measures and whether processing can proceed.

Comments/recommendations from Privacy and Data Protection Team:	Any consideration of use of BWV outside this DPIA must be discussed with the TfL Privacy team and if necessary this DPIA should be updated.	
DPO Comments:		
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):		If overruled, you must explain your reasons below.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will kept under review by:		The DPO may also review ongoing compliance with DPIA.

Glossary of terms

<b>Anonymised data</b>	<p>Anonymised data is information held in a form that does not identify and cannot be attributed to individuals.</p> <p>Anonymous information is not subject to the GDPR, and, where possible and appropriate, should be used in place of identifiable or <a href="#">pseudonymised</a> personal data, particularly where sharing information with third parties or contemplating publication of data.</p> <p>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.</p>
------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	If information can be linked to an identifiable individual the data is not anonymous and you must treat it as personal data.
<b>Automated Decision Making</b>	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.
<b>Biometric data</b>	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 identifying individuals.
<b>Data breaches</b>	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 <a href="mailto:DPO@tfl.gov.uk">DPO@tfl.gov.uk</a> .
<b>Data minimisation</b>	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: <ul style="list-style-type: none"> <li>• when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary;</li> <li>• when deciding what information to record, you must consider what information is required, what is relevant and whether any information is excessive;</li> <li>• 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.</li> </ul> Disclosing too much information about an individual may be a personal data <a href="#">breach</a> .  When deciding how long to keep information, you must consider what records you will need, and whether some personal data can be deleted or <a href="#">anonymised</a> .
<b>Data Protection Rights</b>	The GDPR provides the following <a href="#">rights for individuals</a> : <ul style="list-style-type: none"> <li>• The right to be informed;</li> <li>• The right of access;</li> </ul>

	<ul style="list-style-type: none"> <li>• The right to rectification;</li> <li>• The right to erasure;</li> <li>• The right to restrict <a href="#">processing</a>;</li> <li>• The right to data portability;</li> <li>• The right to object;</li> <li>• Rights in relation to <a href="#">automated decision making</a> and <a href="#">profiling</a>.</li> </ul>
<b>Data quality</b>	<p>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."</p> <p>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.</p>
<b>Function creep</b>	<p>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.</p>
<b>Genetic data</b>	<p>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.</p>
<b>Marketing</b>	<p>Direct marketing is "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".</p> <p>This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations.</p> <p>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 <a href="#">privacy regulations</a> apply.</p> <p>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).</p> <p>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 <a href="#">privacy regulations</a> apply.</p>
<b>Personal data</b>	<p>Personal data is information, in any format, which relates to an identifiable living individual.</p>

	<p>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.</p> <p>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.</p> <p>The definition can also include <a href="#">pseudonymised</a> 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.</p>
<p><b>Privacy notice</b></p>	<p>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.</p> <p>TfL adopts a layered approach to privacy notices, with clear links to further information about:</p> <ul style="list-style-type: none"> <li>• Whether the information will be transferred overseas;</li> <li>• How long we intend to keep their personal information;</li> <li>• The names of any other organisations we will share their personal information with;</li> <li>• The consequences of not providing their personal information;</li> <li>• The name and contact details of the Data Protection Officer;</li> <li>• The lawful basis of the processing;</li> <li>• Their <a href="#">rights</a> in respect of the processing;</li> <li>• Their right to complain to the Information Commissioner;</li> <li>• The details of the existence of <a href="#">automated decision-making</a>, including <a href="#">profiling</a> (if applicable).</li> </ul>
<p><b>Processing</b></p>	<p>Doing almost anything with personal data. The GDPR provides the following definition:</p> <p>‘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</p>



<b>Profiling</b>	<p>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.</p>
<b>Pseudonymised data</b>	<p>Pseudonymisation separates data held about an individual from information that identifies the individual. This can be achieved by encrypting (hashing) the individual’s name, MAC address or ID code, masking an individual’s exact location or changing an image to make an individual unrecognisable.</p> <p>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.</p> <p>The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes.</p> <p>Pseudonymised data (if irreversible) is not subject to the individual’s rights of rectification, erasure, access or portability.</p> <p>Pseudonymisation is an important security measure and must be considered as part of Privacy by Design and Default approach. If you use pseudonymised data you must ensure that an individual can not be re-identified with reasonable effort. The risk of re-identification is higher when information about the same individual is combined. For example, whilst a post code, a person’s gender or a person’s date of birth would be very unlikely to identify an individual if considered without other reference data, the combination of these three pieces of information would be likely to enable a motivated individual to re-identify a specific individual in most circumstances.</p> <p>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.</p>
<b>Significant effects</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• financial circumstances;</li> <li>• health;</li> <li>• safety;</li> <li>• reputation;</li> <li>• employment opportunities;</li> <li>• behaviour; or</li> </ul>

	<ul style="list-style-type: none"> <li>• choices</li> </ul>
<p><b>Special Category data</b></p>	<p>Special category data consists of information about identifiable individuals':</p> <ul style="list-style-type: none"> <li>• racial or ethnic origin;</li> <li>• political opinions;</li> <li>• religious or philosophical beliefs;</li> <li>• trade union membership;</li> <li>• genetic data;</li> <li>• <a href="#">biometric</a> data (for the purpose of uniquely identifying an individual);</li> <li>• data concerning health; or</li> <li>• data concerning a person's sex life or sexual orientation.</li> </ul> <p>Information about criminal convictions and offences are given similar protections to special category data under the <a href="#">Law Enforcement Directive</a>.</p>
<p><b>Statutory basis for processing</b></p>	<p>TfL is a statutory body created by the <a href="#">Greater London Authority (GLA) Act</a> 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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Traffic signs</li> <li>• Traffic control systems</li> <li>• Road safety</li> <li>• Traffic reduction</li> </ul> <p>We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs).</p>

	<p>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 11 of the Act.</p> <p>Activities may have a statutory basis related to other legislation, for instance the requirements to publish information under the Local Government Transparency Code.</p>
<p><b>Systematic processing or monitoring</b></p>	<p>Systematic processing should be interpreted as meaning one or more of the following:</p> <ul style="list-style-type: none"> <li>• Occurring according to a system</li> <li>• Pre-arranged, organised or methodical</li> <li>• Taking place as part of a general plan for data collection</li> <li>• Carried out as part of a strategy</li> </ul> <p>Examples of activities that may constitute a regular and systematic monitoring of data subjects include:</p> <ul style="list-style-type: none"> <li>• operating a telecommunications network;</li> <li>• providing telecommunications services;</li> <li>• email retargeting;</li> <li>• data-driven <a href="#">marketing</a> activities;</li> <li>• <a href="#">profiling</a> and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering);</li> <li>• location tracking, for example, by mobile apps;</li> <li>• loyalty programs; behavioural advertising;</li> <li>• monitoring of wellness,</li> <li>• fitness and health data via wearable devices;</li> <li>• closed circuit television;</li> <li>• connected devices e.g. smart meters, smart cars, home automation, etc.</li> </ul>
<p><b>Vulnerable people</b></p>	<p>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.</p>

## Appendix A – Plan for issue of BWV to [REDACTED] Engineers

### Why are we doing this?

Urgently need to address that the ULEZ camera installation supplier, [REDACTED], has reported incidents of work place violence and aggression whilst on site delivering the cameras.

### What is our solution?

TfL will provide [REDACTED] with 25 Body Worn Video Cameras with clips and a USB dock.

### How are we enabling this?

#### Process

1. [REDACTED] have been asked to pick up the Cameras from [REDACTED]. The Cameras will be available from Friday 8 September.
2. Upon their arrival at [REDACTED] (all hours), [REDACTED] need to let reception know they are meeting with the [REDACTED]. The TSO team at [REDACTED] will collect the [REDACTED] for a 60mins briefing on:
  - do a brief demo,
  - share the process should an incident occur (the tagging template and email address)
  - share a one-pager on how to use the Camera “handy-helper”
  - provide a Card that enables the de-docking of the Camera and
  - associated accessories.

with this template and someone will reply quickly so the [REDACTED] can return to [REDACTED] to swap the Camera.

#### Funding (Internal for TfL only)

This will be funded by the ULEZ project

1. [REDACTED] to provide a high level cost estimate by COP on Friday (most likely to be internal time cost)
2. [REDACTED] to provide a WBS code

#### When will this be available from?

- The Cameras will be available from Friday 8 September, **as long as [REDACTED] can provide the details request in this spreadsheet by 3pm today. (21 Operatives to attend training on 08/09/23, spreadsheet has been updated)**
- [REDACTED] need to provide information on how long these cameras will be used by [REDACTED] for by 15 Sept

#### Where are the key locations?

Key addresses

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

**Caveats**

- TfL has a policy that we should be building in the provision of Body Worn Cameras aligned to our Work Place Violence and Aggression Strategy into our contracts with suppliers. This is an exception considering the urgency.
- We need to consider GDPR and how we address this

**Who are the engaged Stakeholders?**

Internal TfL

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]