F7526 A3 Data Protection Impact Assessment (DPIA) Checklist

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

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

Your details			
Name:	Chloe Davies	Date DPIA completed	24 July 2020
Job title:	Senior Product Manager	Proposed launch date	Internal Alpha – May 2019 Internal Beta – December 2019 External user testing – July 2020

Name and description of the project:	**TfL Go – iOS app Alpha, internal Beta trials and external user testing (pre-public launch)** TfL Go is a new, location aware, mobile app concept providing travel support to users. In advance of the public launch, TfL has carried out some trials with a small number of people and this DPIA assesses those trials. The initial Alpha trial included approx. 125 TfL staff, from outside of the project development team. A wider internal Beta included around 500 staff from across TfL. Additionally external focus groups were run carrying out an external user testing with members of the public, run through an agency with a long-established relationship with TfL, with around 24 users over two weeks. The apps developed for these trials are iOS apps and only available for iOS users. The public launch of the iOS app is expected in August 2020 and a separate DPIA will be completed for the public launch as the users and data processed for the trials is different for the public launch. This DPIA also allows the opportunity to review privacy considerations unique to the trials (eg participant recruitment and surveys) and to identify and incorporate privacy considerations into the full public launch. Future versions of TfL Go will involve the collection of mobile device data – this will be the subject of a separate DPIA.				
Personal Information Custodian (PIC)	Ben Gammon	Is PIC aware of this DPIA?	Y	Project Sponsor	Ben Gammon

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.	Y	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.	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.	Y	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.		Prevent individuals from exercising a right or using a service or contract.	

Step 1 – Identify the need for a DPIA	
Explain broadly what your project aims to achieve and what type of data and processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	**Project overview** TfL Go is a new mobile app that will support customers as they travel in London. The longer-term vision is for the app to become 'your personal travel assistant' – including all modes of transport and with an experience that is highly personalised to the individual. *Separate DPIA to be completed to look at collection of mobile device data.* The first public release will focus on the tube and be built around the tube map. It will include the following features, which will be introduced incrementally during the Alpha, internal Beta phases and external user testing: • A data-driven, interactive tube map, including a step free map view, and live service status updates (no personal data required) • Location-awareness, so that the user understands where they are in relation to the tube map and any maps embedded in the app (personal data processed – location data) • Multi-modal journey planning via the map – tap on a station to get the best route from a current location (personal data processed – location data and intended destination data, ie journey plans) • The option to set accessibility preferences. These are stored in the app and determine the specific accessible maps and journey plans presented to the user (personal data processed – in the longer term this could include Special Category data, as relating to accessibility needs. A step free mode button on the map screen will toggle the tube map between the standard tube map and step free tube map, this may indicate that the anonymous user has an accessibility need, or is a user with a buggy/luggage, etc.) ○ It is possible that in the future accessibility preferences would be saved to an individual's TfL ID account, meaning that data is stored outside of the app and would apply to all services (*this is not currently on the roadmap*). *Separate DPIA to be completed at an appropriate point to look at wider use of accessibility data* • Stop views – this will provide information on what step free characteristics exist for getting between a station entrance and a platform (or train) – whether the route involves lifts/stairs/escalators, and the step and gap information between the train and the platform. Stop views will also provide station information, including available facilities (eg live lift status, types of toilets available and live Tube and rail arrivals (no personal data required) • General interface improvements will also happen throughout the trials, this covers general tweaks to existing

functionality that won't have material impact on the functionality itself.

The first public release of TfL Go will not include any sign-in or account functionality; however, this will be added to later versions to enable more tailored experiences. This will likely include full integration with TfL accounts and payments activity. The Privacy and Data Protection team will remain engaged with the TfL Go project team and assess any privacy requirements as development continues. Where necessary amendments will be made to the public launch DPIA, or new DPIAs compiled where the processing is fundamentally different to that described here. However, where appropriate a 'risk and mitigation log' will be maintained to address privacy related impacts of new app versions which do not require a full DPIA revision. The TfL Go project team will have regular contact with the Privacy and Data Protection team and advise of functionality updates at an early stage.

Once the app is launched, TfL will revisit the idea for TfL Go to have a commercial partner, most likely in the form of app sponsorship. This is unlikely to be looked at again until 2021. At the current time, we do not expect to share customer data with this partner (beyond high-level, aggregated app usage stats) but this may be something Customer and Revenue wish to explore in the future. *The Privacy and Data Protection team will assess at an appropriate point if a separate DPIA is required to review sponsorship and any proposed data sharing.*

The original business case papers have been shared with the Privacy team for reference.

Alpha, internal Beta trials and external user testing

The app is due to launch to the public in August 2020. Ahead of this, we ran some small-scale trials, initially with TfL staff and then with a small number of external users. The Alpha trial was managed via an online tool provided by our research partner 2CV; the Beta trials was managed by the TfL Go project team. The external user testing was carried out remotely and managed by our research partner 2CV.

<u>Alpha</u>

- This ran from May to July 2019, facilitated by an external research supplier 2CV
- Approx.125 TfL staff were recruited from the wider TfL staff network, in addition to project team members and stakeholders
- It was run in two cohorts (46 participants in stage one and 79 in stage two), with additional functionality added between stages one and two
- The research report prepared by the external supplier, 2CV, has been shared with the Privacy team

	<u>Internal Beta</u> • This ran from c. December 2019 to March 2020 • 769 TfL staff were recruited from the wider TfL staff network, in addition to project team members and stakeholders. The Internal Beta was managed by the TfL Go project team • Invitations to download the app were sent out in three cohorts, linked to app updates being made <u>External user testing</u> • Recruitment was carried out by a third party research partner 2CV. • The beta version of the app was also tested by non-TfL users in order to test the concept and usability of the app. New features include step free tube map and the option to set accessibility preferences, Voiceover and Dynamic Type support. • 24 testers were recruited from members of the public. Some of the users who tested the app were people with mobility impairments ("MIPs") and visual impairments ("VIPs"). • The app is designed to be inclusive and to work for as many people as possible. MIPs are likely to require information about step free journeys or more granular information on moving around stations. VIPs will benefit from TfL Go using OS-level accessibility features such as VoiceOver (which reads out text on screen) and Dynamic Type (which seamlessly increases font size), as stipulated by the Web Content Accessibility Guidelines (WCAG) standards. For Alpha and internal Beta trials, participants all lived in London as at that time the app did not support journey planning outside of London. This functionality was built in for the external user testing so testers in the external user testing lived in London or outside of London (but travelled at least once a week to London during the test). All participants were over 18. The Alpha, Beta trials and external user testing allowed us to gain valuable insight into the usage, performance and perception of the TfL Go app. This helped optimise the launch proposition and formulate the post-launch roadmap.

Step 2: Describe the nature of the processing	
How will you collect, use, and delete data? What is the source of the data? Will you be sharing data with anyone? Are you working with external partners or suppliers? Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.) Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones? How and where will the data be stored? Will any data be processed overseas? You might find it useful to refer to a flow diagram or other way of describing data flows.	The data processed as part of this project falls into the following categories: • Trialist information • App usage data • Location data • Feedback Each type of data has been considered in turn below. • **Trialist information** We needed to recruit and manage participants for the Alpha, internal Beta trials and external user testing, which involves collecting personal data. We used a recruitment questionnaire to collect information in the alpha, internal Beta trials and external user testing. The purpose and benefit of collecting and processing the trialist information was purely for successful recruitment; to enable us to onboard participants and to ensure that the right mix of people was included. **1) The Alpha trial** The trial was advertised on Yammer and Source and respondents completed a Microsoft Forms questionnaire to register their interest and to allow the selection of a range of suitable participants. The questionnaire submission process included a privacy notice and the questionnaire collects following personal information: • Name – required for identification and communication purposes • Email address – required for communication purposes • Age range – required to ensure a spread of trialists (only for Alpha trial) • Device type and OS version – required to ensure app compatibility

	• Availability during the alpha trial period • Local tube or train station and 2 or 3 other stations that they regularly travel to/from • How often the participants use the tube for work and how often do they take the tube other than their work commute • An app the participants use and what they like about it 260 people submitted the Forms questionnaire, of which 125 were selected to take part in the Alpha trial. These were split across two cohorts: the first had 46 participants who downloaded the app; the second had 79 participants. The submission process included an opt-in for respondents to indicate if they were happy for the TfL Go team to keep their details for subsequent phases of the trial. 238 of the 260 respondents indicated that they were happy to be contacted again. The Alpha trial was managed using TfL's research partner, 2CV's online research tool.This is a closed online network allowing participants to share feedback with TfL via 2CV. The details of all respondents were shared with 2CV, to enable them to shortlist and select participants. Respondents' details were shared with 2CV via a password protected Excel file, shared using a secure file sharing system. Any passwords were shared separately, for example in a follow-up email. The details of unsuccessful respondents were retained during the trial period, to enable a pool of replacement trialists in case of drop-outs. Trialists could opt for their data to be held for involvement in future TfL Go trials. Selected participants were onboarded to the 2CV online tool, and subsequent communications predominantly managed from there. The onboarding process included trial terms and conditions and a privacy notice. 2CV delivered reports based on the trial findings. These provided insight framed by a demographic type (eg age, gender). For Alpha trial all data is held within the UK. TfL and 2CV grant access to personal information processed on a need-to-know basis. Only a small number of people working on the project have access to the online platform and participants' details: • At TfL, the UX research lead had access to the participants' details • At 2CV, the Research Director and Associate Director had access to the participants' details. Up to 20 researchers have access to the online platform (which doesn't include any personal information)

	but only the three members of the team working on the project accessed the TfL project area The Go project team will delete any trialist information 1 month after the trials are completed, except for those who have agreed for us to keep their information on file for use in future trials. **2) The Internal Beta trial** The trial was advertised on internal TfL digital channels (eg Yammer, Source, and staff email newsletters) and through attendance at team meetings. 769 TfL staff were recruited from the wider TfL staff network, in addition to project team members and stakeholders. The first cohort was made up from the 238 people who consented to be contacted again when they signed up for the Alpha trial. These people were emailed a link to the Internal Beta Microsoft Forms recruitment questionnaire, the questionnaire submission process includes a privacy notice and the questionnaire collects the following information: • Device type and OS version • How often the participants use the tube • Nearest tube or rail station to home Applicants also have the option to agree for us to keep their details on file for other TfL digital trials. Participants may also be sent an occasional survey. This will be sent to the email address they signed up with. The survey may include demographic information to better understand the results; but would not request any direct personal information except for an optional email address field if they are happy for us to contact them with any follow-up questions. Any survey will be shared with the Privacy team before distribution. 80 people completed the form of which 75 were selected to take part in the first cohort. Subsequent cohorts were recruited via a Microsoft Forms questionnaire (similar to that used for the Alpha trial). Initially unsuccessful respondents' details were retained during the trial, to provide a pool of participants should they

	be needed later in the trial. No data will be stored overseas. Respondents' details were kept in a password-protected Excel spreadsheet, stored in SharePoint and accessible only to a small number of TfL Go trial project team members. The Go project team will delete any trialist information 1 month after the trials are completed, except for those who have agreed for us to keep their information on file for use in future trials. The TfL Go project team managed the trial internally and TestFlight will be used to test the internal beta app. When testing apps with TestFlight, Apple will collect and send crash logs, users' name and email address, usage information and any feedback users submit to the developer through the app (not including information emailed to the developer directly) to improve their products and services. **3) External User Testing** The recruitment was carried out by a third party research partner 2CV under a contract with TfL. 24 testers were recruited from members of the public, including people with mobility impairments ("MIPs") and visual impairments ("VIPs"). Testers were asked for information to provide insight into the type of user they represent on a screener questionnaire. 2CV has provided a privacy notice in the screener questionnaire and used the screener questionnaire to collect the following information: • Sex • Age • Marital status

	• Working status • Whether they have children • Current occupation and job title, industry • Whether the participants' job fall into one of the trade/organisations that we do not recruit from • London borough and zone participants live in • Frequency of using different modes of transport • Reason for reverting to using car/carb when travelling in London • Purposes of using public transport in London • Impairment that limit the participants' daily activity or work they can do, brief description of impairment and tools/aids/support used/needed (special category data) • Whether the participants travel with a pram • Device type, Make and model of device • Whether the participants currently download and use apps on their personal iPhone • Which activities do they do by app on their iPhone? • Which apps the participants use when using public transport to get around London • Whether the participants use Dynamic type, Voice over iOS or other features on their iPhone • When travelling, how the participants intend to listen to their voiceovers • Statements that best describe the participants' attitude to technology in general Due to Covid-19 lockdown enforced by the Government making in person testing infeasible, the user testing was carried out remotely and managed by 2CV using a tool called Lookback to view customer's device screen and capture audio and/or video. Lookback is a live video streaming app. The videos are recorded to give the opportunity to the research team to observe the participants user of the app and double check how participant reacted to the use of certain features in the app, while creating a report. This is standard as part of a market research study and the video recording is part of the marketing study. 2CV used Lookback to collect the following personal information from testers:

	• First name • Email address • Device name • IP address • Audio footage from the device's microphone, • video footage of the device's screen (including all gestures/touches or mouse movements and clicks performed on the device) and tester's face Note: • Following advice from the privacy and data protection team, 2CV instructed participants to use a fake first name and email address when registering with Lookback, update their device name to a fake name before starting the user testing to minimise the personal information collected. • IP address is required by Lookback so that they can debug errors and improve the service. • We recorded 2 hour maximum of footage for each participant, 1 hour on the first day of the study and another 1 hour after 1 week to terminate the marketing study. • It is optional for testers to share the front facing camera to capture their face. It is standard practice in a marketing study to observe the participant, in user testing this includes recording the screen and the face of the participant. This is to allow the researcher/us to capture unfiltered user reaction on the app features. This is a standard technique to probe the truthfulness of what the user says. For example, someone can use a feature and say that they like it but show boredom and little or no interest, researchers can gather this by observing their face expression/tone of voice more than their words. Testers can choose whether to share the front facing camera to capture their face on Lookback, without obligation, although it is useful for insights on the usability and appeal of the features in the TfL Go app. 2CV obtained testers' consent to collect the personal information above through the screener questionnaire. When using Lookback, sessions cannot be started automatically, participants always have to explicitly enable screen sharing, microphone sharing and camera sharing before a session can start. 2CV stores and processes personal information collected on the questionnaire on servers in Amsterdam. Lookback (the tool that 2CV uses) stores and processes personal information collected via the Lookback app in Ireland. Lookback uses a US hosted analytics service connected to Lookback's data warehouse in Ireland, so data is not duplicated into the US, but it's used in that service. The Privacy and Data Protection team is carrying out a review of 2CV and their tools separately.

	TfL, 2CV and Lookback grant access to personal information processed on a business need-to-know basis, similar to the Alpha trial. TfL project team only have access to first name, audio/video footage collected via Lookback and do not have access to the information on the screener questionnaire. 2CV will provide a report to the TfL Go project team with aggregated data which does not contain personal information. The report from 2CV will be analysed in context against other user testing sessions, but the data will not be used or combined with other datasets. The Go project team will delete any trialist information 1 month after the trials are completed, except for those who have agreed for us to keep their information on file for use in future trials. 2CV will be requested to delete any trialist information 1 month after the testing is completed, except for those who have agreed for us to keep their information to notify them of future trials or for 2CV to use their information for other purposes. TestFlight will be also used to test the external user testing app. When testing apps with TestFlight, Apple will collect and send crash logs, users' name and email address, usage information and any feedback users submit to the developer through the app (not including information emailed to the developer directly) to improve their products and services. **Usage data** Usage data is information about participants' use of the app. We processed usage data in the internal Beta trial and external user testing, but not in the Alpha trial. The usage data we collect in TfL Go (see below) are standard app usage fields. We collect this data in order to gain quantitative insight into how TfL Go is used, how it performs and potential areas for improvement. The insight helps us to iteratively improve the product and influences the product roadmap. For example, if analysis shows that the app is primarily accessed from outside Greater London we may prioritise Network Rail related

	developments ahead of bus data, or perhaps services for visitors to London. At the trial stages, this is valuable to work alongside the qualitative data obtained through direct feedback. Once the app is live, the data will be the primary way to measure success and understand where to focus development. This is of high value to TfL, and subsequently to users who benefit from a continually improving service. In the longer-term, the success of TfL Go should also benefit wider London society through a more efficient transport network and empowered users who can use the app to manage disruptions and minimise the knock-on impact of network issues. For internal Beta trial and external user testing participants, we asked users for their consent to share their usage data with us when the app is first launched (in one of the onboarding screens) and they can withdraw or change their consent in app settings at any time. Additional details about how we process usage data is included in the privacy notice embedded in the app (accessible on the onboarding screen and in app settings). If participants have given consent, we will use Adobe Analytics tags embedded in TfL Go (a technology similar to cookies) to collect their usage data, which includes: • Device type, model and OS • Unique ID – pseudonymised from device ID / MAC address, but providing the ability to track usage on a specific device over time • Session information – number, duration, time/date, location (mapped to a region, eg London Borough) • When and where accessed (this is based on IP address and is not taken from device GPS data) • Screens viewed and interaction on screens, eg zooming and panning on the map • App interaction – including stations tapped on and journeys planned (ie stations and search terms entered into the 'to' and 'from' fields in Journey Planner, but not addresses and postcodes) • Behaviour flows (journeys through the app – eg where someone exits) • App crashes The data collected is pseudonymised. It allows for user activity to be tracked over time, by collecting activity completed against a consistent device ID. We need to know a specific user's behaviour changes over time.

	However, it is not about tracking specific journeys made/planned, rather the fact they have planned journeys at all, at what time, frequency, etc. TfL has no way to identify an individual from the Adobe Analytics data or insight, and we have no ability to directly interrogate the data against a device ID (eg run a report for all journey planner searches for device ID 123456). We can only view usage data in aggregate form. However, due to the small number of people involved in parts of the trial, it is possible that we may be able to infer a certain user's behaviour. TfL may be able to identify a user if this individual provides enough details of his/her usage data, however, TfL does not intend to ask for any usage data details from users to try and identify them. The risk is low as Adobe analytics will only be used to capture stations (but not addresses or postcodes) entered into the 'to' and from 'fields' in the Journey Planner, the number of people with access to Adobe Analytics is small and the team will only look at app usage patterns, not travel behaviours. The usage data is stored and processed on Adobe Analytics' platform in the UK. Usage data is automatically deleted by Adobe on a 36 month rolling basis. Adobe Analytics is the analytics platform used across TfL's digital products. Through Adobe Analytics, TfL can understand the user's use of different digital products (eg the website, TfL Go, Oyster ticketing app). This data combination is managed by Adobe, and TfL cannot identify an individual from this data. TfL access data via an online reporting portal, with no way of accessing directly identifiable information. A separate DPIA is in development for Adobe Analytics. • **Location data** In Alpha, internal Beta trials and external user testing, TfL Go used the device 'Location Services' to offer an optimum in-app experience to users and location data is provided by iOS Location Services. If participants allow TfL Go to access their location data, we will use it to tailor their experience, for example: • To show them where they are in the tube map,

- To show them where they are and walking directions in the geographic map,
- To make it easier for them to use the journey planner, for example, we will use their current location as the “from” location automatically and they can tap on a station to get the best routes from their current location.

If participants choose not to allow TfL Go to access their location data, they won’t be able to use features that are based on location data - they won’t see where they are in the maps and they need to enter their “from” and “to” location manually when using the journey planner. But they can still use the app, the app has logic in place to manage these features that usually rely on location, for example, the app launches to central London if the location is now known, instead of launch to their nearest station.

We asked for participants’ consent to access their location data when the app is first launched and they could change their consent for TfL Go or all apps via Location Services in device settings at any time. Additional details of how we process location data and a link to Apple’s Location Services page were provided in the privacy notice embedded within the app(accessible on the location data consent pop-up and in app settings)

The internal Beta, external user testing versions of the iOS app were only set up to support devices on iOS 11 and above, and cannot be downloaded on devices running iOS versions below this. Users had the option to allow TfL Go to access the device location data at the following levels:

- **Never** – the app cannot access Location Services, and the app defaults to a location-unaware state
- **Once only** (iOS 13 and 13+ only) – the app can access Location Services for this session only. Permission must be requested each time the app is opened
- **While using the app** – the app can access Location Services every time the app is open (whether in the foreground, or in active use in the background)

Note that TfL Go did not request the fourth level of Location Services access, ‘**At all times**’ in the Beta, external user testing, as the features available in this version of the app do not require location data while the app isn’t in use.

The Location services data use is ephemeral. We do not store any location data to the device storage at any point. Location data is only used in the app locally and no data is stored or processed on TfL servers. The most

	recent location point is held in memory (RAM) by the app to allow for users to see themselves on the maps and to plan their journeys from their current location. The location data is never stored in the app itself, although when location data is not available, the app will 'remember' which section of the Tube map was previously shown and continue to highlight that part of the map, this is not done by saving the actual location data. The location data is protected from compromise as iOS apps are sandboxed and the memory is not visible to other processes and apps running on the device. The location data was not shared with third parties or suppliers, an exception was the journey planner which requires a call to the Journey Planner engine, provided by a third party, MENTZ GmbH, under contract with TfL. If participants use the journey planner in this app, the app submits latitude and longitude for the "from" and "to" location to process their journey requests, this is required for the journey planner engine to return accurate directions. If the participant has chosen to allow TfL Go to access location data, the latitude and longitude will relate to the user's current location, but there is nothing to relate that Journey Planner call to an individual user. • The Alpha trial didn't include journey planner feature. • For the first Internal Beta app release, the "from" location in the journey planner would represent the user's location at the point of making the journey planning call, as the only option available in this version was based on starting from the device's current location. The latitude/longitude must be at an accurate/granular level to support the initial walking leg of journey plan results (ie how many minutes to the tube station, bus stop, etc). It would undermine the service delivered by the app if the location pinpointed is not precise • The second Internal Beta release introduced the option for the user to select a different start point as the "from" location in the journey planner. The data the app submited to the Journey Planner engine did not indicate where the location data comes from, so from that point onwards it would not be possible for exact location information to be derived from the Journey Planner calls. We would know in Adobe Analytics the proportion of journeys planned where the 'from' field was edited, but it would not receive the specific latitude/longitude generated by a journey plan • The external user testing: same with the second Internal Beta release.

Our journey planer engine provider will keep the “from” and “to” location in journey requests for a maximum of 48 hours.

Additional journey planner functionality within the app includes:

- In the iOS app, we are using Apple’s MapKit to show geographic maps, which is a framework for embedding map components within apps and no personal information is shared with or collected by Apple. This is not a link to Apple Maps itself. The map displayed to users will show a ‘location dot’ and walking directions, both of which are added by our app – ie the display of this is dependent on whether you have given TfL Go permission to access your location (not the settings you have arranged for the Apple Maps app). We will be exploring similar functionality for Android devices.

Integration with Google Places functionality – this is already available on the TfL website version of Journey Planner, and involves a call being made to Google when data is entered in the ‘to’ and ‘from’ fields. An autocomplete feature is initiated which provides options to the user from the Google Places dataset. A separate DPIA will be completed for Journey Planner, with a more detailed explanation of Google Places within that. However, it is important to note in this context that a user’s phone will not speak directly with Google when a search is being carried out. The request is passed to TfL’s own API, which then forwards the request to Google. This means that users’ IP address, latitude and longitude coordinates and data about the type of device making a search will not be passed to Google. For Google to be able to charge us for use of this service for each search a session token ID is assigned – this is a random string which identifies an autocomplete session for billing purpose, it’s only linked to one complete search and is not reused should the same device complete a new search. To provide predictions for the search terms you entered into the Journey Planner, your search terms and a session token ID will be passed to Google. Google collect users’ search terms and may use this data to provide and improve Google products and services. For more information about how Google handles users’ personal information, please see Google’s Privacy Policy.

Feedback:

We collected participants’ feedback to fix problems they reported and reply to their communications. We will also use their feedback to identify areas for improvement.

The key benefit for TfL in running trials of TfL Go is that this is an opportunity to test the app and identify key

	improvements that can be made prior to launch, or form part of a post-launch roadmap. Participants' feedback helps TfL to identify areas for improvement and this in turn benefits future app users by ensuring the design has been well thought through. Participants could provide feedback in two ways: • Users could provide feedback via an email link in the TfL Go app. The email link would open the email client on the user's device, so it was possible that the feedback email could come from their personal email address rather than their TfL one for Alpha and internal Beta participants. If users were not comfortable with using their personal email address, they could copy the feedback email address from their personal email client and paste into their TfL email to provide feedback. • Users also had the option to provide feedback to the developer directly within the app. This could be anonymous or can include user name, depending on how they have signed up for TestFlight. The feedback emails and messages were sent to a dedicated TfL Go inbox and only a small number of TfL Go project team members have access to it. The feedback emails and messages are stored and processed in the UK. Feedback emails will be kept for 3 years and the Contact Centre will delete them after the retention period. Feedback submitted within the app directly will be deleted after the public launch of the app by the Go project team.

Step 3: Describe the scope of the processing

Who does the data relate to? How many individuals are affected? Does it involve children or vulnerable groups? If children's data is collected and used, are they aged under 13? What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*) Specify which special category data or criminal offence data are to be processed? Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data? How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process? Is the data limited to a specific location, group of individuals or geographical area?	See step 1 and step 2.

Step 4: Describe the context of the processing

Is there a statutory basis or requirement for this activity? What is the nature of TfL's relationship with the individuals? *(For example, the individual has an oyster card and an online contactless and oyster account.)* How much control will individuals have over the use of their data? Would they expect you to use their data in this way? Are there prior concerns over this type of processing or security flaws? Is it novel in any way, or are there examples of other organisations taking similar steps? What is the current state of technology in this area? Are there any security risks? Are there any current issues of public concern that you should factor in? Are you or your delivery partner signed up to any code of conduct or certification scheme?	For the Alpha, internal Beta trials and external user testing, the user explicitly chose to take part in the TfL Go trial; they have provided consent via the recruitment and onboarding process (privacy notice and permission modal drafted with support from the Privacy and Data Protection team) and thus would expect us to use their data in the way described. Any user not wishing to share data with TfL in this way could choose not to be a part of the trial. Once the TfL Go app is publicly released, they will be able to download the app with more control over their data. One risk during the internal Beta trials was that the relatively small number of active app users may have made it possible to identify an individual user's travel patterns from Adobe Analytics usage data. However, we had no way to attribute that user's travel back to a particular individual – for example, we may have been able to see that one user regularly plans a journey from station A to station B, but we won't have known who that user was as we did not collect address as part of the trialist recruitment. The risk of identification from this data potentially increases if friends and family of staff with access to the Adobe Analytics dataset took part in the External user testing. To mitigate this risk it was decided that details added to the 'to' and 'from' fields in Journey Planner would not be collected by Adobe Analytics. **Trialist information** The user (for the Alpha and Internal Beta trials) submitted their personal information directly to TfL when they registered their interest in taking part. As part of this process, the use and storage of their information was made clear in a privacy notice. The required information should be expected by users, as it is standard, relevant and required to recruit for and run the trial successfully. Should a volunteer or participant choose to withdraw from the trial, we would have deleted their personal data after removing them from the trial. However, any insight garnered to date would still have been kept (although without being attributable to the individual). For example, if the user completed and responded to Task one before withdrawing, we would keep the response as part of the overall results (X% successfully completed the task), or if they reported a bug with the app, we would keep the bug report – which contains details of the issue but not who raised it. 2CV are members of the Market Research Society and therefore obliged to maintain the anonymity of respondents. **Usage data** TfL uses a leading industry analytics provider, including tracking parameters that are common practice across all

	digital products. Whilst it is not expected there is any security or reputational risk in collecting this usage data a separate DPIA is in progress specifically to review use of Adobe Analytics across TfL products and services. From the Internal Beta version of TfL Go, the app included the option for a user to opt-in or out of sharing usage data with TfL on first use and to change their preference in settings. The Alpha trial did not support usage tracking so user consent was not required at this stage. **Location data** The user consented to allowing the app access to device location data via the app onboarding process – it isn't possible for the TfL Go app to access the device Location Services unless the user has consented to this through their operating system (OS) modal pop-up. Once in the app, we continue to use the single step OS modal pop-up for managing access to location data: if the TfL Go app does not have access to Location Services, when the user attempts to use a feature that requires access (such as tapping the 'locate me' button) the OS modal pop-up will be triggered. Consent could be withdrawn at any time through the device Settings. Both iOS and Android OS are introducing changes to Location Services to give the user more information about and control over the location data they share with app developers; this is something that is in line with TfL's approach to transparency. As it is a travel app, users will expect TfL Go to use Location Services to optimise the service provided. Access to Location Services is a common request within many apps, but particularly so for any that are to do with travel or events where localised information is particularly useful. We do not believe that there is any reputational risk from the TfL Go app asking for permission to access Location Services. Even though this is a common request for many apps in the marketplace, we must be as transparent with our users as possible about how we use location data. More details of how location data is processed is provided in a privacy notice embedded within the app. If updates to the app result in amendments to the privacy notice, when a user downloads the new app version it will be flagged to them that the privacy notice has been amended. **Feedback** We collected participants' feedback to fix problems reported and identify areas for improvement before the public launch or to form part of the post-launch roadmap, which will support us to fulfil our statutory functions.

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?	See Step 2.

Step 6: Consultation process

Consider how to consult with relevant stakeholders:
 	
Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.
 	
Who else do you need to involve within TfL?
 	
Have you discussed information security requirements with CSIRT?
 	
Do you plan to consult with external stakeholders? If so, who?
 	
Who will undertake the consultation?
 	
What views have been expressed by stakeholders?
	Trial participants received terms and conditions and were required to agree to these to be accepted onto the trial. These T&Cs outline the data collected and how it is processed.
	
	Internal TfL stakeholders are:
	
	• Information Governance – to ensure compliance with GDPR and PECR / ePrivacy, and to collaboratively identify the most appropriate level of data collection and processing that balances privacy considerations with business needs
	• Data & Analytics (*in regard to device data – see separate DPIA*) – responsible for the storage and processing of device data and data analysis and insights. Also, they are the interface to other TfL business areas for requirements and use cases for the data collected from the TfL Go app, including:
	  ▪ Transport Planning
	  ▪ Customer Marketing & Behaviour Change
	  ▪ Travel Demand Management
	• CSIRT – to ensure the tools used for the trials are acceptable, and the level of information security testing required at each stage of the trial.
	  ▪ Based on CSIRT advice, we used Microsoft Forms for trial participant recruitment and surveys (instead of Survey Monkey as originally intended) and they assessed the app and use of feeds before the External Beta phase, confirming that they are comfortable with the risk level
	  ▪ A pentest is not necessary at the trial stage as the app is still in development stage, the pentest would become invalid as soon as any changes are made.
	  ▪ A pentest is completed in July 2020 and CSIRT has signed off for the app for the public launch in July 2020, more details are provided in the public launch DPIA.
	  ▪ CSIRT believes the 2CV/Lookback set up for Go is suitable from a cyber security perspective
	• Customer and Revenue – to ensure that commercial considerations are understood from the outset and that decisions made for this phase do not preclude us from deriving commercial value in the future
	
	External stakeholders are:
	
	• 2CV – TfL's research partner, who managed the Alpha trial and external user testing. To ensure the online

	platform and all data collected for the trial is being processed appropriately • Apple and Google – to gather insight and tips for a best practice approach to collecting useful data while maintaining a high level of user privacy • Information Commissioner's Office (ICO) – an obligation under the GDPR is that for any DPIAs which 'result in a high risk in the absence of measures taken by the controller to mitigate the risk' we must consult with the ICO. However, we should engage with the ICO on this work, whether high risks remain or not. There is a precedent for this proactive approach to the regulator as this is something TfL did for the Wi-Fi insights pilot and rollout into business as usual. The engagement was incredibly positive for the project. The Privacy and Data Protection team first raised TfL Go with the ICO in May 2020. The initial app to be launched was discussed, as were our future plans for the collection of mobile device data. The ICO raised some areas for further consideration in these future plans that must be incorporated into the project going forward. An update prior to the August public launch will be sent to the ICO, stressing that we wish to continue to engage with them as we work towards the collection of mobile device data in future versions of the app.

Step 7: Assess necessity and proportionality	
Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals about how their data is used? What measures do you take to ensure suppliers processing personal data on our behalf provide adequate assurances about their ability to process this data safely and lawfully?	**Trialist information** For the Alpha, internal Beta trials and external user testing, we believe that the data collected is required and proportionate. We collected the minimum amount of personal information required to successfully recruit and run the trials, and will use it purely for the purposes stated, thereby avoiding function creep. If a trialist informs us of an error in the data they shared with us, we and 2CV will update our records accordingly. The processing of trialist information achieved the purpose of delivering the trials. We would not have been able to recruit or run the trials if we didn't collect the limited personal information required to (a) ensure a representative sample and (b) share the app and communicate with trialists. A privacy notice was provided to all participants in the Alpha, internal beta trial and external user testing. **Usage data** The processing of usage data achieved our purpose as it provided valuable insight that is required to deliver an effective product. There is no other practical way to gain quantitative insight into how the app is used, other than by implementing usage tracking. The scope is understood, and uses tags implemented in the app to a defined specification, therefore it will not be possible for function creep to occur. Mechanisms are in place to ensure the data is aggregated to insight and doesn't allow individuals to be identified. As previously noted, use of Adobe Analytics will be the subject of a separate DPIA. Unlike many mobile apps, we were transparent about the collection of usage tracking data and give users the option to opt-in or out of this (and still be able to use the app if they do not opt-in). **Location data** The local processing of Location Services data enabled us to achieve the purpose of offering a useful and relevant travel app that is optimised to the individual's current needs. There is no other way that a localised service can be offered; hence users who opt not to share location data with the app will receive a more generic service. As part of the onboarding process and consent OS modal pop-up, the app will provide the user with a short description of why the Location Services data is required for an optimal service. We are clear that the long-term scope of location data includes the option for users to share this data (and other device data) with TfL for server-side processing; however, at this stage of the product development, it isn't

	possible for function creep as the location data is used locally on the device (eg to place a user on the tube map) and for the specific action of journey planning. The app will use the standard Location Services data, which is available to apps where the user has consented; we assume that this meets the data quality and data minimisation requirements at the OS level. **Feedback:** The processing of feedback enabled us to achieve the purpose of fixing problems with the app and identifying areas of improvement for the app. This is the most efficient way to obtain feedback from participants. All feedback was collected anonymously. Reports, statistics and insight generated from the trial will not include any personal details that allow an individual participant to be identified. We have been transparent about the collection of feedback in the privacy notice.

To be completed by Privacy & Data Protection team What is the lawful basis for processing? How will data subjects exercise their rights? How do we safeguard any international transfers? Could data minimisation or pseudonymisation be applied? Are data sharing arrangements adequate?	The lawful basis of processing: • The lawful basis for processing trialist information is consent. Participants have provided consent in the recruitment and onboarding process. Any users who do not wish to share data with TfL in this way can choose not to participate in the trials. Participants can withdraw from the trials by contacting the Go project team, the Go project team will remove them from the trials and delete their data. • The lawful basis for processing usage data is consent. For internal Beta and external user testing, we ask for users' consent to share their usage data with us when the app is first launched and they can withdraw or change their consent in app settings at any time. • The lawful basis for processing location data is consent. We ask users for their consent to access their location data when the app is first launched and if the app does not have consent to access location data - when the user attempts to use a feature that requires access to location data, such as tapping the 'locate me' button. Participants can change their consent via Location Services in device settings at any time. • The lawful basis for processing feedback is to perform tasks in support of our statutory functions to undertake activities to promote and encourage safe, integrated, efficient and economic transport facilities and services, and to deliver the Mayor's Transport Strategy. Participants can exercise their information rights with TfL under existing processes. Personal data will be stored and processed within the EEA. TfL and 2CV's questionnaires are designed to collect the minimum amount of personal data required for the project objectives. Participants in the external user testing will be instructed to use fake name, email address and update their device name to a fake name to minimise the personal data processed. The Location services data use is ephemeral. We do not store any location data to the device storage at any point. Location data is only used in the app locally and no data is stored or processed on TfL servers. The most recent location point is held in memory (RAM) by the app to allow for users to see themselves on the maps and to plan their journeys from their current location. This is the minimum data access that can be used to deliver the app objective.

	The Go project team has applied data minimisation principles when collecting usage data and feedback, The app usage data standard app usage fields necessary to achieve the purpose for this project and feedback emails and feedback submitted in the app only collects the information necessary for the purpose for this project above. We use third party service providers to process trialist information, usage data and Journey Planner search requests, see more details in Step 2.

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 probably	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
1.Where participant numbers are small, there is a potential to identify individuals from usage data collected	Possible	Significant	Medium
2. Currently there is no established process to extract and delete app usage data	Probably	Significant	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
1. Where participant numbers are small, there is a potential to identify individuals from usage data collected	Adobe Analytics will only be used to capture stations (but not addresses or postcodes) entered in the 'from' and 'to' fields in Journey Planner. The number of staff who have access to Adobe Analytics is small and they will only look at app usage patterns, not travel behaviours. TfL may be able to identify a participant if this individual provides enough details of his/her usage data, however, TfL will not ask for any usage data details from participants to try and identify them.	Reduced	Low	Yes
2. There is no established process to extract and delete app usage data to respond to data subject right requests	TfL Privacy and Data Protection team is carrying out a separate DPIA on Adobe analytics, which will review options to extract and delete app usage data.	Reduced	Low-Medium	Yes

Step 10: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Richard Bevins	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Richard Bevins	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:	Recommendations in Step 9 to be implemented by the Go project team.	
DPO Comments:	These recommendations are necessary for risk mitigation. This DPIA has been invaluable for progressing TfL Go to public launch	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):	Accepted	If overruled, you must explain your reasons below.
Comments: Feedback reviewed and implemented		
Consultation responses reviewed by:	Jacob Uzzell Chloe Davies	If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:	The Go project team, the Privacy and Data Protection team	The DPO may also review ongoing compliance with DPIA.

Glossary of terms

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

	• when deciding whether to share or make use of information, you must consider whether using all information held about an individual is necessary for the purpose. Disclosing too much information about an individual may be a personal data breach. When deciding how long to keep information, you must consider what records you will need, and whether some personal data can be deleted or anonymised.
Data Protection Rights	The GDPR provides the following rights for individuals: • The right to be informed; • The right of access; • The right to rectification; • The right to erasure; • The right to restrict processing; • The right to data portability; • The right to object; • Rights in relation to automated decision making and profiling.
Data quality	The GDPR requires that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*." This means you must take steps to ensure that the data you use is sufficiently accurate, up to date and comprehensive for your purposes, and that you take steps to effectively mitigate any detriment to individuals that is likely to result from inadequate data.
Function creep	Function creep describes the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Review and update your DPIA, or undertake a new DPIA to reflect changes in the purpose or the means by which you process personal data.
Genetic data	Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
Marketing	Direct marketing is “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations. Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects

	details to use in future marketing campaigns, the survey is for direct marketing purposes and the privacy regulations apply. Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the privacy regulations apply.
Personal data	Personal data is information, in any format, which relates to an identifiable living individual. Personal data means any information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The definition can also include pseudonymised data (where we hold data that has had the personal identifiers replaced with codenames); depending on how difficult it would be to re-identify the individual.
Privacy notice	A privacy notice must let people know who we are, what we intend to do with their personal information, for what purpose and who it will be shared with or disclosed to. TfL adopts a layered approach to privacy notices, with clear links to further information about: • Whether the information will be transferred overseas; • How long we intend to keep their personal information: • The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information; • The name and contact details of the Data Protection Officer; • The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner;

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