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:	Digital, Technology & Data Privacy and Data Protection, Information Governance	Date DPIA updated	2 December 2020
		Proposed launch date	8 December2020

Name and description of the project:	**TfL Go – public launch** TfL Go is a new, location aware, mobile application providing travel support to users. In advance of a public launch, TfL ran trials with a small number of people. Those trials are the subject of a separate DPIA. The launch of TfL Go had been impacted by the COVID-19 pandemic, with uncertainty over the public launch date. However, from June 2020 Digital proposed the accelerated public launch of the iOS app. The reason for acceleration is that the app will support key COVID-19 'restart' priorities – for example enhanced service information, and the promotion of walking and cycling routes. The Android app will be launched in December 2020.				
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.	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.	X	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.	X	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.	X
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. *A separate DPIA is to be completed to consider the intention for future versions of the app to deliver personalisation and specifically the collection of mobile device data.* The iOS app was launched in August 2020 and the Android app will be launched in December 2020. Launch activities will include: • Press communications • Coverage on TfL blogs • Social media posts • Engagement with external stakeholders • Internal communications • Customer email communications The app will be available within the Apple App Store and Google Play store for anyone to download. The first public release will focus primarily on the tube network and be built around the tube map, with inclusion of bus arrival information and walking and cycling routes. It will include the following features: • A data-driven, interactive tube map, including a step free map view, and live service status updates, such as notification of closed stations and lines (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, including walking routes and basic cycling routes (personal data processed – location data and intended destination data, ie journey plans) ○ Not anticipated for the initial public launch, but scheduled for soon after, will be the inclusion of live bus arrival times, cycle hire routes and promotion (with links to hire via Santander Cycles app/website)

	• COVID-19 messaging – a dismissible alert shown on the tube map that allows a user to link through to content promoting the latest travel advice and providing live updates on station busy-ness (no personal data required) • 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 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, for example ○ 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*). *A separate DPIA will be completed, if necessary, 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) • Display of crowding information on station stop pages to encourage travel outside peak times, for example detailing peak times for a specific station (no personal data required) • General interface improvements will also happen on a continuous basis – for example covering general tweaks to existing functionality that won't have material impact on the core functionality itself • Nearby bus stops – this will provide information on bus stops near users' current location and the full stop view, which will show all buses and where users are on a geographic map. This feature is currently only available in the iOS app and will be added to the Android app later. 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 this 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 inform of functionality updates at an early stage. In the future 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 for TfL Go have been shared with the Privacy team for reference. The personal data processed as part of this project falls into the following principal categories (see more details in Step 3): 1. App usage data 2. Location data 3. Feedback data This DPIA, and the previous TfL Go trials DPIA, allow us to assess the privacy considerations and risks involved in this processing. Given the public awareness of mobile apps, location data and privacy we are planning on publishing this assessment to support our transparency responsibilities. **ICO Age Appropriate Design Code** We have referred to the ICO Age Appropriate Design Code during preparation of this DPIA, as it has been identified that the app is a 'relevant Information Society Service' and is 'likely' to be accessed by children – ie those under the age of 18. Whilst at the time of completion of this DPIA the code is not yet in full effect, we have used the current published version as a reference point. TfL Go is not aimed directly at children, nor has it been directly designed for them. It has been designed for all travellers on the TfL network. However, it would not be inappropriate for a child to use the app, with app functionality that could be helpful for under-18-year olds travelling on the TfL network. We will refer to our responsibilities towards children using the app throughout this DPIA, and then specifically within step 8. The Code supports a risk-based and proportionate approach to implementation of the standards contained within it. At this stage in the DPIA it is helpful to outline our view that TfL Go (in its current form) poses a low risk to children using it in terms of the potential impact on them and any harm or damage the processing may cause. It is our anticipation that the DPIA highlights this throughout, but we reflect below on a few reasons for this

	opinion here:
	• Limited data collection, with location data for example being processed primarily on the app itself
	• No external sharing of data with other data controllers
	• The proposed app functionality would not appear to cause concern of the following:
	  ○ Physical harm
	  ○ Online grooming or other sexual exploitation
	  ○ Social anxiety, self-esteem issues, bullying or peer pressure
	  ○ Access to harmful or inappropriate content
	  ○ Misinformation or undue restriction on information
	  ○ Encouraging excessive risk-taking or unhealthy behaviour
	  ○ Undermining parental authority or responsibility
	  ○ Loss of autonomy or rights (including control over data)
	• Concerns could be raised in relation to the following, however the proposed app functionality and intended data usage seems unlikely to pose substantial risks:
	  ○ Compulsive use or attention deficit disorders
	  ○ Excessive screen time
	  ○ Interrupted or inadequate sleep patterns
	  ○ Economic exploitation or unfair commercial pressure – it is particularly hard to envision how this would be a risk. You cannot carry out transactions in the app with financial implications, and there are no current plans to display advertising within the app

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.	**App usage information** This data is pseudonymised, so we will not be able to identify an individual from it, and as the volume of people using the app rises the risk of determining any travel patterns would reduce. Adobe Analytics is the app analytics platform used across TfL's digital products. *A separate DPIA will be prepared to look specifically at this platform.* We have a contract in place with Adobe for the delivery of this service, which covers use of the tool on the TfL website also. Adobe Analytics helps to understand customer behaviour and app performance. The insight helps us to iteratively improve TfL Go 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. Data is collected via Adobe Analytics tags embedded in the TfL Go app. The data is sent to, stored and processed by Adobe. The TfL Go tagging specification document has been shared with the Privacy team. 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. Only specific people within two Technology & Data (T&D) teams have access to the reports and aggregated outputs. These two teams are T&D Digital and T&D Online Development. When users launch the app for the first time, they will be made aware of the plan to collect app usage data, the purpose for collecting this data and provided with the option to accept or decline in the app. As we are relying on consent as our 'legal basis' for the collection of this data, and we have identified that children are likely to access the app, we have taken steps to meet the obligations of Article 8 of the GDPR. We have incorporated a message targeted at individuals under the age of 13 as part of this process. We direct them to speak with their parent or guardian to assist with making the decision of whether to accept or decline the collection of usage data. The appropriateness of this approach will be referred to in step 8. This opt-in stage will form part of the first time use on-boarding sequence in the app, and the participant can change their preferences at any time via the app settings. Additional detail about Adobe Analytics is also included in the privacy notice, published within the suite of TfL Privacy and Cookies pages. **Location data** TfL Go uses user's location data to offer an optimum in-app experience to users.

	This data is provided by Apple's location services , Google's location services and device location; If users allow TfL Go to access their location data, the TfL Go app will use location data locally in the app to show users' current location on the tube map, to show them where they are and walking directions in the geographic map, to autofill in the 'from' location on the journey planner which makes it quicker to plan a journey and to show them bus stops nearby, if users tap on a bus stop, it will also show them the full stop view with all buses and where they are on the geographic map. There is no server-side processing of this data and location data will not be shared with third parties or suppliers. Some users can also control the accuracy level of location data TfL Go can use. iOS users (iOS 14 and 14+) can do so by managing their preference for Precise Location when we ask for their permission to access location data and in their device settings. Android users can do so by managing their preference for Location Accuracy (Android 9 and 9+) or Mode (Android 8) in their device settings. An exception is the Journey Planning feature, which requires a call to the Journey Planner engine, provided by a third party, MENTZ GmbH, under contract to TfL. The app submits latitude/longitude for the start and end points of the journey request; this is required for the engine to return accurate directions. The latitude/longitude could relate to the user's current location, but there is nothing to relate that Journey Planner call to an individual user. 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 data the app submits to the Journey Planner engine does not indicate where the location data comes from (eg from selecting to plan from current location or to select another location), so it will not be possible for exact location information to be derived from the Journey Planner calls. We will know in Adobe Analytics the proportion of journeys planned where the 'from' field was edited, but it will not receive the specific latitude/longitude generated by a journey plan. 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). In the Android app, we use Google Map to show geographic maps and won't share personal information with Google in this process. • 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.* 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 purposes, it's only linked to one complete search and is not reused should the same device complete a new search. 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, see Google's Privacy Policy **User Feedback** We collected users' 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 is that users' 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. 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 the feedback email could come from their personal email address. The feedback emails are sent to a dedicated TfL Go inbox, only the TfL Contact Centre and a small number of TfL Go project team members have access to it. The feedback emails 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.

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?	**Who will be using the app?** The data collected (or processed directly on the device) relates to individuals that choose to download the TfL Go app. It may involve users that are children or from vulnerable groups, however TfL will have no way of directly identifying (with certainty) that this is the case. Whilst we cannot state with certainty how many users will download the app, we have carried out some analysis on this. Taking into consideration the impact of the COVID-19 pandemic, we have an assumed figure of 250,000 downloads of the app by December 2020. As discussed earlier in this DPIA it is felt that the app is 'likely' to be accessed by children in regard to the parameters of the ICO Age Appropriate Design Code. We have reviewed the age ranges proposed by the Code and feel it is most likely that use would begin during the range of 10-12 (ie the 'transition years'), and continue with 13-15 and 16-17 (the 'early teens' and 'approaching adulthood' age ranges respectively). The Code itself states that children in the age range of 10-12 are likely to see a change in their online activity and transition from primary to secondary school means children are more likely to have their own personal device (predominantly smart phones). A 2019 Ofcom report (Children and parents: Media use and attitudes) found that half of 10 year olds now own their own smartphone, with ownership doubling between the ages of 9 and 10. They cite this as 'an important milestone in children's digital independence as they prepare for secondary school'. Whilst we feel it most likely that use would begin during the 'transition years', we recognise there is a chance that children below the age of 10 could access the app. However, we refer to step 1 and our view that TfL Go (in its current form) poses a low risk to children using it in terms of the potential impact on them and any harm or damage the processing may cause. We have previously considered restricting use of the app to those aged 13 and over, however it was not felt fair to restrict an app that may have legitimate uses for those under 13. The level of possible harm also does not warrant such a restriction. However, users' use of the app is subject to Apple or Google's rules and policies (including age requirements). The data being processed, for this version of the app, is not limited to a specific location, group of individuals or geographical area. Whilst the app itself supports travel on the TfL network (ie within the London area) there is no restriction on use of the app only being within London. **Usage data** When app users launch TfL Go for the first time, they will have the option to accept or decline the collection of usage data within the app. The selected choice will be reflected in the 'Settings' section of the app, from where

	the participant can change it at any time. A full breakdown of usage data collected is held in separate documents (made available to the Privacy team), but it 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 (eg stations and Google Places selected) • Behaviour flows (journeys through the app – eg where someone exits) • App crashes The above are all standard app usage fields, required to help TfL to understand how the app is being used and where there are opportunities to improve it. 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 be able to track a specific user to see how 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. TfL may be able to identify a user if this individual provides enough details of their usage data, however, TfL does not intend to ask for any usage data details from users to try and identify them. Data is automatically deleted by Adobe on a 36-month rolling basis. **Location data** An app user can grant permission to allow TfL Go to access their location via Apple's Location Services and Google's Location Services and device location. Users are provided a link to Apple's Location Services page and Google's Privacy policy to see more details in the privacy notice. Users' location data will be used by the app

	locally. An exception is the Journey Planning feature, which requires a call to the Journey Planner engine, provided by a third party, MENTZ GmbH, under contract to TfL. The app submits latitude/longitude for the start and end points of the journey request; this is required for the engine to return accurate directions. The 'from' and 'to' locations entered into the Journey planning feature are kept for a maximum of 48 hours. App users can alter their location permission settings by turning on or off Location Services for all apps or for the TfL Go app specifically in their device Settings. The data relates to the individual's device and its location. It affects all users who download the TfL Go app and give permission for the app using Location Services. Sharing Location Services data is optional but required to deliver certain features. This includes showing where a user is on the Tube map, showing where a user is and walking directions on the geographic map, planning a journey from their current location and showing bus stops nearby, also the full stop view with all buses and where a user is on the geographic map if the user taps on a bus stop. Users who choose not to share location data are not prevented from using the app; it 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 not known, instead of launching to the nearest station). For the accuracy level of location data, if iOS users turn off Precise Location and if Android users turn off Location Accuracy or select Mode options other than High Accuracy, these features will still work but it may impact the accuracy of location data TfL use.The app displays search history under the journey planner and users have an option to clear it right below the search history displayed. The Privacy and data protection team has requested the addition of functionality to manage preference for remembering search history, but due to the development work required and other app development work priorities, this hasn't been added to the app yet. The project team will start development work for this functionality in January 2021. Location data is only used by the app locally on the device; no data is stored or processed on TfL servers. This is the minimum data access that can be used to deliver the app objectives and it does not include any special category personal data. The Location Services data use is ephemeral. We do not store any location data to the device storage at any point. The most recent location point is held in memory (RAM) by the app to allow for users to plan journeys from their current location and to locate them on the schematic map. This 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 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 iOS app is only set up to support devices on iOS 11 and above and cannot be downloaded on devices running iOS versions below this. Users have 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 a 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) The Android app supports Android 8.0 and above. Users have the option to allow TfL Go to access their location data at the following levels: • While using the app – the app can use your location only when you're using the app • Only this time- every time you open the app, it'll ask to use your location. The app can use the setting until you close it • Deny – the app cannot use your location, even when you're using the app. Note that TfL Go will not be requesting the possible fourth level of Location Services access, '**At all times**', as the features available in this version of the app do not require location data while the app isn't in use. TfL Go won't access users' location data when it is placed in the background. **User Feedback:** see P9 in 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?	Our processing of this data relates, at least partially, to our obligations under the Greater London Authority (GLA) Act 1999. More detail of this is in included in step 7. The relationship that TfL has with the individuals is that they have downloaded the TfL Go app, which has been developed in-house by TfL. They could be individuals that travel on the transport network that TfL provides. They could also be a 'registered' customer, meaning that TfL will know some additional information about them (eg name, contact details, etc). However, for both 'registered' and 'unregistered' customers, we have no means of linking data processed by the app to a known individual. Individuals can exercise some control over the collection of this data – covered under each section below. **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 will specifically review use of Adobe Analytics across TfL products and services. The app will include 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 giving them control over the collection of this data. The opt-in process has been designed to reflect that children may access this app, and to ensure that we meet our data protection obligations in regard to requesting consent from children. We have incorporated a message targeted at individuals under the age of 13 as part of this process. We direct them to speak with their parent or guardian to assist with making the decision of whether to accept or decline the collection of usage data. **Location data** A user will be asked if they give the app permission to access their device location data via the app onboarding process – it isn't possible for the TfL Go app to access the device location data unless the user has agreed 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 going forward. If the TfL Go app does not have access to user's device location data, 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. Permission to access this data can be withdrawn at any time through the device Settings. Both iOS and Android 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 and device location to optimise the service provided. Access to Location Services and device location is a common request within many apps, but particularly so for any that are to do with travel or events where local information is particularly useful. We do not believe that there is any reputational risk from the TfL Go app asking for permission to access this location data. 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. The Privacy team will be working with the project team to ensure key messages are included in the privacy notice and messages embedded in the app itself. 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. CSIRT (Cyber Security and Incident Response team) completed a review of the app at the trial stage and did not identify any security risks. Ahead of iOS public launch an external company carried out a penetration test of the app for a full evaluation of risks. No high risk concerns were identified and CSIRT signed off the app for launch. There were some low risk concerns identified which will be resolved after launch. For the Android launch, CSIRT required one risk to be fixed before go live and this has been done, The remaining risk items will be fixed post launch and these have been added to the development back log. There is a plan to have another round of PEN testing for both apps to confirm the remaining risks have been mitigated. Our approach to this data processing has kept areas of public concern as a focus. For example, concerns that an individual's personal data is being misused or is not transparently used. There is currently a heightened profile for the role of data ethics in the implementation of personal data processing solutions, and in addressing issues of public concern we have kept ethical considerations to the fore. The design of this solution has been strongly challenged throughout development and will continue to be so as use and development progresses. We are also conscious that releasing an app during the COVID-19 pandemic, and one that supports 'restart' of the transport network, is done so within a context of public concern for the security of data and clear use purposes within 'track and trace' apps. **Feedback** We collected users' feedback to fix problems reported and identify areas for improvement 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?	We are launching this app in order to provide travel support to users, in a way that we have previously only been able to do directly on our website. It is being launched in August 2020 with an additional aim to that expected in the app's initial inception – to support key COVID-19 'restart' priorities. This includes providing enhanced service information, and promotion of walking and cycling routes. It should be noted that regarding children using the app, there are no specific intended effects for them alone. The intended achievement and effects are the same for all app users. **Usage data** The purpose of collecting and processing usage data is to gain quantitative insight into how the TfL Go app is used, and how it performs. This can be assessed alongside any qualitative data obtained through direct feedback channels. This 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. **Location data** The purpose of using location data is to provide an optimum service to users. The individual benefits from a number of location-based features above, such as showing where they are on the tube map. The benefit to TfL is to provide the greatest chance of the product succeeding – a travel app which doesn't offer localised services is unlikely to succeed in the current market. 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. **User Feedback** 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?
	There have been 5 sets of defined user research/consultations, along with ongoing informal testing within the Digital and development teams:
	
	<u>Ethnographic study with 8 mobility impaired customers in October 2018</u>
	
	This study resulted in usability feedback on the prototype, feature suggestions and further context on how users would expect to discover and use the app.
	
	<u>An Alpha study with 99 TfL employees in July 2019</u>
	
	Provided quantitative feedback on usability, future feature requests and proposition.
	
	<u>A marketing focus group with 24 customers in June/July 2019</u>
	
	In depth discussion on the marketing proposition, testing three concepts and how TfL Go would fit into the existing set of available apps.
	
	<u>Beta testing with 24 customers in March 2020</u>
	
	Further usability testing with the updated version of the app, focusing on journey planning and overall app navigation.
	
	<u>Beta testing with mobility impaired and visually impaired persons in July 2020</u>
	
	Exploring how the current features and device accessibility implementation works for users and what features in the future would be useful.
	
	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
	
	• CSIRT – to ensure the app incorporates the appropriate security controls and that the level of information security testing required is implemented
	
	  ○ They have previously assessed the app and use of feeds before any external testing took place, confirming that they were comfortable with the risk level
	
	  ○ A pentest was not considered necessary at the trial stage as the app was still in development. The

	pentest would have become invalid as soon as any further changes were made. A pentest for the iOS app was completed in July and a pentest for the android app was completed in November ○ CSIRT have signed off the iOS and Android app for launch • Data & Analytics – to support the display of crowding information on station stop pages. They will also be involved in the apps longer-term vision to become 'your personal travel assistant' with the collection of mobile device data to support the delivery of direct customer benefits and aggregated business insight • Customer Services – engagement will take place with Customer Services to ensure Contact Centre agents are equipped to respond to any app-related queries they receive • Press Office – to prepare a press release and reactive lines to take for queries received • Communications – to prepare a communications plan ahead of public launch • Legal – to support development of the app terms & conditions and any patent applications to be made • Customer and Revenue – to ensure that commercial considerations are understood from the outset and that decisions made now do not preclude us from deriving commercial value in the future External stakeholders are: • Apple – to gather insight and tips for a best practice approach to collecting useful data while maintaining a high level of user privacy • Google – as above, for the Android platform • 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 have (and will continue to) 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 Wi-Fi insights 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?	Information about how individual's data is being processed will be provided to app users within: • A privacy notice in the suite of TfL Privacy and Cookies webpages. The privacy notice will be linked to from within the app • Information available on pop-up screens when setting app usage and location settings – these have been designed to be concise and in a clear language. The privacy team has provided updates to the iOS location data permission modal based on the new nearby bus stops feature and TfL's research findings in desktop research and expert interviews that users feel a sense of control and are more likely to share their location data if there are clear user benefits and explanation for the purpose of sharing location data. The update hasn't gone into the latest iOS release due to other app development work priorities but it will be implemented as soon as possible. The Android location data permission modal doesn't incorporate information on purpose and user benefit for sharing location, but users can access this information in TfL's Privacy and Cookies webpages on TfL Go, a link to this page is also available in the app settings. The app is designed to be inclusive and simple to use. This means that it is likely that children would also be able to use the app. When installing the app for the first time, the app asks the user whether they would consent to sharing usage data. There is equal visual prominence to a line of text that states: 'If you are under 13, ask your parent or guardian to answer this question for you.' This guides any children who have downloaded the app without parental/guardian supervision to ask an adult who is able to consent to answer that question. The privacy and cookies page on TfL Go also tells users that their use of the app is subject to Apple and Googles' rules and policies (including age requirements) and advises children that if there is anything they don't understand, they should talk to a trusted adult such as their parent or guardian and ask them for help. The TfL Go app has considered privacy issues throughout development, including ensuring that data minimisation is a focus. **Usage data** The processing of usage data will achieve our purpose as it provides 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.* We are clear 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 (ie within the app itself) of Location Services data enables 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 the OS modal pop-up will display, providing 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 only (eg to place a user on the tube map, on map showing a walking route, etc) 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 given their permission at an OS level. **User 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 users. All feedback was collected anonymously. Reports, statistics and insight generated will not include any personal details that allow an individual 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?	We are relying on two lawful bases for processing: • For the processing of location data, we are relying on Article 6(1)(e) of the 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" • For the processing of usage data, we are relying on Article 6(1)(a) of the GDPR – "The data subject has given consent to the processing of his or her personal data for one or more specific purposes" • For the processing of user feedback, we are relying on Article 6(1)(e) of the GDPR , the processing is necessary for the performance of 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. Regarding processing of location data, our public task relates to our obligations under the Greater London Authority (GLA) Act 1999. This gives us powers to undertake activities to promote and encourage safe, integrated, efficient and economic transport facilities and services, and to deliver the Mayor's Transport Strategy. 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. Data subjects (ie app users) will be able to exercise their information rights with TfL in accordance with existing processes. There are no international transfers taking place. Data minimisation principles have been applied and data will be limited to that needed to achieve the objectives of the app. Data minimisation will continue to be a focus as developments occur and new app versions are published. We use third party service providers to process usage data and Journey Planner search requests, see more details above.

Step 8: Age Appropriate Design Code	
Describe how compliance with the age appropriate design code has been considered. Including explaining what specific measures have been taken to meet each of the standards in the code, where applicable.	We have referred where appropriate throughout this DPIA to the processing of data relating to children. This section however is a brief summary referring to each standard from the Age Appropriate Design Code. 1. Best interests of the child – the Code requires us to put the best interests of the child first. Nonetheless, we would propose that by taking a clear 'privacy by design' approach we have put the best interests of all app users first 2. Data protection impact assessments – we have completed a DPIA in advance of public launch 3. Age appropriate application – we haven't felt it appropriate to single out the specific age ranges as stated in the Code, rather to identify that we think age 10+ is the most likely age from which the app will be accessed. We have then proposed that we largely take the same approach to all app users. This is with one exception, regarding the obtaining of consent for the collection of usage data, in order that we comply with our obligations under Article 8 of the GDPR. We realise that our chosen method of asking the individual to speak with their parent or guardian could be circumvented, however given the privacy protections built into the app we feel this would result in a low risk 4. Transparency – a privacy notice for the app is hosted on the TfL website, alongside other privacy notices for TfL services. It is linked on the initial data usage consent screen, as well as in the app settings menu. It is also available by searching on the TfL website. Within the privacy notice reference is made to speaking with a parent or guardian if there is anything they do not understand within the app or the privacy notice 5. Detrimental use of data – we cannot see any immediate reason as to how our processing activities would be detrimental to the wellbeing of any children accessing TfL Go 6. Policies and community standards – through regular review we will work to ensure that we uphold our own published terms, policies and community standards 7. Default settings – our privacy settings are 'high privacy' for all app users 8. Data minimisation – the principle of data minimisation has been applied throughout and will continue to be so as the app is further developed 9. Data sharing – there are no current data sharing requirements 10. Geolocation – for the app to function at its full capacity, location-awareness is an essential component. However, owing to the privacy controls embedded within Apple devices, sharing of location data with the app is switched off by default until the device user grants permission. If permission is granted steps have been taken within the app to *remind* users when location is being used – for example showing a blue dot pinpointing

	location on maps embedded in the app 11. Parental controls – we have decided that parental controls within the app itself (as described in the code) are not necessary within this current version of the app 12. Profiling – this is not applicable for this version of the app 13. Nudge techniques – we have reviewed any app pop-up screens (ie opting in to sharing app usage data and sharing location) to ensure we are not implementing any inappropriate nudge techniques 14. Connected toys and devices – this standard is not applicable for the TfL Go app 15. Online tools – we do not feel that it has been necessary, in this stage of the app's development, to design specific tools to support the exercise of data protection rights. Within the app itself there is a way to directly provide TfL with feedback via an email address, and information rights are referred to within our privacy notice

Step 9: Identify and assess risks			
Describe source of risk and nature of potential impact on individuals. Include risks of damage or distress as well as associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
1.If the app is only downloaded by a very small number of users, there is a potential to identify individuals from usage data collected	Remote	Significant	Low
2. App updates – app functionality could be added which changes the privacy considerations of app usage	Possible	Significant	Medium
3. Currently there is no established process to extract and delete app usage data	Possible	Significant	Medium
4. A child under the age of 13 could opt-in to usage data collection without parental/guardian consultation	Possible	Minimal	Low
5. Given the app release has been accelerated to support COVID-19 ‘restart’ priorities we could face concern that appropriate privacy by	Probable	Significant	Medium

design measures have not been considered or documented			
6. Due to the development work required and other app development work priorities, the requested functionality to manage preference for remembering search history hasn't gone into the app yet.	Probable	Significant	Medium
7. Due to other app development work priorities, the requested update to iOS location permission modal hasn't gone into the recent iOS release yet.	Probable	Minimal	Low
8. The Android Location permission modal doesn't allow incorporating information on purpose and benefit for sharing location data.	Probable	Minimal	Low

Step 10: 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. If the app is only downloaded by a very small number of users, there is a potential to identify individuals from usage data collected	Access controls applied, so only minimal amount of staff have access to usage data. Staff trained on privacy compliance and concerns discussed with Privacy and Data Protection team. Adobe Analytics will not collect postcodes and addresses entered in the 'to' and 'from' fields of Journey Planner	Reduced	Low	Yes
2. App updates – functionality could be added which changes the privacy considerations of app usage	Continuous engagement with the Privacy and Data Protection team as updates are proposed – either amending this DPIA or updating a separate 'risk and mitigation log'. Prompts always provided to app users if updates have privacy considerations	Reduced	Medium	Yes

3. Currently there is no established process to extract and delete app usage data	TfL Go project team to investigate the feasibility of extracting and deleting app usage data, with support from Privacy and Data Protection team. It should be noted that previous investigations have shown that data held by Adobe Analytics is not used for the identification of individuals, with controls in place to limit the risk of re-identification	Reduced	Low-Medium	Yes
4. A child under the age of 13 could opt-in to usage data collection without parental/guardian consultation	We have included a request to seek parental/guardian support in responding to the request for usage data. We have identified this as appropriate to the level of risk that an individual under the age of 13 would be exposed to if they were to continue to opt into usage data collection	Accepted	Low	n/a
5. Given the app release has been accelerated to support COVID-19 'restart' priorities we could face concern that appropriate privacy by	Ensure that TfL maintain a transparent approach, and continuously review how we communicate key messages to our customers. Prepare key lines to take to support	Reduced	Low	Yes

design measures have not been considered or documented	our response to any queries raised, providing responses in a prompt manner. Publish this DPIA			
6. Due to the development work required and other app development work priorities, the requested functionality to manage preference for remembering search history hasn't gone into the app yet.	Users have an option to clear this information right below the search history displayed. TfL Go project team to start development work for this functionality in January 2021, with support and guidance from the Privacy and Data Protection team.	Reduced	Low - Medium	
7. Due to other app development work priorities, the requested update to iOS location permission modal hasn't gone into the recent iOS release yet.	TfL Go project team to implement the update in the next iOS release.	Reduced	Low	
8. The Android Location permission modal doesn't allow incorporating information on purpose and benefit for sharing location data.	Users can access details about user benefit and purpose of sharing location data in the privacy and cookies page on TfL Go, a link to this page is also available in app settings.	Accepted	Low	

Step 11: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Richard Bevins, 3 December 2020	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Richard Bevins, 3 December 2020	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Richard Bevins, 3 December 2020	Privacy & Data Protection team should advise on compliance, Step 10 measures and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	T&D Digital must continue to work with the Privacy and Data Protection team to complete any outstanding actions noted in Step 10. T&D Digital must continuously engage the Privacy and Data Protection team as the app is further developed. This will allow the assessment of any privacy requirements as development occurs. Where necessary and appropriate, amendments will be made to this DPIA, or a new DPIA compiled where the processing is fundamentally different to that described here.	
DPO Comments:	It is important that the recommendations above are actioned, throughout the lifecycle of the app.	
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:		
Consultation responses reviewed by:	Project team	If your decision departs from individuals' views, you must explain your reasons.
Comments:		

This DPIA will kept under review by:	Digital, Technology & Data, and Privacy and Data Protection team, Information Governance	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	A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or

people	others from harm or exploitation. All children are considered vulnerable by virtue of their age and immaturity.