F7526 A5 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:	Christopher McDonnell	Date DPIA completed	September 2023
Job title:	Associate Product Manager (Payments)	Proposed launch date	By February 2024

Name and description of the project:	Delivery of a new travel Concession – the Care Leavers 18-25 Bus & Tram Discount scheme.				
Personal Information Custodian (PIC) or band 5 lead	David Kershaw (Payment Operations and Assurance Manager)	Is PIC aware of this DPIA?	Y	Project Sponsor	Lucy Preston – Senior Product Manager

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.	**X**	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.		Process personal data 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.	**X**
Use new technologies or make novel use of existing technologies.		Process personal data on a large scale or as part of a major project.	**X**	Process personal data without providing a privacy notice directly to the individual.	
Use personal data in a way likely to result in objections from the individuals concerned.		Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	
Process biometric or genetic data in a new way.		Undertake systematic monitoring of individuals.		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.	The Mayor aims to improve the London-wide offer for care leavers, firstly by signing up to the Care Leaver Covenant in 2018 and later asking Transport for London to develop a travel concession for care leavers aged between 18-25 providing half price travel on TfL buses and trams. This will be delivered via a new Oyster concessionary photocard, which will offer half price travel on buses and trams in London. The proposed scheme eligibility criteria and card validity period developed from these discussions has been endorsed by the Mayor's Office. It's estimated that 16,000 young people will be eligible at any one time with between 50-100 new applications each month. This group will be aged 18-25. 18 has been chosen as the starting age because 16/17 year olds, irrespective of their family or care status, can apply for a 16+ concessionary Oyster photocard which provides a more generous discount. As is the case with existing concessions, it is important to ensure that the application process for the new Oyster photocard is simple whilst minimising opportunity for fraudulent applications. We have identified that this group of young people may not have the necessary identity documents to apply via existing scheme application processes so we have secured support from London Councils to assist in verification of an applicant's care leaver status. London Councils have access to this data (e.g. name, date of birth, responsible borough), which is provided to them by individual London local authorities via the London Innovation & Improvement Alliance (LIIA) team. In turn, by sharing this data with TfL, this will allow us to issue Oyster photocards giving half price bus & tram travel to those eligible applicants without them having to provide identification documents during the application process such as a passport or birth certificate. The eligibility check will rely solely on this LIIA verification step. There will be no option available for applicants to upload other ID or address verification documents they may have. The applicant will provide their name, address, email address, date of birth photograph and the name of the local authority responsible for providing support during the online application process for the concession. The applicant will be presented with TfL's Privacy Notice and scheme terms and conditions during the application process. (The privacy notice will also be published online alongside the rest of TfL's suite of privacy notices). The London Innovation & Improvement Alliance (LIIA), which is part of London Councils, have a dedicated team who will collate the Care Leaver applicant eligibility data from across the 33 London boroughs. When a young Londoner becomes involved with the care system, the borough they live in or are assigned to, becomes their 'Responsible Borough'. Irrespective of whether they subsequently reside in other parts of London, their Responsible Borough will always remain the same and does not transfer.

	T&D's Data Control team will grant approved LIIA personnel access to a new scheme specific area in our Concessions application System ('InNovator'). LIIA will provide the personnel details to the nominated TfL sponsor who in turn requests access via an email to the Data Control EUC Outlook Inbox, stating the access required and what the user requires it for. The Data Control team vets and validates using their matrix. Data Control then emails the request to our third party supplier, who manages the Concessions application system on TfL's behalf - with the person's name, person's email address and the type of permission required for Novacroft to grant the access. LIIA will also be required to sign up to the Cyber Security Management Schedule, which defines the Cyber Security Requirements for Businesses that require access to TfL Systems and Data. Once access has been granted LIIA personnel will be able to upload eligible care leaver data (name, date of birth and name of their responsible borough) - in CSV format - so applicant data can be matched against it and if a match is found then the applicant will be issued with an Oyster photocard allowing them to travel at half adult rate on buses & trams. Data will be uploaded at regular intervals, with a new dataset overwriting the existing/previous one. Care leaver data will only be included in the upload in the following circumstances; • They meet the defined age criteria; • They have confirmed to their responsible borough that they wish to apply and • They have been made aware and understand that their data will be shared with TfL as part of the application verification process. (The relevant local authority will be responsible for managing this process.) Data will be uploaded in CSV format and then added by our service provider to a database table, and it is this table that applications will be verified against. New data uploads will not include anyone who has already applied for and received the photocard. We will develop functionality that will restrict LIIA access permissions so they can only 1 - upload the specified data. 2 - run two specified reports that will be created for this scheme. These reports will comprise: • a report that confirms whether an individual has made an application and received the concession; and • a report (by date range) showing number of successful applications by responsible borough and number of rejected applications by responsible borough. They will be prohibited from viewing any other data held in relation to other concessionary Oyster Schemes or

	perform other any actions. Delivery of this photocard scheme will result in the following information being processed and held in our database: • Full name • Date of birth • Address • Email address • Telephone number • Login credentials (ie username/password/security question and answer) for photocard account) • Photograph • Responsible London Borough • Payment card details (for processing of admin fee) • Contact and/or marketing preferences This is using the minimum amount of personal data necessary to process an application and is in line with TfL's other concessionary schemes. Once a card is provided additional data will be collected, including a record of journey history and any purchases made (eg Pay as You Go credit or season tickets). A DPIA is required as this project involves the creation of an entirely new concessionary travel scheme and we will be processing personal data for a new group of applicants. We will also require a new data sharing requirement between TfL and LIIA in respect of the data required in order to verify applications.
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	TfL will be able to assist in the delivery of one of the strands of the Pan London Care Leavers Compact. Those deemed eligible (as a result of using the data provided by LIIA) will receive a concessionary Oyster photocard giving them half price travel on buses and trams. In turn this will support the inclusion of young people leaving care into society and to live independently.

Will the processing directly affect the individuals concerned?	Yes, checking applicant data against the uploaded data provided by the LIIA will allow us to determine whether an applicant is eligible for the 18-25 Bus & Tram Discount scheme.

Step 2: Describe the nature of the processing (You might find it useful to refer to a flow diagram or other description of data flows).		Could there be a privacy risk?
What is the source of the data?	There are two sources: 1. The applicant will be providing their own data as part of the online application process 2. LIIA will be uploading data collated from individual boroughs. Data uploaded will only include the details of those care leavers that have expressed an interest in the scheme, and therefore have been made aware and understand that their details will be shared with TfL.	Yes
Will you be sharing data with anyone?	The LIIA will have access to a report that confirms whether an individual has made an application and received the concession. This is so that LIIA can remove that individual's data from subsequent upload data (and help ensure that TfL is not holding excessive personal data that is no longer required). No Oyster cards numbers will be included in the report. LIIA users will also be able to run/download InNovator reports (by date range) showing number of successful applications by responsible borough and number of rejected applications by responsible borough.	No
Are you working with external partners or suppliers?	TfL uses an external service provider (Novacroft) to process concessionary Oyster photocard applications, issue photocards and operate the concessionary photocard schemes on a day-to-day basis. This service provider will also operate this new concessionary scheme on TfL's behalf. TfL's T&D Payments team will update the existing disposal schedule and propose that the service provider will be responsible for implementing the disposal schedule and any data retention related processes required for the new scheme. TfL will also be working with the LIIA (part of London Councils) in order to verify eligibility for individual applications for the concession.	No

Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	Novacroft is subject to a written contract for services connected to delivering TfL's concessionary travel schemes that contains appropriate processor clauses and data protection requirements/obligations. (This will need varying if this proposal proceeds to take account of the new scheme.) The LIIA will be uploading care leaver data collated from the 33 London boroughs and providing to TfL relevant extracts of those who have indicated to their borough that they intend to apply for the concession. This data will be in CSV format. TfL and LIIA will need to create a data sharing agreement and associated data sharing processes in place to reflect this data upload and any subsequent access to information by the LIIA (e.g. via reports).	Yes
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?	Our supplier Novacroft have been TfL's Concessions System provider for over 10 years. The introduction of this new scheme and system functionality will mean that additional activities will need to be written into the existing contract. Bidders for services that include handling personal data are required to respond to (and pass) a number of data protection questions at the ITT stage of a procurement exercise. All TfL contracts for services that include personal data processing include privacy and data protection clauses as well as clauses relating to the requirement for regular security and data protection audits carried out by in-house and third party auditors. The results of these audits are required to be shared with TfL. TfL also carry out regular service reviews with Novacroft. Novacroft personnel are also required to complete TfL's online data protection training.	No
Will the data be combined with, or analysed alongside, other datasets? If so, which ones?	There will no combining or analysis of bulk datasets. There may be individual instances where it is identified that an applicant already has an active 16+ or 18+ concessionary photocard. TfL will put in place appropriate messaging and guidance for applicants in cases where this occurs.	No

Will AI or algorithms be used to make decisions? What will the effect of these decisions be?	Yes – and this is in line with existing concessionary scheme online application processes. When the applicant enters their address and date of birth, the system uses simple logic to validate that their postcode is within the relevant London boroughs and date of birth to confirm whether they are less than either 14 days prior to their 18th birthday or 14 days prior to their 26th birthday. This determines whether the applicant is eligible and can proceed with their application or not. Simple data matching rules will also be used to check whether an applicant's data provided by them matches against the data provided by LIIA. If a positive match is made a card will be issued. This will use a data table uploaded by LIIA into the Concessions System.	No
How and where will the data be stored?	It is proposed that the applicant data for this concession will be stored alongside all other applicant data within the Concessions System. Data is currently stored on-premise in the TfL hosted Oracle database. This will be the case for both the application data provided by the individual customers as well as the data uploaded by London Councils. The Concessions System is moving to a fully cloud hosted option in 2024 with the database and the record management tool, InNovator, moving to a cloud based solution.	No
Will any data be processed overseas? Which countries?	No – UK based datacentres will be used.	No
Are you planning to publish any of the data? Under what conditions?	We expect to publish reports detailing the number of applicants from each London borough and the number of cards issued by age. (These are reports which already exist for TfL's other concessionary travel schemes.) Any data published will be anonymised as it will take the form of statistics.	No

Step 3: Describe the data		Could there be a privacy risk?
Who does the data relate to?	The data relates to applicants of the 18-25 Bus & Tram Discount scheme – the eligibility criteria means that all applicants will be care leavers residing in Greater London.	No
How many individuals are affected?	It's estimated that 16,000 young Londoners will be eligible at any one time with between 50-100 new applications each month.	No
Does it involve children or vulnerable groups? If children's personal data is processed, how old are they? Consider the ICO Age Appropriate Design Code	Care leavers may be considered to be a vulnerable group and may face various challenges, disadvantages and inequalities. Some local authorities treat the experience of care as a protected characteristic. In terms of the 18-25 scheme, the identity verification steps within the application process have been designed to take account of the fact that care leavers may not have the necessary identity documents usually required. TfL's interaction with care leavers will be limited to delivering the travel concession and providing associated customer service thereafter. This does not present any specific or different privacy risks to any other Oyster card customer.	No
What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*) Are there any Special Category or sensitive data (list all): Race or ethnicity; Physical or mental health, Political opinions; Religious or philosophical beliefs; Trade Union	For the application process we will collect the following: • Full name • Date of birth • Address • Email address • Telephone number • Login credentials (ie username/password/security question and answer for photocard account)	No

membership; Using genetic or biometric data to identify someone; Sex life or sexual orientation; Criminal allegations or convictions	• Photograph • Responsible London Borough • Payment card details (for processing of admin fee) • Contact and/or marketing preferences Once a card is provided additional data will be stored within the account, including a record of journey history and any purchases made (eg Pay As You Go credit or season tickets). We will also routinely accept an upload of data from LIIA which includes the details of all those that are eligible for the scheme and have expressed an interest (ie they understand that LIIA will share their data with TfL as part of the application process and will receive a report as to whether their application has been successful or rejected.). No special category or other sensitive data will be held.	
What is the nature of TfL's relationship with the individuals? *(For example, the individual has an oyster card and an online contactless and oyster account.).* Is the data limited to a specific location, group of individuals or geographical area?	The data subjects will have applied directly for a photocard. The applicants will have created an online photocard account in order to submit the application. Once issued, recipients will be able to add their concessionary card to an Oyster web account, should they wish. The data is limited to Londoners aged 18-25, who are leaving care but still under the responsibility of a London local authority and residing within a London borough.	No
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	No. A concessionary Oyster photocard has to be issued to a named individual and it is necessary to verify that an applicant is entitled to receive the discounted travel and meets the defined eligibility criteria. Processes have been created so that the minimum data possible is uploaded by LIIA and shared with TfL – and to ensure that it is regularly refreshed to remove data that is no longer required.	No
How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?	The majority of the data will be supplied by the applicants themselves and so they will be responsible for providing accurate data to TfL. The data provided by the LIIA will be subject to their own internal validation/accuracy checks before it is uploaded, and previous successful applicant data removed. In the event that any inaccurate	No

	data is identified, this can be corrected in a subsequent upload by LIIA. This will also form part of the requirements included in the information sharing agreement.	
How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process? Do you have a documented disposal process?	It's proposed that the application data will be retained for the 3 years after the photocard has expired (the day before a cardholder's 26th birthday). This three-year period is in alignment with all other data held in relation to a photocard holder and applicant. The data uploaded by LIIA will be overwritten each time a new upload is made – this applies both to the actual file uploaded by LIIA and the data transferred from the file to a separate database table. The deletion process would be administered by Novacroft, under the express instruction of TfL. TfL will be responsible for ensuring the deletion process is routinely implemented. The Concessions contract supplier, currently Novacroft, is responsible for implementing the deletion process based on TfL's instructions. TfL will be responsible for ensuring the deletion process is routinely implemented. There is a documented local disposal schedule which is held by the Payments Products team in T&D. This is being updated to include the rules of this new scheme as part of the Project delivery. Any journey data stored in the account once the card is in active use will be stored for the standard retention period for Oyster journey data, as described in the published Oyster privacy notice.	No

Step 4: Describe the context of the processing		Could there be a privacy risk?
Is there a statutory basis or requirement for this activity?	Yes - 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. The Mayor has a general power in section 30(1) of the Act to do anything he considers will further one or more of the Greater London Authority's principal purposes of promoting economic development and wealth creation, promoting social development, and promoting the improvement of the environment in Greater London. The Mayor is also under a duty under sections 174(1) and 155(1) to direct TfL as to the general level and structure of fares to be charged on TfL public passenger services. A Mayoral Delegation and Direction will be required in order for TfL to implement and operate the Travel Concession	No
Is there any use of Artificial Intelligence or automated decision making?	It's expected that simple data matching rules will be used to check whether an applicant's data provided by them matches against the data provided by LIIA. If a positive match is made a card will be issued. Like other existing schemes there will be simple logic to validate the applicant's postcode is within the relevant London boroughs and date of birth to confirm whether they are less than either 14 days prior to their 18th birthday or 14 days prior to their 26th birthday	No
Will individuals have control over the use of their data? If so, how can they control it?	Individuals will have limited control over the use of their data as this is largely set out by the requirements and design of the concessionary travel scheme. A new privacy notice will be required, and this will describe the purposes for which personal data will be	No

	processed. Applicants will also be asked to confirm that that are aware and understand that their data will be shared by the responsible borough (VIA LIIA) with TfL - ie they express an interest in the scheme. The relevant London Borough will be primarily responsible for this part of the process, but it will also be included in TfL's own privacy notice which will be presented to applicants before they submit any application information. Individuals will be able to exercise their information rights under Articles 15-21 of the UK GDPR (i) to be informed, (ii) of access, (iii) to rectification, (iv) to erasure, (v) to restrict processing, (vi) to data portability, (vii) to object and (viii) to automated decision-making including profiling). Each request will be considered on a case by case basis.	
Would they expect you to use their data in this way?	Yes. An individual would expect there to be a formal application process in order to receive concessionary travel – and that this would include verification of eligibility with the relevant agencies. Some applicants will also have been previous holders of a TfL travel concession (ie a Zip or 16+ Oyster photocard) and so may possibly have some familiarity with application/verification requirements.	No
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?	A privacy notice will be provided to applicants before they submit their application, which is consistent with the process for other concessionary Oyster cards. This will be supplemented with the creation of a new, concession-specific privacy page published on the TfL website: www.tfl.gov.uk/privacy The TfL Privacy and Data Protection team will be responsible for creating this content. We will expect that the relevant London Borough (or LIIA on their behalf) will also provide individuals with information about the proposed information sharing which will be necessary to verify an application.	No
Are there prior concerns over this type of processing or security flaws?	No immediate concerns from TfL's perspective as we will be utilising a data upload mechanism already in place with other concessionary Oyster Schemes (ie Police & Athletes concessionary travel schemes). TfL's Cyber Security team will be consulted and approval to proceed will be sought. LIIA will need to secure agreement from their own Information Governance/Cyber teams to proceed with uploading data to TfL's systems. LIIA will be required to demonstrate they are able to meet TfL's security requirements before access permissions will be granted.	No

Is it novel in any way, or are there examples of other organisations taking similar steps?	Transport for Greater Manchester also administer a concessionary travel scheme for care leavers. https://tfgm.com/tickets-and-passes/care-leavers However, given that there are only 10 local authorities in the area and a much smaller client base of less than 3000, they have decided on a different approach. Upon application their system triggers an automatic email to the applicant's local authority to confirm eligibility. A 'yes' response leads to a simple issuing of the pass (this still requires a manual hand to trigger it). The actual application process and the technology/systems involved has been in use by TfL for many years.	No
What is the current state of technology in this area? Is this innovative or does it use existing products?	The functionality proposed uses an existing mechanism (currently used by the Police and British Olympic Association) whereby the body holding the eligibility data uploads the data to TfL's system for matching. The actual application process and the technology/systems involved has been in use by TfL for many years.	No
What security risks have you identified?	No Specific security risks have been identified in relation to implementing this new concessionary scheme. There are existing access and security processes for the systems used and these will be replicated going forward. LIIA will be required to comply with the TfL Cyber Security Management Schedule, which defines the Cyber Security Requirements for Businesses that require access to TfL Systems and Data.	No
Are there any current issues of public concern that you should factor in?	None identified	No
Is the processing subject to any specific legislation, code of conduct or certification scheme?	No	No
Will there be any additional training for employees?	There will be training for employees (TfL and Novacroft) on the new Scheme. There will be training for LIIA on using InNovator to upload data.	No

Does the processing actually achieve your purpose?	Yes, the data fields processed as part of the application process are necessary in order to produce and issue the concessionary card. The data sharing is necessary as it allows TfL to protect its revenue as it ensures only eligible care leavers (as deemed by the LIIA) receive the valuable travel concession.	No
Is there another way to achieve the same outcome?	There is no viable alternative to the data sharing itself, as it is the only reliable method of verifying eligibility for this group of customers (who may not have the usual proofs of identity/residency that we would normally require). In earlier discussions we had considered a possible alternative approach whereby we queried the collated data (sitting in a dedicated LIIA data platform) with the applicant's details to see if they were on the collated data list. This would have been via a secure API from TfL's system to London Councils for verification with a Y or N returned back to the concession system. This potential alternative was found to be a more time consuming (and costly) method to validate applicants' eligibility. It would also require a longer lead time to implement additional APIs with LIIA/London Councils, which would lengthen delivery timescales.	No
Who will own this initiative and ensure there is no function creep without a review of this DPIA?	Product Manager, Payments team.	No

Step 5: Consultation process		Could there be a privacy risk?
Consider how to consult with relevant stakeholders: Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.	It is not considered necessary to consult with the intended data subjects on this occasion. The delivery of the new concessionary travel scheme is intended to benefit the data subjects and does not, in itself, constitute a high risk activity that could result in harm or detriment to individuals. .	No
Which business areas have been consulted within TfL?	Cyber Security team Counter Fraud and Corruption team Privacy and Data Protection Team Public and Regulatory Law team	No
Have you discussed information security requirements with Cyber Security? If so, who is your contact in Cyber Security?	Yes, the Cyber Security team is aware, and we are working with a Senior Cyber Security Advisor on this project.	No
Do you plan to consult with external stakeholders? If so, who?	Whilst we will be discussing delivery progress with external stakeholders (including London Councils and the Mayor's Office) about the new scheme we will not be consulting about the data processing or information sharing elements of this project.	No
Who will undertake the consultation?	N/A	No
What views have been expressed by stakeholders?	N/A	No

Step 6: Identify and assess risks				
Describe source of risk and nature of potential impact on individuals. Include risks of damage or distress as well as associated compliance and corporate risks as necessary.	**Likelihood of harm** **Remote = Less than 10%** **Possible = 10-50%** **Probable = Over 50%**	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Is this risk included in project or other risk register?**
Unauthorised access to data held in the TfL concessions system by LIIA users due to access permissions being set up incorrectly	Remote	Severe	Medium	tbc
Unauthorised access to data in the TfL concessions system by LIIA users due to ineffective movers/leavers/joiners process, meaning that individuals can access data or reports when they no longer have a legitimate need to do so	Remote	Severe	Medium	tbc
Inaccurate data supplied by LIIA meaning that an individual's application is refused	Remote	Significant	Low	tbc

Lack of privacy notice/transparency provided to applicants by their responsible borough meaning that they do not understand or are not aware of the information sharing required to verify their application	Remote	Minimal	Low	tbc

Step 7: Identify measures to reduce risk					
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8					
Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated, reduced or accepted)	**Residual risk** (Low, medium or high)	**Measure approved** (Yes/no)	**Who is responsible for implementation?**
Unauthorised access to other data held in the TfL concessions system by LIIA users due to access permissions being set up incorrectly	T&D's Data Control team vets and validates using their matrix to determine type of permission profile required for Novacroft to grant access to the Concessions system. This Role Based Access Control (RBAC) limits access to only the areas needed for the function they are performing. Users will all have to complete an online GDPR course prior to gaining access for awareness of responsibilities. Each permission request will require authorisation from TfL	Reduced	Low	Yes	T&D Data Control Team

	concessions gatekeeper Approved LIIA personnel will be granted access to a new scheme specific area in the Concessions Application System allowing eligible care leaver data to be uploaded. This will utilise a data upload mechanism already in place with other concessionary Oyster Schemes (ie Police & Athletes schemes). LIIA's access permissions will be restricted so that LIIA personnel cannot perform any other actions outside those described as required to administer the Care Leavers concession.				
Unauthorised access to data in the TfL concessions system by LIIA users due to ineffective movers/leavers/joiners process, meaning that individuals can access data or reports when they no longer have a legitimate need to	Data control grant and remove access in to InNovator. An email or mover/leaver form is sent to the Data Control team inbox by	Reduced	Low	Yes	T&D Data control Team

do so	TfL gatekeeper to remove/amend access. Quarterly reviews of Innovator access is also completed. LIIA data team IP addresses will be whitelisted by Novacroft to enable access into InNovator specific to those users. If the users move away from the team or leave LIIA, then their IP address will not reflect those authorized to access. The IP address whitelisting will give access to the Care Leavers area only. Novacroft will create an "organisation" for LIIA in InNovator where they only have Care Leaver related access. TfL and LIIA will need to create a data sharing agreement and associated data sharing processes including guidelines				

	around authorised access.				

To be completed by Privacy & Data Protection team		Could there be a privacy risk?
What is the lawful basis for processing?	The lawful basis for processing in this case is Article 6 (1) (e) of the UK GDPR – "The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."	No
Are there any Special Category or sensitive data?	No special category (or crime-related) personal data will be processed by TfL.	No
Is this use of personal data compatible with our original purposes for collecting the data?	Yes, the personal data will be collected for the purpose of administering the new concessionary travel scheme, which is the original purpose	No
Are changes to Privacy Notice required?	A new privacy notice will be required The responsible borough for an individual will also have a role in ensuring that an applicant is aware how their data will be shared at the point they are asked if they'd like to apply for the travel concession.	Yes
How will data subjects exercise their rights?	Data subjects will be able to exercise their information rights with TfL in accordance with existing processes, which are published on our website on various pages, including Access your data, and Your Information Rights.	No
How do we safeguard any international transfers? Is any data being processed outside the UK?	No international transfers are expected.	No
Could further data minimisation or pseudonymisation be applied?	No. The application process captured the minimum possible data necessary (and is broadly consistent with the application requirements for other concessionary travel schemes)	No
Have appropriate security measures been considered, with Cyber Security involvement where necessary?	Cyber Security will be fully involved in the project and will implement the required security measures for any third party access to TfL systems.	No

Are data sharing arrangements adequate? Do they require further documentation?	A new information sharing procedure between London Councils and TfL will be required before data sharing can commence.	Yes
Is the data likely to be and remain adequate, accurate and up to date?	LIIA will be responsible for ensuring the care leaver information they provide to TfL is accurate and up to date. Individual card holders will be able to update any contact information in their TfL photocard account themselves.	No

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	**Privacy Team Leader: 26/09/2023**	**Integrate actions back into project plan, with date and responsibility for completion.**
Residual risks approved by Privacy Team:	**Privacy Team Leader: 26/09/2023**	**If accepting any residual high risk, consult the ICO before going ahead.**
Privacy & Data Protection team advice provided:	**Privacy Team Leader: 26/09/2023**	**Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed.**
Comments/recommendations from Privacy and Data Protection Team:	**Information sharing agreement to be created and signed by both partners** **New privacy notice to be created and published on TfL website** **Assurance to be sought from LIIA that adequate privacy notice and transparency will be given to applicants by their responsible borough when expressing an interest on applying for the scheme** **This DPIA to be published on the TfL website**	
DPO Comments:	**Close management attention will be required to ensure the movers/leavers process maintains sufficient control over access to Innovator by LIIA staff while this Concession is in existence. Assurances it remains effective should be provided to the Privacy and Data Protection team on a regular basis.**	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):	Yes	If overruled, you must explain your reasons below.
Comments: No further comments		
This DPIA will kept under review by:	Associate Product Manager (Payments)	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 Top of Form 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. Bottom of Form
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. Bottom of Form
Function creep	Function creep describes the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Review and update your DPIA or undertake a new DPIA to reflect changes in the purpose or the means by which you process personal data.
Genetic data	Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Marketing	Direct marketing is "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals". This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations. Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the privacy regulations apply. Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the privacy regulations apply.
Personal data	Personal data is information, in any format, which relates to an identifiable living individual. Personal data means any information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The definition can also include pseudonymised data (where we hold data that has had the personal identifiers replaced with codenames); depending on how difficult it would be to re-identify the individual.
PIC (Personal Information Custodian)	Personal Information Custodians are senior managers, who are responsible for the Processing of Personal Data within their assigned area of control.
Privacy notice	A privacy notice must let people know who we are, what we intend to do with their personal information, for what purpose and who it will be shared with or disclosed to.

	TfL adopts a layered approach to privacy notices, with clear links to further information about: • Whether the information will be transferred overseas; • How long we intend to keep their personal information: • The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information; • The name and contact details of the Data Protection Officer; • The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner; • The details of the existence of automated decision-making, including profiling (if applicable).
Processing	Doing almost anything with personal data. The GDPR provides the following definition: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Profiling is the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Bottom of Form
Pseudonymised data	Pseudonymisation separates data held about an individual from information that identifies the individual. This can be achieved by encrypting (hashing) the individuals name, MAC address or ID code, masking an individual's exact location or changing an image to make an individual unrecognisable. TfL can hold the same data in identifiable and anonymous form, provided appropriate controls are in place to prevent re-identification of the pseudonymised data. The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes. Pseudonymised data (if irreversible) is not subject to the individual's rights of rectification, erasure, access or portability. Pseudonymisation is an important security measure and must be considered as part of Privacy by Design and Default approach. If

	you use pseudonymised data, you must ensure that an individual cannot be re-identified with reasonable effort. The risk of re-identification is higher when information about the same individual is combined. For example, whilst a post code, a person's gender or a person's date of birth would be very unlikely to identify an individual if considered without other reference data, the combination of these three pieces of information would be likely to enable a motivated individual to re-identify a specific individual in most circumstances. If you use a "key" to encrypt or hide their identity you must ensure it is sufficiently protected to prevent the individual being re-identified. A Data Protection Impact Assessment can help you assess whether pseudonymisation is reversible in a given scenario.
Significant effects	A DPIA will be required for processing relating to an individual, or group of individuals that has an effect on their legal status or legal rights or will otherwise affect them in a significant way. These effects may relate to a person's: • financial circumstances; • health; • safety; • reputation; • employment opportunities; • behaviour; or • choices
Special Category data	Special category data consists of information about identifiable individuals': • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data (for the purpose of uniquely identifying an individual); • data concerning health; or • data concerning a person's sex life or sexual orientation. Information about criminal convictions and offences are given similar protections to special category data under the Law Enforcement Directive.
Statutory basis for processing	TfL is a statutory body created by the Greater London Authority (GLA) Act 1999. This Act gives the Mayor of London a general duty to develop and apply policies to promote and encourage safe, integrated, efficient and economic transport facilities and services to, from and within London. The Act also states that we have a duty to help the Mayor complete his duties and implement the Mayor's Transport Strategy. In particular, we are required to provide or secure the provision of public passenger transport services, to, from or within Greater

	London. As a highway and traffic authority for GLA roads, we regulate how the public uses highways and we are responsible for: • Traffic signs • Traffic control systems • Road safety • Traffic reduction We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs). The GLA Act contains specific powers to provide information to the public to help them to decide how to make use of public passenger transport services and to provide or secure the provision of public passenger transport, as well as a broadly scoped power to do such things and enter into such transactions as are calculated to facilitate, or are conducive or incidental to, the discharge of any of its functions. Further miscellaneous powers are set out in Schedule 11of the Act. Activities may have a statutory basis related to other legislation, for instance the requirements to publish information under the Local Government Transparency Code.
Systematic processing or monitoring	Systematic processing should be interpreted as meaning one or more of the following: • Occurring according to a system • Pre-arranged, organised or methodical • Taking place as part of a general plan for data collection • Carried out as part of a strategy Examples of activities that may constitute a regular and systematic monitoring of data subjects include: • operating a telecommunications network; • providing telecommunications services; • email retargeting; • data-driven marketing activities; • profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); • location tracking, for example, by mobile apps; • loyalty programs; behavioural advertising; • monitoring of wellness, • fitness and health data via wearable devices;

	• closed circuit television; • connected devices e.g. smart meters, smart cars, home automation, etc.
Vulnerable people	A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or others from harm or exploitation. All children are considered vulnerable by virtue of their age and immaturity.