F7526 A4 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:	Nicholas Allen	Date DPIA completed	27/01/2022 (last updated 22/06/2023)
Job title:	Technology Improvement Lead - LU	Proposed launch date	Q1 2022

Name and description of the project:	Name of Project: Smart Stations Proof of Concept Description: Trial of an enhanced analytics platform at Willesden Green London Underground Station. The analytics technology uses data from CCTV cameras to deliver real-time insights to station staff on customer movement, security, safety, and the station environment, to enable them to provide the best possible customer experience. Phase 1 of the deployment focused on use cases that did not identify specific individuals. Phase 2 trials the

	technology to assess how it can be used to detect and tackle fare evasion. Whereas Phase 1 used facial blurring, CCTV images that indicate fare evasion will be used to identify, apprehend and prosecute fare evaders, and will not be blurred.				
Personal Information Custodian (PIC)	Ray Adabra (Head of Customer Service – Jubilee Line)	Is PIC aware of this DPIA?	Y	Project Sponsor	Ray Adabra (Head of Customer Service – Jubilee Line)

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

Use profiling or automated decision-making to make decisions that will have a significant effect on people. Significant effects can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits.		Process special category data (relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life or sexual orientation) or criminal offence data on a large scale.		Make changes to processes and systems that are likely to result in significantly more employees having access to other peoples' personal data, or keeping personal data for longer than the agreed period.	
Use data concerning children or vulnerable people. A person with vulnerability is usually described as someone who is at a higher risk of harm than others.		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.	Y	Process personal data in a way which involves tracking individuals' online or offline location or behaviour.	Y	Match, compare or combine datasets, or have the potential to deny anonymity or re-identify people.	

Use new technologies or make novel use of existing technologies.	Y	Process personal data on a large scale or as part of a major project.		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.		Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	Y
Process biometric or genetic data in a new way.		Undertake systematic monitoring of individuals.	Y	Prevent individuals from exercising a right or using a service or contract.	

Step 1 – Identify the need for a DPIA	
Explain broadly what your project aims to achieve and what type of data and processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	Our objectives are to: a) Help staff improve the passenger experience within stations b) Drive enhancements in station safety, security and environment, and c) Test the viability of Smart Station technology in LU d) Detect, monitor and prosecute fare evasion As part of the Proof of Concept we expect the Smart Stations technology to process real-time analytics of CCTV imagery from [redacted] cameras around Willesden Green Station. Our current scope is aiming to deliver insights across 26 use cases, including four fare evasion use cases. Each of which will have its own success criteria and benefits. Ultimately the technology aims to deliver meaningful operational prompts to station staff of instances that may warrant their attention. The analytics technology will make use of advanced image recognition to pick up on environmental and people movement conditions and prompt alerts to station staff devices via an app/dashboard. The technology does not make any biometric measurements of the people in the CCTV imagery. With the exception of images used to identify and take action against fare evaders, data outputs are anonymised. The technology will also not make any decisions for station staff, it is intended only as an enabler to make them aware of a potential situation that may require their attention. No automated decisions will be taken by the technology as a result of the analytics processing performed. We have discussed this project with Simon Guild, TfL's Head of Privacy and Data Protection from the initial scoping phase as we are aware there are data protection risks to be considered when processing CCTV imagery, and in feeding analytics to station staff.

Step 2: Describe the nature of the processing	
	Smart Stations utilises a solution provided to TfL by O2 Telefonica, from their partner Integration Wizards. Our discussions with Commercial colleagues have indicated that we have a robust contract in place with O2 for the various services that they provide to us, Smart Stations will be delivered by them as part of a proof of concept using the transformation fund we have built up with them. Integration Wizards are a third party engaged by O2, we have a contract variation that has been worked through between the TfL Commercial Team, O2 Legal, as well as colleagues in TfL Data Protection. All stakeholders are satisfied that we have the necessary data protection clauses updated and included into the contract with O2.
How will you collect, use, and delete data? What is the source of the data?	**How will you collect, use, and delete data? What is the source of the data?** Data will be gathered from analysing real-time CCTV camera images from [redacted] Willesden Green Station cameras. The analytics engine will be looking for instances of use cases occurring such as a passenger falling over. If the analytics engine detects this, an alert will be triggered and sent to the Smart Stations dashboard. For the purposes of training the analytics engine, we will provide sample footage from the selected CCTV cameras to Integration Wizards in order to train the AI what to look for and set the parameters of the triggers. The sample footage will be facially blurred by TfL before it is shared with Integration Wizards. For the most part, no personally identifiable data is stored as a result of the operation or evaluation of the system. Where snapshots are taken, faces will be blurred. The exception in phase 2 of the project is that images that appear to detect fare evasion will be saved and reviewed by station staff and Revenue Control Inspectors with the express purpose of identifying individuals. Fare evasion images will not be blurred.
Will you be sharing data with anyone?	**Will you be sharing data with anyone?** Data will be processed by Integration Wizards via their on-premise edge processing device in order to generate use case alerts for station staff. Data generated from the analytics and anonymised images will

	be hosted in a cloud environment hosted at a data centre within the UK (Microsoft Azure). Discussions are underway with British Transport Police (BTP) to explore whether images of prolific fare evaders might be shared by TfL with the BTP for the purpose of identification and to establish their address so that TfL can bring a private prosecution. This will be taken forward under a separate information sharing agreement if it progresses.
Are you working with external partners or suppliers?	**Are you working with external partners or suppliers?** Yes, the trial is being provided by O2 Telefonica and their visual analytics partner, Integration Wizards.
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	**Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment).** Yes, a contract variation has been agreed with O2 and TfL to the existing O2 contract. TfL Commercial have led the drafting in consultation with Simon Guild for updates to the necessary data protection clauses within the contract. Current data protection clauses within the contract are sufficient as they do not mention the anonymity of images.
Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?	**Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?** Anonymized data relating to instances of fare evasion at Willesden Green will be shared with the data and analytics team in TfL, specifically around the gateline footfall data and instances where customers have been identified as having evaded paying a fare. No personally identifiable images of fare evasion will be provided, only redacted images including the time, and date of the evasion incident, as well as the type of gate, and type of fare evasion, and location within the station, and direction of travel i.e. in or out of the station. Fare evasion incidents will be compared with WASAAB reports to identify footage of prolific fare evaders.
How and where will the data be stored?	**How and where will the data be stored?** All communications to and from the device are encrypted using TLS 1.2 and AES 256 BIT encryption. [redacted] devices are certified as Microsoft security compliant. Data will be stored in an Azure data

	centre within the UK.
Will any data be processed overseas? You might find it useful to refer to a flow diagram or other way of describing data flows.	**Will any data be processed overseas?** No, the data processing we be performed on site at Willesden Green Station, by the [redacted] processing device supplied by Integration Wizards. Once the alerts data is extracted from the CCTV footage it is stored in a cloud hosted Azure database within the UK. You might find it useful to refer to a flow diagram or other way of describing data flows: See also the Architecture section in page 20 of the Appendix 1 [redacted]

Step 3: Describe the scope of the processing	
Who does the data relate to?	**Who does the data relate to?** Customers and staff at Willesden Green Station.
How many individuals are affected?	**How many individuals are affected?** Pre-pandemic there were approximately 25,000 customer entries and exits to Willesden Green per day (according to data on gateline taps). [redacted] No monitoring of specific staff members shall be performed using the Smart Stations dashboard. This has been agreed with the CSM and AM at Willesden Green and will be made clear to TU Reps and all Willesden Green staff. As the technology is a proof of concept rather than a standard operational tool, we are also communicating the technology as voluntary for staff members to use. Though it would help to prove the utility of the technology if as many staff members would participate as possible.
Does it involve children or vulnerable groups?	**Does it involve children or vulnerable groups?** Yes, the analytics may identify children or vulnerable groups that may trigger an alert to a station staff member of those customers are identified to have fallen into one of the use cases, including someone who may require mobility assistance with a mobility or visual disability, someone requiring assistance on stairs with a pram, or a lost child. However, whilst an alert will be generated, no information captured will be attributable to the individual alert concerns, as no personal information about the customer shall be captured, only that in that instance there is a customer in the station that may require assistance. Integration Wizards will not collect sensitive types of personal data, classed as Special Categories of Personal Data under GDPR.

If children's data is collected and used, are they aged under 13?	**If children's data is collected and used, are they aged under 13?** The analytics will be trained to identify whether a person is an adult or a child for the purposes of excluding children from scenarios such as fare evasion by using height relative to the gate. No data about the children's identify will be captured and with the exception of fare evasion images, all faces of all persons shall be blurred by the analytics engine.
What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*)	**What is the nature of the data? (Specify data fields if possible; For example, name, address, telephone number, device ID, location, journey history, etc.)** Data captured by the solution shall fall into two categories. The first is details of a use case being triggered as a result of customer behaviour in the station. This shall include which behaviour or situation has been triggered, the date and time of the trigger, and the camera location. The data captured involves analysing CCTV imagery every 1/10th of a second and tracing body movements to identify triggers. Therefore, with the exception of fare evasion images (which do not involve biometric identification), there is no capturing of an identity about an individual or biometric measurement, only their position and behaviour. This data shall be retained for 4 years for trend analytics purposes. The second the of data captured is a series of snapshot images to assist the station staff in resolving the incident identified. The images shall be facially blurred by the solution before they are viewable by station staff. Only CSSs and CSMs shall be able to view the images (in line with access to the station CCTV system). Images shall be retained by the solution for 14 days from the point when the alert was triggered, after this point they shall be permanently deleted. Images of fare evasion incidents are not blurred. WASAAB reports of regular fare evaders are used to find footage that can be used to identify fare evaders. The automated saving of fare evasion images greatly reduces the time it takes for Revenue Inspectors to locate footage of fare evasion events. The basis for any fare evasion prosecution is the witness statements of LU employees, so the inclusion of an apparent fare evasion incident identified through the Smart Stations trial is not used to determine whether or not a fare evasion offence has taken place.
Specify which special category data or criminal offence data	**Specify which special category data or criminal offence data are to be processed?** None

are to be processed?	
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	**Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?** We believe we are capturing the minimal possible anonymised data in order to achieve the aims of the proof of concept. Integration Wizards utilise face blurring technology so that no personal identification of individuals is performed by the analytics engine. A unique identifier is assigned to an individual identified by the engine.
How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?	**How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?** We would expect to be compliant with TfL data retention policies – P023 A3 Privacy and Data Protection Policy, and with G2206 A3 - Information and Records Management Factsheet 6: Legislative requirements for managing and disposing of TfL's information assets. Images captured by the solution shall be retained for 14 days, in alignment with LU policy concerning retention of CCTV data. Data captured about alerts shall be retained for 4 years from the date of creation.
Is the data limited to a specific location, group of individuals or geographical area?	**Is the data limited to a specific location, group of individuals or geographical area?** Yes, only inside Willesden Green Underground Station, at selected camera locations that satisfy the proof-of-concept use cases.

Step 4: Describe the context of the processing	
Is there a statutory basis or requirement for this activity?	**Is there a statutory basis or requirement for this activity?** There isn't a statutory requirement to carry out processing in this way. However, the objectives of the processing may fall under GLA Act 1999 - 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. Schedule 11 of that Act contains powers to carry out research into matters affecting, or arising out of, the exercise of the functions of Transport for London or any of its subsidiaries,
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.)*	**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.)** Customers and staff.
How much control will individuals have over the use of their data?	**How much control will individuals have over the use of their data?** None. CCTV cameras cover large areas of the station environment.
Would they expect you to use their data in this way?	**Would they expect you to use their data in this way?** Customers may not expect LU to be using intelligent analytics at a station. However, they are aware of the use of CCTV within stations. Therefore, we will notify customers within the station environment, likely within the ticket hall and platforms, that the Smart Station PoC is operational. There is signage in stations which states that CCTV is in operation and is being recorded and monitored for the purposes of safety, security and the detection of crime.

Are there prior concerns over this type of processing or security flaws?	**Are there prior concerns over this type of processing or security flaws?** Not that we are aware of, however we are engaged with our Cyber Security and Solution Architecture Teams, and we will go through the Architecture Review Board process to ensure the necessary TfL T&D stakeholders have reviewed and approved the solution design.
Is it novel in any way, or are there examples of other organisations taking similar steps?	**Is it novel in any way, or are there examples of other organisations taking similar steps?** Network Rail have been trialling the O2 technology for 12 months or so. O2 also utilise it within their own retail stores.
What is the current state of technology in this area?	**What is the current state of technology in this area?** TfL operates CCTV technology across all stations on the network. [redacted] Camera footage is stored for 14 days before being deleted. [redacted] A trial was performed to take historic CCTV footage and analyse mask compliance at up to 30 stations on the network. Whilst this used similar image recognition technology it was not used in a live operational environment to assist station staff. Refer to the DPIA published here: https://content.tfl.gov.uk/dpia-face-covering-compliance.pdf
Are there any security risks?	**Are there any security risks?** We are engaged with our Cyber Security and Solution Architecture Teams, and we will go through the Architecture Review Board process to ensure the necessary TfL T&D stakeholders have reviewed and approved the solution design.

Are there any current issues of public concern that you should factor in? Are you or your delivery partner signed up to any code of conduct or certification scheme?	**Are there any current issues of public concern that you should factor in?** No, We have discussed this with Simon Jones from the Customer Experience Team. **Are you or your delivery partner signed up to any applicable code of conduct or certification scheme?** No

Step 5: Describe the purposes of the processing

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the processing – for TfL, for other external stakeholders, for the individuals concerned and for society in general?

Refer to our use cases below – success criteria and customer outcomes to be confirmed.

Grouping	Ref	Use Case	Use Case Description
Station Environment	UC1	Slip/trip hazards	Monitor the movement customers and the station environment to identify instances where there are slip or trip hazards within key areas of a station on a real-time basis, and prompt action(s) to remove hazards where necessary.
Station Environment	UC2	Items on tracks	Monitor the environment and customers around tracks within a station in order to identify items that have fallen/been dropped onto tracks and may cause a safety issue on a real-time basis, and prompt action(s) to remove hazards where necessary.
Station Environment	UC3	Unattended items	Monitor the environment and customers around key areas of a station in order to identify unattended items that may have been left unattended on a real-time basis, and prompt action(s) to direct staff to attend to these items where necessary. Monitor the environment and customers around key areas of a station in order to identify suspicious items / packages that may have been discarded by customers on a real-time basis, and prompt action(s) to direct staff to items / packages where necessary.
Movement and Behaviour	UC5	Anti-social behaviour	Monitor the movement of customers around key areas of a station in order to identify instances when customers may either be carrying out or be

			the victims of anti-social behaviour on a real-time basis, and prompt action(s) to influence customer behaviour where necessary.
Movement and Behaviour	UC6	Stranded customers (individuals unable to exit gate line)	Monitor the movement of customers around key areas (including the gate line) of a station in order to identify instances of individuals that are unable to exit or enter the station, or use lifts, on a real-time basis, and prompt action(s) to assist customer(s) where necessary.
Movement and Behaviour	UC7	Vulnerable customers	Monitor the movement of customers around key areas of a station in order to identify instances of passengers that may be lost, not moving, or stuck in an area within the station on a real-time basis, and prompt action(s) to assist customer(s) where necessary.
Movement and Behaviour	UC8	Injured / unwell customers and staff	Monitor the movement of customers around key areas of a station in order to identify customers who are injured or unwell on a real-time basis, and prompt action(s) to assist customer(s) where necessary.
Movement and Behaviour	UC9	Workplace violence incidents	Monitor the movement, audio and behaviour of customers and staff around key areas of the station in order to identify instances of violence against staff members by customers, and prompt action(s) to be taken to intervene on a real-time basis
Movement and Behaviour	UC10	Crowd anomalies (e.g. running en mass)	Monitor the movement of customers around key areas of a station in order to identify mass crowd movements such as running en masse and crush incidents on a real-time basis, and prompt action(s) to influence customer movement where necessary.
Movement and	UC11	Unauthorised access	Monitor the movement of customers in public and

Behaviour		to non-public areas of a station	non-public areas of a station to identify instances when customers have gained access to non-public areas on a real-time basis, and prompting action to remove the customer from the non-public area.
Movement and Behaviour	UC12	Historic crowd movement (Flow)	Store all customer movement information around key areas of a station for a defined period of time in order to perform analysis on trends in crowd movement. Data may be aggregated in order to aid speed of analysis.
Movement and Behaviour	UC13	Face coverings	Monitor the movement of customers around a station to identify whether customers are wearing face coverings or not. This shall be tracked for analytical purposes and will not result in real-time alerts to station staff.
Movement and Behaviour	UC14	Fare evasion	Monitor the movement of customers through station gatelines in order to identify instances where customers may have evaded paying a fare, or the correct fare, for their journey. This shall be tracked for analytical purposes and will not result in real-time alerts to station staff.
Technical Feasibility	UC16	Use of Existing Cameras	Test the viability of a representative selection of existing cameras to ensure that the image quality and connectivity are suitable to enable the smart camera analytics for the Smart Stations initiative.
Technical Feasibility	UC17	Camera Alignment or Moves	Monitor the positioning of cameras to ensure that they are not out of the desired alignment, and prompt action to be taken by the appropriate staff member if instances of misalignment/movement of the camera have been identified.
Technical Feasibility	UC18	New Camera Integration	Ensure that any new camera added to the TfL estate would be able to comply with the integration requirements of TfL Engineering,

				including but not limited to: integration with the station management system, LUCC, and ability to use cameras for other purposes in future where required. *Comment: We do not expect to have to install any new cameras as part of this project, but we will explore this if the current camera quality is insufficient to be able to recognise use cases.*

	[redacted]

Step 6: Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.

Who else do you need to involve within TfL?

Have you discussed information security requirements with Cyber Security?

Do you plan to consult with external stakeholders? If so, who?

Who will undertake the consultation?

We have consulted with a wide range of internal TfL colleagues to understand and scope this initiative. A full of scoping stakeholders is below.

Name	Role	Function
Nick Allen	Technology Improvement Lead - LU	T&D - LU
Ben Gillard	Business Technology Design Lead	T&D - LU
Will Henderson	Senior Business Analyst	T&D - Tech Dev
Kelvin Blackie	Business Technology Design Lead	T&D - LU
Alan Perryman	Senior Product Manager - LU Operations	T&D - LU
Nick Rusz	Product Manager	T&D - LU
Andrew McKeever	Product Manager	T&D - LU
Jose Pereira	Improvement Lead (Network Ops)	LU - Customer Operations
Alistair Montgomery	Improvement Manager (Network Ops)	LU - Customer Operations
Ryan Sweeney	Data and Analytics Portfolio Manager	CCT - Data & Analytics
Lisa Johns	Data & Analytics Product Manager	CCT - Data & Analytics
Vasiliki Bampi	Data Scientist	CCT - Data & Analytics
Jamie Case	Technology Improvement Lead - LU	T&D - LU
Felicia Harris	SHE Business Partner	SHE
James Ingram	Senior SHE Environment Manager	SHE
Simon Abernethy	CS Modernisation Delivery Manager	LU - Network Ops
Jessica Bradley	CS Modernisation Delivery Manager	LU - Network Ops
David Kelly	CCTV Data Manager	LU - Network Delivery
Gordon Barnes	Network Security Risk & Planning Manager	LU - Network Delivery
Sarah Swalheim	Customer Experience Manager	CCT - Customer
Simon Jones	Customer Experience Manager	CCT - Customer
Helen Dimond	Customer Experience Lead	CCT - Customer

What views have been expressed by stakeholders?

Ray Adabra	Head of Customer Service Jubilee Line	LU - Customer Operations
Amanda Elias	Fit for the Future - Stations Resource	LU - Customer Operations
Gemma Davies	Change Design Manager	LU Finance - Change Design and Delivery
Trevor Hardy	Technical Head - Telecoms	LU - Engineering
Roberto Rincon	Technology Strategy Manager	LU - Engineering
Waqas (Kye) Hussain	Commercial Innovation Manager	ST - Innovation
Rikesh Shah	Head of Commercial Innovation	ST - Innovation
David Mead	Continuous Improvement Manager	LU - Line Operations
Jacqueline Attoh-Ammah	Relationship Manager (Systems)	T&D - Surface
Ben Jones	Solution Architecture Manager	T&D
Kulvinder Matharu	Senior Product Manager	T&D
Campbell Mcilroy	T&D Ops Tech Principal Sec Eng (sec)	T&D
Simon Guild	Head of Privacy and Data Protection	General Counsel
Nas Ali	Customer Service Manager 3	LU - Customer Operations
Vanda Bruce	Area Manager Jubilee North	LU - Customer Operations
Kevin Jones	CSS2 (5D) Early	LU - Customer Operations
Carl Vincent	Customer Service Supervisor 2	LU - Customer Operations
Kayode Jimoh	Customer Service Supervisor 2	LU - Customer Operations
Simon Ponsonby	Customer Service Manager 3	LU - Customer Operations

Operational Consultation

We have consulted with operational staff members about the scope and use cases in the PoC via the LU Staff Engagement Team facilitated by Amanda Elias, on 5th July 2021.

We have been in consultation with the LU Strategy and Development Trade Union Reps Sub-Group. Our proposal for running the proof of concept was taken to them for initial consultation on 24th August 2021.

We have since consulted local Trade Union representative for the Willesden Green Area on 24th

	November 2021, and Functional representatives on 2nd December 2021. No significant concerns that would hold back the project were raised at either of these sessions. However, colleagues provided very useful feedback to help us with delivering the PoC in the most effective means possible. We are also involving staff from Willesden Green in the design of the proof- of-concept, and have the approval of the HOCS for the Jubilee Line and the Area Manager for Jubilee North to proceed. These stakeholders will be involved throughout the design and running of the proof of concept. **Technical Consultation** We have involved the following technical SMEs in our initial technical discussions with O2 and Integration Wizards: Tom Williams (Operational Tech Principal Security Engineer) Alan Harding (Senior Cyber Security Analyst) Kulvinder Matharu (Senior Product Manager) Hardy Trevor (Technical Head – Telecoms, Network Technology) John Nield (SEL Telecoms, TRAIN SYSTEMS) Michael Hauptfleisch (Communications Engineer, GM STN - Premises Station Services) Jesse Field – Solution Architect

Step 7: Assess necessity and proportionality	
Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose?	**Does the processing actually achieve your purpose?** We strongly believe that the best way to test the appropriateness of the Smart Stations technology is to run a real-world trial at one of our stations. Network Rail have run similar PoCs at three of their stations and have seen significant benefits and insights from running this to augment their day-to-day operations.
Is there another way to achieve the same outcome?	**Is there another way to achieve the same outcome?** To achieve the same level of visibility and customer assistance in a station as the camera analytics achieves, you would need to employ far more staff members than we do now. Either to watch camera footage live, or to physically watch the station areas. Therefore, we believe the Smart Stations technology will be a useful addition to our current staffing model and help them to be even more effective.
How will you prevent function creep?	**How will you prevent function creep?** We have a project steering group in operation which is accountable for the outcomes of the proof of concept, and ensuring that the scope remains within the agreed objectives. The steering group is chaired by Nick Allen and meets every three weeks.
How will you ensure data quality and data minimisation?	**How will you ensure data quality and data minimisation?** The approach that Integration Wizards will take, will continually look to improve the accuracy of the alerts generated based on machine learning and feedback from the users of the dashboard. Only minimal amounts of data are created by the analytics engine based on the footage that it sees. Alerts will only be generated when a use case is triggered by the [redacted] module.

What information will you give individuals about how their data is used?	**What information will you give individuals about how their data is used?** We have signage in stations and publish our privacy notice at https://tfl.gov.uk/corporate/privacy-and-cookies/cctv
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?	**What measures do you take to ensure suppliers processing personal data on our behalf provide adequate assurances about their ability to process this data safely and lawfully?** The processing is covered by a data processor contract and steps have been taken to ensure that data is both minimised and secured during processing.
To be completed by Privacy & Data Protection team	
What is the lawful basis for processing?	The lawful basis is Public Task.
How will data subjects exercise their rights?	Data subjects already have the right to request access to their data. There is a right to object to processing of personal data where the lawful basis relied upon is public task, but as this involves a balancing test between the rights and freedoms of the individual and the legitimate grounds for the project to proceed, it is unlikely that any objection would be successful.
How do we safeguard any international transfers?	There are no international transfers.

Could data minimisation or pseudonymisation be applied?	The camera images will be blurred unless necessary for fare evasion detection, no further opportunities for data minimisation have been identified.
Are data sharing arrangements adequate?	Data sharing will be subject to contract with O2 and between O2 and IW.

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
Hidden processing caused by lack of signage and supporting information	Possible	Minimal. There is no change to the CCTV images being recorded, or the stated purposes it is used for. With the exception of fare evasion, the images are depersonalised. Revenue Inspectors already review CCTV recordings when investigating fare evasion, the Smart Stations tool simply makes it quicker to locate and extract incidents.	Low
Loss of control of LU data processed by O2 and Integration Wizard	Possible	Significant. Whilst the data would remain subject to GDPR, LU would no longer control how it is processed	Medium

Step 9: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced or accepted	**Residual risk** Low, medium or high	**Measure approved** Yes/no
Hidden processing caused by lack of signage and supporting information	Monitor project and consider changes to web page if the project is taken into wider rollout.	Reduced	Low	Yes
Loss of control of LU data processed by O2 and Integration Wizard	Check contract with O2 and request copy of O2 – IW contract.	Reduced	Low	Yes

Step 10: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Simon Guild – 02/08/2023	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Craig Marshall – 18/08/2023	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:	Blurring of images and human decision-making mean that there are low risks to individuals. Privacy Team will be represented on the Smart Stations Steering Group Have reviewed contract variation and risks - 18/08/2023 - Craig Marshall	
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

Anonymised data	Anonymised data is information held in a form that does not identify and cannot be attributed to individuals. Anonymous information is not subject to the GDPR, and, where possible and appropriate, should be used in place of identifiable or pseudonymised personal data, particularly where sharing information with third parties or contemplating publication of data. Anonymised data will often take the form of statistics. If you are reporting statistics on a small number of individuals, or there is a level of granularity that allows reporting on small groups of individuals within the overall data set, you must exercise caution to avoid inadvertently allowing the information to be linked to an individual. If information can be linked to an identifiable individual the data is not anonymous and you must treat it as personal data.
Automated Decision Making	Automated Decision Making involves making a decision solely by automated means without any meaningful human involvement. Automated Decision Making is restricted and subject to safeguards under the GDPR. You should consult with the Privacy and Data Protection team before rolling out a process involving Automated Decision Making based on personal data.
Biometric data	Biometric data is a general term used to refer to any computer data that is created during a biometric process. This includes test samples, fingerprints, voice recognition profiles, identifiers based on mouse movements or keystroke dynamics and verification or identification data excluding the individual's name and demographics. Biometric data is subject to additional safeguards under the GDPR when it is processed for the purpose of identifying individuals.
Data breaches	A ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored or otherwise processed. Personal data breaches must be reported immediately to DPO@tfl.gov.uk.

Data minimisation	Data minimisation means using the minimum amount of personal data necessary, and asking whether personal data is even required. Data minimisation must be considered at every stage of the information lifecycle: • when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary; • when deciding what information to record, you must consider what information is required, what is relevant and whether any information is excessive; • when deciding whether to share or make use of information, you must consider whether using all information held about an individual is necessary for the purpose. Disclosing too much information about an individual may be a personal data breach. When deciding how long to keep information, you must consider what records you will need, and whether some personal data can be deleted or anonymised.
Data Protection Rights	The GDPR provides the following rights for individuals: • The right to be informed; • The right of access; • The right to rectification; • The right to erasure; • The right to restrict processing; • The right to data portability; • The right to object; • Rights in relation to automated decision making and profiling.
Data quality	The GDPR requires that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*." This means you must take steps to ensure that the data you use is sufficiently accurate, up to date and comprehensive for your purposes, and that you take steps to effectively mitigate any detriment to individuals that is likely to result from inadequate data.

Function creep	Function creep describes the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Review and update your DPIA, or undertake a new DPIA to reflect changes in the purpose or the means by which you process personal data.
Genetic data	Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
Marketing	Direct marketing is “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations. Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the privacy regulations apply. Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the privacy regulations apply.
Personal data	Personal data is information, in any format, which relates to an identifiable living individual. Personal data means any information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information

	about people. The definition can also include pseudonymised data (where we hold data that has had the personal identifiers replaced with codenames); depending on how difficult it would be to re-identify the individual.
Privacy notice	A privacy notice must let people know who we are, what we intend to do with their personal information, for what purpose and who it will be shared with or disclosed to. TfL adopts a layered approach to privacy notices, with clear links to further information about: • Whether the information will be transferred overseas; • How long we intend to keep their personal information: • The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information; • The name and contact details of the Data Protection Officer; • The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner; • The details of the existence of automated decision-making, including profiling (if applicable).
Processing	Doing almost anything with personal data. The GDPR provides the following definition: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Profiling is the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymise	Pseudonymisation separates data held about an individual from information that identifies the individual. This can be

d data	achieved by encrypting (hashing) the individuals name, MAC address or ID code, masking an individual's exact location or changing an image to make an individual unrecognisable. TfL can hold the same data in identifiable and anonymous form, provided appropriate controls are in place to prevent re-identification of the pseudonymised data. The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes. Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability. Pseudonymisation is an important security measure and must be considered as part of Privacy by Design and Default approach. If you use pseudonymised data you must ensure that an individual can not be re-identified with reasonable effort. The risk of re-identification is higher when information about the same individual is combined. For example, whilst a post code, a person's gender or a person's date of birth would be very unlikely to identify an individual if considered without other reference data, the combination of these three pieces of information would be likely to enable a motivated individual to re-identify a specific individual in most circumstances. If you use a "key" to encrypt or hide their identity you must ensure it is sufficiently protected to prevent the individual being re-identified. A Data Protection Impact Assessment can help you assess whether pseudonymisation is reversible in a given scenario.
Significant effects	A DPIA will be required for processing relating to an individual, or group of individuals that has an effect on their legal status or legal rights, or will otherwise affect them in a significant way. These effects may relate to a persons: • financial circumstances; • health; • safety; • reputation; • employment opportunities; • behaviour; or • choices

Special Category data	Special category data consists of information about identifiable individuals': • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data (for the purpose of uniquely identifying an individual); • data concerning health; or • data concerning a person's sex life or sexual orientation. Information about criminal convictions and offences are given similar protections to special category data under the Law Enforcement Directive.
Statutory basis for processing	TfL is a statutory body created by the Greater London Authority (GLA) Act 1999. This Act gives the Mayor of London a general duty to develop and apply policies to promote and encourage safe, integrated, efficient and economic transport facilities and services to, from and within London. The Act also states that we have a duty to help the Mayor complete his duties and implement the Mayor's Transport Strategy. In particular, we are required to provide or secure the provision of public passenger transport services, to, from or within Greater London. As a highway and traffic authority for GLA roads, we regulate how the public uses highways and we are responsible for: • Traffic signs • Traffic control systems • Road safety • Traffic reduction We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs). The GLA Act contains specific powers to provide information to the public to help them to decide how to make use of public passenger transport services and to provide or secure the provision of public passenger transport, as well as a broadly scoped power to do such things and enter into such transactions as are calculated to facilitate, or are conducive or incidental to, the discharge of any of its functions. Further miscellaneous powers are set out in Schedule 11of the Act.

	Activities may have a statutory basis related to other legislation, for instance the requirements to publish information under the Local Government Transparency Code.
Systematic processing or monitoring	Systematic processing should be interpreted as meaning one or more of the following: • Occurring according to a system • Pre-arranged, organised or methodical • Taking place as part of a general plan for data collection • Carried out as part of a strategy Examples of activities that may constitute a regular and systematic monitoring of data subjects include: • operating a telecommunications network; • providing telecommunications services; • email retargeting; • data-driven marketing activities; • profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); • location tracking, for example, by mobile apps; • loyalty programs; behavioural advertising; • monitoring of wellness, • fitness and health data via wearable devices; • closed circuit television; • connected devices e.g. smart meters, smart cars, home automation, etc.
Vulnerable people	A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or others from harm or exploitation. All children are considered vulnerable by virtue of their age and immaturity.

APPENDIX 1

[redacted]
05.22