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 Product Manager	Date DPIA completed	5 September 2024
Job title:	Product Manager	Proposed launch date	Week commencing 13 January 2025

Name and description of the project:	**Pay & ID functionality in TfL Go** TfL Go is our flagship travel app, launched in 2020. The app is location aware and includes a digital version of the Tube map, a multi-modal journey planner, status information, and live arrival data for Tube, bus and some rail services. Separate DPIAs were produced for the pre-launch trials and the public launch (which has been subsequently updated as new functionality is added).

	We are now adding account and payment functionality to TfL Go. Customers will be able to register for and log in to their TfL ID account, view their Oyster and contactless journey history, top up their Oyster card and buy travel cards/bus & tram passes. This will make the app a single destination for all TfL travel support and is a key milestone in the TfL Go roadmap. Before a public launch of Pay & ID functionality, and in addition to formal development testing, we will be running some internal user acceptance testing (UAT). When we initially launch the functionality publicly it will be via Android and Apple mechanisms which support a phased rollout – i.e. to a limited percentage of users, increasing over time.				
Personal Information Custodian (PIC) or band 5 lead	Head of Technology & Data – Digital Payment Operations and Assurance Manager – PIC for Oyster and Contactless data displayed in TfL Go	Are PICs aware of this DPIA?	Y	Project Sponsor	Head of Technology & Data – Digital

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

Use profiling or automated decision-making to make decisions that will have a significant effect on people. Significant effects can include financial or legal outcomes, intrusions into private life or restrictions on access to services, opportunities or benefits.		Process special category data (relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life or sexual orientation) or criminal offence data on a large scale.		Make changes to processes and systems that are likely to result in significantly more employees having access to other peoples' personal data, or keeping personal data for longer than the agreed period.	
Use data concerning children or vulnerable people. A person with vulnerability is usually described as someone who is at a higher risk of harm than others.		Process personal data which could result in a risk of physical harm or psychological distress in the event of a data breach.		Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.	
Systematically monitor a publicly accessible place on a large scale – e.g. through the use of CCTV or Wi-Fi tracking.		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.		Process personal data on a large scale or as part of a major project.	X	Process personal data without providing a privacy notice directly to the individual.	
Use personal data in a way likely to result in objections from the individuals concerned.		Apply evaluation or scoring to personal data, or profile individuals on a large scale.		Use innovative technological or organisational solutions.	
Process biometric or genetic data in a new way.		Undertake systematic monitoring of individuals.		Prevent individuals from exercising a right or using a service or contract.	

Step 1 – Identify the need for a DPIA	
Explain broadly what your project aims to achieve and what type of data and processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	The Pay & ID functionality in TfL Go meets a core customer need to manage their account on the move and have their payment and travel information in one place. The intention is that the separate Oyster and contactless app will be retired once this functionality is in TfL Go, simplifying our product suite and saving TfL money. Support for account and payment functionality necessarily involves processing personal data, including name, address and email address, and recent journey history. Customers can also save payment cards and register contactless cards and devices, which need to be processed and managed securely. Sign in is optional and users of TfL Go are not mandated to sign in; they may continue to use the travel features in a non-signed in state but will not be able to see or manage their payment information or journey history and carry out any account-based functions. TfL Go will use a product for user authentication upon launch, which includes multi-factor authentication. Once authenticated, users remain signed in for a period of time. The product was the subject of a DPIA prior to launch in the TfL Oyster and contactless app and web accounts in May 2023. Biometric sign-in for some data/functionality within the app and integration with Apple Pay and Google Pay may be added to the app in the future, at which point an update to this DPIA will be made following discussion and review with the Privacy and Data Protection team. Concessionary Oyster cards are not supported in the initial launch scope for Pay and ID functionality in TfL Go, but we do recognise that some customers may still try to add these cards, as they do in the web version of the account. We intend to add this support to TfL Go in the future, following further discussion and review with the Privacy and Data Protection team, and updates to this DPIA. The initial focus will be to support adult concessionary card holders (for example, the 18+ student Oyster photocard and 60+ London Oyster photocard). Support for Zip Oyster photocards (used for under-18-year-olds) may also be added at a future time and will be considered with reference to the ICO Age Appropriate Design Code as appropriate. Before a public launch of Pay & ID functionality, and in addition to formal development testing, we will run internal user acceptance testing (UAT). This will involve circa 50 TfL employees, who will be provided with test Oyster cards and access to the app. The UAT approach has been discussed/reviewed with the Privacy and Data Protection team, who have prepared a privacy statement for participants. The app will be delivered by TestFlight for Apple devices and App Center for Android devices. UAT needs to take place within the production environment. Production is the only environment we can fully test transactions in (e.g. a user topping up and

	collecting at a yellow reader), as it is the only environment fully linked up. If we didn't use the production environment, we wouldn't be able to do any testing on transactions prior to vanguard testing. The UAT will be delivered in alignment with T&D Payments principles, including access controls to production account data (i.e. the project team will receive aggregated account usage statistics and no individual account data). Ahead of UAT there will be regression and integration testing completed, which will be carried out with test data. When we initially launch Pay & ID functionality publicly it will be via Android and Apple mechanisms which support a phased rollout. This means that the update reaches only a percentage of users initially, with the percentage able to increase over time. Percentages will be mirrored across both Android and Apple. A phased rollout has been chosen given this addition of payments functionality to limit the potential risk exposure. This soft launch also gives the opportunity to identify any issues before reaching 100% of users. It is difficult to state exactly when 100% will be reached, but Apple have a rule whereby the maximum rollout period can be 37 days. Users are chosen at random to receive the update, and for Apple users they are only selected at random if they have automatic updates switched on. Apple users who request a manual app update during the phased rollout will also be updated to the new version. For both Android and Apple users they aren't notified if in a phased release, but they will notice additional features in the app that we are choosing to label as 'new'. They will also be informed that the app has been updated as they will be shown a re-consent screen for sharing usage data. More information on phased rollouts is available here: For Android – https://support.google.com/googleplay/android-developer/answer/6346149?hl=en-GB#zippy=%2Cselect-staged-roll-out-percentage%2Cincrease-your-staged-roll-out-percentage%2Chalt-a-staged-roll-out%2Cresume-a-staged-roll-out For Apple – https://developer.apple.com/help/app-store-connect/update-your-app/release-a-version-update-in-phases
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	For TfL, the key benefits of adding account and payment functionality to TfL Go are: 1. It delivers a holistic travel app experience and helps ensure the TfL Go app meets customer expectations. 2. In the medium term, it will deliver financial savings: a. It will allow us to retire the Oyster and contactless app, thus saving operational maintenance and development costs.

	b. It is also hoped that inclusion in TfL Go will also extend the reach of low-cost digital payments to more customers, increasing self-serve and therefore reducing support costs. 3. It will extend the reach of the TfL ID account and increase the number of people registering an Oyster or contactless card. This helps TfL to build a direct digital relationship with customers, and provides greater insight into our customer base to improve services. 4. TfL ID account integration will enable other features in future, such as personalisation in the app and tailored push notifications informed by the customer's travel history and profile. (Separate privacy assessments will take place of these features to identify any associated privacy risks and mitigations). For individuals, the key benefits are: 1. A single place to manage their TfL travel and ticketing needs, putting them in control. 2. A more intuitive user experience for payments, including support for the latest accessibility standards. 3. A more tailored experience in the future. For stakeholders, and the wider society, the key benefits are: 1. Providing useful digital tools in an intuitive, joined-up experience helps support and drive public transport usage, contributing to a healthier city. 2. Data collected about the way travel services are utilised will help with the planning and delivery of future transport services. The impact of the Pay & ID functionality will be measured through the following (some of these measures might not be possible until the Oyster and contactless app has been decommissioned, because whilst dual running both apps, transactions cannot be attributed to each distinct app): 1. Use of the functionality in TfL Go: a. The number of TfL Go users who register for or sign in to TfL ID b. The number of Oyster and contactless cards registered to a TfL ID account c. The number and value of transactions processed through TfL Go 2. Migration away from the current Oyster and contactless app: a. A reduction in usage of the Oyster and contactless app, aligned to an increase in visits to the TfL Go payment area

	b. The green light to begin the retirement process for the Oyster and contactless app
Will the processing directly affect the individuals concerned?	Yes, this processing is required to deliver the account and payment functionality that individual users will experience.

Step 2: Describe the nature of the processing (You might find it useful to refer to a flow diagram or other description of data flows).		Could there be a privacy risk?
What is the source of the data?	There are a number of sources of data used to enable the Pay & ID functionality in TfL Go. • User authentication product. Accessed via an in-app web view for sign-in. *The app interacts with other in-app web views at times also (including; sign in, create an account, forgot password, claim a refund, add contactless card).* • Mobile services. This is an existing solution that pulls data from TfL systems to then support other solutions by being able to call back data via an API (e.g. list of Oyster cards the user has registered to their account, associated transactions, journey history, etc). • Customer data entry. For example, when registering for an account the user will enter their name and email address and provide details of Oyster and contactless cards if registering these. TfL Go will fetch 56 days / 8 weeks worth of Oyster and contactless journey history from mobile services to display in the app (see associated risk). In summary, additional information will be available if a customer logs in to their account via the website, such as details of travel caps reached, intermediate journey taps, pending payments not yet collected and a longer period of journey history.	Yes

Will you be sharing data with anyone?	There will be no additional sharing of personal data enabled through this project. The data will continue to be available to staff in areas of TfL that already have access to account information through other channels. Where applicable some of our suppliers also have access to this account information.	No
Are you working with external partners or suppliers?	We will not be working with any new external partners or suppliers as part of this project. Existing relationships are already in place.	No
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	Contracts are already in place with third party suppliers and are not specific to this project.	No
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?	Data protection is a key requirement for external contracts where applicable, and suppliers are managed via a pre-defined contract management process that is not specific to TfL Go. The same data obtained or accessed via existing channels is already processed by these third-party suppliers, therefore the additional risk through TfL Go is small.	No
Will the data be combined with, or analysed alongside, other datasets? If so, which ones?	Any data collected or accessed through Pay & ID functionality in TfL Go will feed into existing systems and processes (which are not the subject of this assessment) via integration with mobile services. However, to give some explanation - for example, creating a new TfL ID account will generate an entry in the Digital Marketing database to manage customer communications. This will then be combined with other datasets, as defined by that product, such as tagging the existence of a Road User Charging account that uses the same email address. App usage data from TfL Go feeds into a data analytics tool. This will include data related to use of the Pay & ID functionality for users who have opted in to sharing their usage data – at the point of app onboarding users are given an option to consent to sharing usage data (this is described in more detail in the already published TfL Go DPIA, prepared when the app was first launched in 2020).	Yes

	This data is pseudonymised and through this tool, the Digital Analytics team will have access to non-personally identifiable data such as the number of account registrations, sign-ins and transactions actioned through TfL Go. However, personal data will not be shared, and it will not be possible to infer individuals' usage or details from this data. Currently the data for TfL Go is collected and stored in this data analytics tool separately from data collected through the TfL website and the Oyster and Contactless app, and these datasets cannot be combined to give an overall picture of an individual's use of the TfL digital services. Furthermore, it cannot be combined with journey history data to provide a holistic view of the individual's use of TfL's digital services and network. In the future, we would like to implement a unique user identifier (which may be the TfL ID), allowing us to combine datasets and understand how individuals use TfL's range of digital services (TfL website, TfL Go, Oyster and Contactless app) alongside their network usage, through the availability of journey history data. A separate DPIA will be produced if and when this implementation is planned, so that a complete privacy assessment can take place, ensuring that any privacy risks are identified and appropriately mitigated before. Users can access non-account functionality within TfL Go and there is no way to link between signed in and signed out usage for an individual user. We do not send any sort of identifier to non-payments backend endpoints that could be used to link with an account. The only thing we send that varies between API requests (other than the request itself) is whether the request has come from Android or iOS. On the payments side we also don't track logins or journey history entries through analytics.	
Will AI or algorithms be used to make decisions? What will the effect of these decisions be?	TfL Go uses algorithms to provide the following Pay & ID functionality: • Low Balance icon: When a user's Oyster card balance falls below a certain threshold, an icon appears on the Pay card in the main user interface. This alerts the user to the fact that they may need to take action. • Travelcard Expiry icon: When a user's travelcard will expire in a defined number of days, an icon appears on the Pay card in the main user interface. This alerts the user to the fact that they may need to take action. When push notifications for Low Balance and Travelcard Expiry are introduced (not in scope for the first release) algorithms will also be used to determine when the notification needs to be sent. Notifications are the subject of a separate privacy assessment.	No

	TfL Go will not use AI to make any decisions based on a user's account data. Any data originating from TfL Go that passes into other systems, may then be subject to AI or algorithmic processing, subject to the rules already in place for those systems.	
How and where will the data be stored?	Very little data is stored in the TfL Go app or its specific back-end service; the approach taken is for TfL Go to principally display data passed from the existing core systems (via mobile services). The exceptions to this, where data is held locally on a device, are detailed below. The TfL Go app persists account related data to the device (phone / tablet, etc.) to improve performance, and offline functionality. With iOS this data is saved to the Keychain and is deleted on sign-out or launching the app post-reinstall (more detail on Keychain security is available here: https://support.apple.com/en-gb/guide/security/secb0694df1a/1/web/1). With Android this data is saved in an encrypted shared preference file that is only accessible to TfL Go, and is deleted on sign-out or when uninstalling the app. To further explain for iOS – if someone deletes the app whilst still signed in, whilst not guaranteed, the locally stored information in the Keychain is likely to persist on the device indefinitely. Unfortunately Apple does not provide an option to automatically delete the associated Keychain data for an app when it is uninstalled. To mitigate any associated risks of this – TfL have added a feature whereby if someone then reinstalls the deleted app, when the app launches, it will log the user out and delete any saved information. The following data is persisted locally on the device: Account information (for example, first name) Customer ID First name Last name Title Address Email address	No

	List of Oyster cards & Travel cards/bus & tram passes List of Contactless cards (partial card details) List of saved Payment cards and the last used payment card (partial card details) User details like name, address and email etc. Journey History Card order information (full Oyster card number and Contactless card identifier, Flag to Show/Hide, Position in the list) Contactless card nickname (Card identifier & card name) Oyster card nickname (full Oyster card number & card name) The last three items remain when someone signs out, so that the preferences can be displayed when they sign back in. However, it is deleted when the app is uninstalled (or reinstalled in the case of iOS) or when another user signs in on that device. As described elsewhere in this DPIA, account related data is pulled from other systems, which will not be described in detail in this DPIA. This includes, as part of the logging in process, data is captured and stored in order to authenticate users and manage access to Payment functionality. Where data is stored in the TfL Go app, we make use of the encryption offered by the relevant device OS (operating system): • For iOS, this uses the Keychain. More information is available here: https://developer.apple.com/documentation/security/keychain_services • For Android, all user data is stored in an encrypted folder which is accessible only to the TfL Go app and this data gets deleted when the app is uninstalled. This follows the standard Android OS security protocols. More information is available here: https://developer.android.com/topic/security/data	
Will any data be processed overseas? Which countries?	Neither TfL Go nor the underlying ID and payment systems process any new data overseas, outside of the UK or EEA. We will continue to process services in Europe.	No

Are you planning to publish any of the data? Under what conditions?	TfL Go will not publish any personal or individual account or payment information. Top level statistics relating to take-up of the features will be shared internally as part of standard app reporting and may be published. No individual data will be published, and it will not be possible to infer an individual from this.	No

Step 3: Describe the data		Could there be a privacy risk?
Who does the data relate to?	The data relates to anyone using the TfL Go app containing pay & ID functionality and who choose to create or sign into a TfL ID account.	No
How many individuals are affected?	As of 19th March 2024 the Oyster and contactless app has had c.5.5m downloads to date, and currently has c.597K monthly active users (all of whom must sign into an account to use the app). Over time, a similar number of people are likely to sign in and use payment features in TfL Go. As of 30 November 2024, TfL Go currently has 7.5m downloads with c.1m monthly active users.	No
Does it involve children or vulnerable groups? If children's personal data is processed, how old are they? Consider the ICO Age Appropriate Design Code	When the original TfL Go app launched in 2020 it was not aimed directly at children, nor has it been directly designed for them, and adding account functionality has not changed this. 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 have referred to the ICO Age Appropriate Design Code during development of TfL Go functionality and additional detail in regard to this can be found in the main TfL Go DPIA here. Any payment activity requires a payment card to be registered which is likely to minimise the number of children who try to use the feature, and so is hard to envision a risk of economic exploitation or unfair commercial pressure. Where appropriate any messaging in the app also	No

	directs users under the age of 13 to ask their parent or guardian's permission for any data sharing - i.e. where we rely on consent as a legal basis for sharing usage data. This was already incorporated into the original app and will be considered for any specific account functionality. This includes as part of account registration an individual is asked if they want to consent to TfL and TOCs (train operating companies) offers and promotions emails. However, this registration screen is part of a separate interface and so any updates must be considered as part of any future work for that interface. As explained in the main TfL Go DPIA our view is that TfL Go 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 believe this does not change with the addition of account functionality.	
What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*) Are there any Special Category or sensitive data (list all): Race or ethnicity; Physical or mental health, Political opinions; Religious or philosophical beliefs; Trade Union membership; Using genetic or biometric data to identify someone; Sex life or sexual orientation; Criminal allegations or convictions	The data captured and/or displayed for TfL Go's Pay & ID functionality are: • Title • First name • Last name • Contact mobile number and contact other number (both are optional) • Address • Email address • Oyster card number • Card nickname • Oyster Pay as You Go balance • Oyster card products – travelcard/bus & tram passes, discounts, auto-top-up • Oyster journey history – up to 8 weeks • Oyster journey details (entry and exits) • Payment card details for Oyster purchases: card number (partial), expiry date (not displayed or captured by TfL Go – it is captured in mobile services and provided to TfL Go as needed via a token), card type • Cardholder name and billing address • Most recent Oyster card journey (only if journey made in the last 8 weeks) • Details for Contactless card used for travel: last 4 digits of card number, card type • Transaction history – top-ups, fares charged, refunds – up to 8 weeks • Contactless journey history – up to 8 weeks	Yes

Captured only:

- Authentication phone number (used for authentication, but can't be seen in the app)
- Password (can only be amended via the web, can't be seen in the app)
- Oyster card security answer (can only be amended via the web, can't be seen in the app, only used for initial verification)
- Journey History entry (completing validation when adding an Oyster card)
- Marketing preferences (captured as part of account creation, but can't be viewed in the app once account set up)

When a customer logs into TfL Go to access the Pay experience, some information will be registered. The table below describes the fields stored to authenticate users and manage access to Pay functionality.

Field
deviceIdentifier
platform
deviceType
osVersion
appVersion
notificationInstallID
notificationHandle
tflAccountID
updated
created

	Various functionality within TfL Go is delivered via API calls, which can result in the collection of data in logs – this has been described in the previous DPIA and in our public facing privacy notice. Account functionality will also be delivered via API calls to mobile services and a review has taken place to understand if this results in the collection of account data in API logs. It has been confirmed that only limited data is captured. The system is not configured to save the output of these API requests, but it may save information about incoming API requests (e.g. order ID, customer ID, Oyster card number) in certain points in a transaction. This is to help trace an issue such as failed payments and incomplete orders. We are not saving order details and customer details such as full name, customers complete details and complete details of the order. As part of a separate project work is ongoing to remove data where possible and get to a point where every API and function is set to the appropriate log level. No Special Category or sensitive data is currently included. A future iteration is likely to involve biometric (fingerprint or facial recognition) sign in; the DPIA will be updated if and when this takes place. This will utilise the device Operating System (iOS or Android) capability and no biometric data will be shared with TfL back-end systems. Usage data related to the Pay & ID functionality will be collected and fed into an analytics tool, for users who have opted in to sharing their data in this way. Screens and actions are tracked, in some cases with additional context data. **Screens:** a screen view is tracked when a screen is displayed, the screen name is the same for all users. **Context data:** this data is specific to the user, the fields tracked are listed below: • Top up amount ("5", "10", etc. tracked in the checkout and purchase complete screens) • Card type ("oyster" or "contactless") • Card types concatenated (possible values: "Oyster", "Contactless" or "OysterContactless") • Sign state (signed in or not signed in) • Selection of offers and promotions ("TfL", "TfL - Train Companies" or "Train Companies") • Duration (season ticket duration) • From zone (travelcard from zone)	

	• To zone (travelcard destination zone) • Travel product (values “bus” or “tram”) • Start date (for a travelcard) • Renewal date (for a travelcard) **Actions tracked:** • Select a card from a list • Sorting cards • Select ticket duration • Select zone • Select a start date **Not tracked**: • Name • Last name • Name on card • Card number • Postcode • Address • Expiry date	
What is the nature of TfL’s relationship with the individuals? *(For example, the individual has an oyster card and an online contactless and oyster account.).* Is the data limited to a specific location, group of individuals or geographical area?	All individuals will have, or will be creating, a TfL ID Single Sign On account. The functionality is available to anyone choosing to create or sign into their account; only those customers within Europe will be able to create an account or sign in. TfL ID functionality includes: • Create account • Sign in • Forgotten password • My account section, including, Delete an account, Manage Account (links to website) and Sign out The individual may have an Oyster card registered to their account. This is not mandatory but is required to make use of the Oyster functionality in TfL Go, including: • Card list (including sort and edit cards)	No

	• Nickname card • Card View • Travel card summary information (if the user has a travel card on their account) • History (including journeys, incomplete journey refunds, purchases) • Top up and checkout including add payment card • Purchase/renew a travelcard • Low Balance and Travelcard Expiry icon The individual may have a contactless card registered to their account. This is not mandatory but is required to make use of the contactless card functionality in TfL Go, including: • Card list (including sort and edit cards) • Nickname card • Card View • Journey history	
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	No, the purpose of this feature is to offer the user access to their TfL travel and payment information and management of their payments to TfL. All fields are required for processing transactions and to fulfil the user needs.	No
How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?	TfL Go is linking in with existing systems that have processes in place to ensure data quality and accuracy.	No
How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?	As TfL Go is linking in with existing systems to deliver the Pay & ID functionality, the data retention and management policies are defined by the systems being used. The Oyster and contactless disposal schedules will apply here. Depending on the operating system in use, data persisted locally in the TfL Go app is removed if the user signs out (including if they are automatically signed out), or when the app is uninstalled or reinstalled. More detail is provided earlier in this DPIA.	No

Do you have a documented disposal process?		
Step 4: Describe the context of the processing		Could there be a privacy risk?
Is there a statutory basis or requirement for this activity?	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 after step 7, completed by the TfL Privacy and Data Protection team.	No
Is there any use of Artificial Intelligence or automated decision making?	There is no use of AI in the first release of Pay & ID functionality in TfL Go. As discussed earlier there are algorithms used to display content in the app – i.e. low balance and travelcard expiry icons, but these would not meet the definition of 'automated decision making'.	No
Will individuals have control over the use of their data? If so, how can they control it?	During the phased rollout users are randomly selected to receive the updated app and therefore have no control over this unless they switch off automatic updates if an Apple device user. If an Apple user decides to manually update their apps, they will be given the new version of the app then also. Individuals can choose not to use the Pay & ID functionality in the app, or to limit the features they enable. For example, by not adding a contactless card to their TfL ID account, no transactional or journey history data from that card will be accessible to TfL Go or linked to their ID profile. When choosing to use these features, the individual cannot control how the data shared is used in the associated TfL systems. Individuals have the option to remove Contactless cards from their ID, which then removes associated data from TfL Go, and they can cancel their Oyster card. They can also delete their TfL ID account via TfL Go. By following the in-app deletion process, they can submit a deletion request. Individuals also have control, as part of the account creation process, as to whether they would like to receive promotional emails from TfL and selected third parties (e.g. train operating companies). Permission for this can be further managed within the account settings section of the TfL website, once the account has been created.	No

	Individuals also have control over whether they opt-in to sharing their usage data, which includes usage of account related functionality, and can change their preference at any point via the app settings.	
Would they expect you to use their data in this way?	We believe that users of the Pay & ID functionality will expect their data to be used in the ways described, as it is not possible to deliver the services without such processing.	No
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?	An update to the current TfL Go privacy notice will be prepared to cover the phased rollout and will then be updated again once the update is released to 100% of users. Updates will also be made to the existing Oyster, contactless and cookies privacy notices where necessary. Throughout the app where necessary there will be 'just in time' privacy related content – e.g. a short form privacy statement when registering for an account and wording relating to under-13's where consent is requested.	Yes
Are there prior concerns over this type of processing or security flaws?	There are no known security flaws currently recorded on the project risk register.	No
Is it novel in any way, or are there examples of other organisations taking similar steps?	TfL Go's use of personal data for Pay & ID functionality is not novel and most ticketing apps would provide similar functionality based on similar processing.	No
What is the current state of technology in this area? Is this innovative or does it use existing products?	TfL Go is integrating with existing systems to deliver the Pay & ID functionality within the app. In particular, the APIs and feature set are closely replicating that currently available in the Oyster and contactless app.	No

What security risks have you identified?	As it is primarily integrating with existing systems, no additional security risks have been identified as part of this project, but a penetration test will be completed before launch.	No
Are there any current issues of public concern that you should factor in?	Our approach to any data processing in TfL Go keeps 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.	No
Is the processing subject to any specific legislation, code of conduct or certification scheme?	The processing is subject to data protection legislation, including the UK General Data Protection Regulation and Data Protection Act 2018. The processing is also subject to the Privacy and Electronic Communications Regulations (PECR) 2003 given it involves some integration with customer facing web frontends which involves the usage of cookies (there are no cookies or similar technologies dropped by the app itself). Compliance with PECR will be managed in two different ways dependent on type of web integration accessed and operating system used. In summary if a link takes a user to the website via a browser on their device, compliance with PECR will be managed via TfL's cookie consent management tool implemented on the TfL website. However, there are some specific functions in the app that go to the web via an in-app web view. For Android devices, these web views will still manage cookies via TfL's cookie consent management tool. But for iOS devices, customers will not interact directly with TfL's cookie consent management tool. Instead, only essential cookies will be dropped in these scenarios. A user could browse the TfL website more widely through these in-app web views, but still only essential cookies will be dropped. This has been discussed extensively with the Privacy and Data Protection team and they have requested assurance/evidence be provided and they will also be describing this within the public facing privacy notices. Any approach to PECR compliance needs to also align with Apple's app tracking transparency obligations. As the app is processing payment card data it is also subject to the PCI DSS (payment card industry data security standard). The project is working with TfL's PCI Compliance Manager on this obligation.	Yes

Will there be any additional training for employees?	Generally, no, as the teams that manage the existing integrating systems will also cover TfL Go elements. We will be engaging customer service teams though to familiarise them with the new functions that will be available in Go. As these functions exist in an existing app (Oyster and contactless app) they are already familiar with any processes.	No
Does the processing actually achieve your purpose?	Yes, the processing allows us to deliver the Pay & ID functionality in TfL Go.	No
Is there another way to achieve the same outcome?	No	No
Who will own this initiative and ensure there is no function creep without a review of this DPIA?	The Digital Product Manager responsible for Pay & ID functionality in Go will own this initiative and keep under continuous review to ensure there is no function creep without proper privacy review. They will liaise with the TfL Privacy and Data Protection team to discuss any further development which may result in changes to this DPIA. TfL Digital also have a regular catch-up with the Privacy and Data Protection team to discuss all TfL Go activity – i.e. account and non-account functionality.	No

Step 5: Consultation process	Could there be a privacy risk?

Consider how to consult with relevant stakeholders: Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.	There are no plans to engage directly with users of the Pay & ID functionality in TfL Go, either during the phased rollout or when released to all users. However, users can provide feedback to TfL: • Using the email address provided in the app. Note that this email link may be replaced by an app feedback form in the future. Once available in the main TfL Go app, individuals can still choose not to create or sign into TfL ID and choose which Oyster and/or payments cards they want to add. If a user already has an account they will be able to see all cards attached to their account. They will be able to access data collection and processing information in an updated privacy notice. We also know that the addition of Pay & ID functionality into TfL Go is a welcome feature for many TfL customers: • Qualitative user research conducted in March 2021 (14 in-depth interviews) specifically tested the value proposition of the Pay & ID functionality in TfL Go. The concept of integrating travel and payments into a single app, and the specific functionality supported, were both positively received by users of TfL Go and the Oyster and Contactless app. • A summary of TfL Go customer suggestions collated in February 2022 (from Apple App Store reviews, Google Play Store reviews and direct email feedback via the app) showed that 'Integrate account / payments' was the 11th most common request, mentioned 23 times in unsolicited feedback. • Prior to the launch of TfL Go, Apple App Store and Google Play Store reviews of the Oyster and Contactless app frequently requested that journey planning functionality be added to the app, showing that there has long been demand for a single integrated app experience.	No
Which business areas have been consulted within TfL?	Information Governance (Privacy and Data Protection) T&D Payments Customer Information Customer Contact Operations (CCO) TfL Go Steering Group provided with regular updates (includes representatives from across the business)	No

Have you discussed information security requirements with Cyber Security? If so, who is your contact in Cyber Security?	Yes. We have contact with a Senior Cyber Security Analyst.	No
Do you plan to consult with external stakeholders? If so, who?	No consultation with external stakeholders is planned. We do expect to notify key external stakeholders though. A press release is also likely to be published when the Pay & ID functionality is released into the main TfL Go app.	No

Who will undertake the consultation?	Any external stakeholder notification or press release will be co-ordinated by the Digital Product Manager responsible for the Pay & ID functionality in Go, working with colleagues in the relevant departments.	No
What views have been expressed by stakeholders?	n/a	No

Step 6: Identify and assess risks				
Describe source of risk and nature of potential impact on individuals. Include risks of damage or distress as well as associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Is this risk included in project or other risk register?**
Customers may raise objections when the Oyster and Contactless ticketing app is decommissioned, such as not wanting to use a location-aware app.	Remote	Minimal	Medium	No
The scope of usage data collected via our analytics tool will alter when Pay and ID functions are added, and people might not want to remain opted in to sharing usage data.	Possible	Minimal	Medium	No
Hidden data processing may occur due to limitations in amount of transparency messaging that can be included on app screens.	Possible	Minimal	Medium	No
Incomplete account/card information shown to app users – for example only showing 56 days / 8 weeks of Oyster and contactless journey history, when more may be available on the	Remote	Minimal	Medium	No

Oyster and contactless app, or via the website.				
Account registration screens are part of a separate solution. Currently there is no under 13 consent wording on the offers and promotion email opt-in screen. TfL Go cannot amend this, and it will not be resolved before launch.	Remote	Minimal	Medium	No
As described in the DPIA PECR compliance for in-app web views (iOS only) will be met by only dropping essential cookies. A concern is that non-essential cookies will be dropped in future and that we cannot fully meet our transparency obligations.	Possible	Minimal	Medium	No

Step 7: Identify measures to reduce risk					
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8					
Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated, reduced or accepted)	**Residual risk** (Low, medium or high)	**Measure approved** (Yes/no)	**Who is responsible for implementation?**
Customers may raise objections when the Oyster and Contactless ticketing app is decommissioned, such as not wanting to use a location-aware app.	As shown in the DPIA there has been feedback that supports the inclusion of Pay and ID functionality in TfL Go, but if objections are received, we can advise how users can use the app without enabling location data use for example. We must continue to maintain a transparent approach so that users are fully aware of the data processing activity in the app.	Reduced	Low	Yes	Digital and Privacy and Data Protection team (where feedback is provided to them).
The scope of usage data collected via our analytics tool will alter when Pay and ID functions are added, and people might not want to remain opted in to sharing usage data.	We should continue to maintain a transparent approach so that users are fully aware of the data processing activity in the app – this must include a review of the current usage data opt-in	Reduced	Low	Yes	Digital

	screen to ensure it is suitable for this revised scope. We must also reconsent users once the account functionality is launched, so that they can be prompted to amend their decision if they would like to.				
Hidden data processing may occur due to limitations in amount of transparency messaging that can be included on app screens.	We should continue to maintain a transparent approach so that users are aware of the data processing activity in the app – this must include a review of in-app screens containing privacy content. Ensure app users have a clear route to view additional privacy information - i.e. include a link to the 'privacy & cookies' pages within relevant in-app screens and from settings.	Reduced	Medium	Yes	Digital, with support for drafting of content from Privacy and Data Protection team.

Incomplete account/card information shown to app users – for example only showing 56 days / 8 weeks of Oyster and contactless journey history, when more may be available on the Oyster and contactless app, or via the website.	We should continue to maintain a transparent approach so that users are aware where more data may be accessible to them via other means. Ideally there will be in-app messaging where relevant, but this will not be available for launch. For launch, the project team should ensure limitations are conveyed to customers, and where these have a direct privacy relation (e.g. showing less travel history) this will be captured in the privacy notice.	Reduced	Medium	Yes	Digital and Privacy and Data Protection team
Account registration screens are part of a separate solution. Currently there is no under 13 consent wording on the offers and promotion email opt-in screen. TfL Go cannot amend this, and it will not be resolved before launch.	The Privacy and Data Protection team will continue to advise Digital on this requirement.	Accepted	Medium	Yes	Digital (with support for wording to use from Privacy and Data Protection team)

As described in the DPIA PECR compliance for in-app web views (iOS only) will be met by only dropping essential cookies. A concern is that non-essential cookies will be dropped in future and that we cannot fully meet our transparency obligations.	The Privacy and Data Protection team have requested assurance to evidence essential cookies only and that the technical solution is monitored on an ongoing basis. Investigations are also taking place to ensure that cookie lists are accurate and that app users are directed to this detail within updated privacy notices.	Reduced	Medium	Yes	Digital and Privacy and Data Protection team

To be completed by Privacy & Data Protection team		Could there be a privacy risk?
What is the lawful basis for processing? Are there any Special Category or sensitive data?	The lawful bases we are already relying on for processing of data in the current version of the TfL app are detailed in the main DPIA and within our current privacy notice. In the specific circumstance of adding Pay and ID functionality into the app we will be relying on the following lawful bases: • For the processing of the account (including administering transactions such as topping up an Oyster card, etc) we are relying on Article 6(1)(b) of the UK GDPR - "The Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". • For the processing of sending offers and promotions emails where someone has opted-in during registration we are relying on Article 6(1)(a) of the UK GDPR - "The	No

	data subject has given consent to the processing of his or her personal data for one or more specific purposes". • For the processing of data for security monitoring purposes we are relying on Article 6(1)(f) – "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". There is a separate DPIA covering this, which serves as our Legitimate Interests Assessment. At this stage we believe there is no Special Category or otherwise sensitive data being processed.	
Is this use of personal data compatible with our original purposes for collecting the data?	Yes, the use of data is compatible with the provision of Pay and ID functionality to the customer.	No
Are changes to Privacy Notice required?	Yes, these changes will be taken forward by the Privacy and Data Protection team, with liaison with the project team for review and amendment.	Hidden data processing may occur due to limitations in amount of transparency messaging that can be included on app screens.
How will data subjects exercise their rights?	Data subjects (i.e. app users and account holders) will be able to exercise their information rights with TfL in accordance with existing processes. In addition, the app will also support the submission of account deletion requests.	No

How do we safeguard any international transfers? Is any data being processed outside the UK?	At this stage we are not aware of any related international data transfers.	No
Could further data minimisation or pseudonymisation be applied?	We believe that data minimisation has been considered throughout and that the data being processed is necessary to deliver the functionality described to customers.	No
Have appropriate security measures been considered, with Cyber Security involvement where necessary?	Yes, and a pen test will be completed before launch.	No
Are data sharing arrangements adequate? Do they require further documentation?	There are no data sharing arrangements which need to be considered further.	No
Is the data likely to be and remain adequate, accurate and up to date?	The adequacy and accuracy of the data will be managed within source systems which are the master holder of data then displayed within the app.	No

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	Head of Privacy and Data Protection 05/09/2024	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	Head of Privacy and Data Protection 05/09/2024	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:	Head of Privacy and Data Protection 05/09/2024	Privacy & Data Protection team should advise on compliance, transparency and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	The Privacy team are happy to approve this DPIA, whilst noting the need to manage the identified risks and complete the proposed testing. This DPIA has been reviewed for publication. Minor amendments have been made where information would be redacted under Freedom of Information rules.	
DPO Comments:	Shared with TfL Data Protection Officer by Head of Privacy and Data Protection on 05/09/2024 Noted and approved by DPO 05/09/2024	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):	Digital Product Manager	If overruled, you must explain your reasons below.
Comments:		
This DPIA will kept under review by:	Digital Product Manager	The DPO may also review ongoing compliance with DPIA.

Glossary of terms

Anonymised data	Anonymised data is information held in a form that does not identify and cannot be attributed to individuals. Anonymous information is not subject to the GDPR, and, where possible and appropriate, should be used in place of identifiable or pseudonymised personal data, particularly where sharing information with third parties or contemplating publication of data. Anonymised data will often take the form of statistics. If you are reporting statistics on a small number of individuals, or there is a level of granularity that allows reporting on small groups of individuals within the overall data set, you must exercise caution to avoid inadvertently allowing the information to be linked to an individual. If information can be linked to an identifiable individual the data is not anonymous and you must treat it as personal data.
Automated Decision Making	Automated Decision Making involves Top of Form making a decision solely by automated means without any meaningful human involvement. Automated Decision Making is restricted and subject to safeguards under the GDPR. You should consult with the Privacy and Data Protection team before rolling out a process involving Automated Decision Making based on personal data.
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.
PIC (Personal Information Custodian)	Personal Information Custodians are senior managers, who are responsible for the Processing of Personal Data within their assigned area of control.
Privacy notice	A privacy notice must let people know who we are, what we intend to do with their personal information, for what purpose and who it will be shared with or disclosed to. TfL adopts a layered approach to privacy notices, with clear links to further information about: • Whether the information will be transferred overseas; • How long we intend to keep their personal information: • The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information;

	• The name and contact details of the Data Protection Officer; • The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner; • The details of the existence of automated decision-making, including profiling (if applicable).
Processing	Doing almost anything with personal data. The GDPR provides the following definition: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Profiling is the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
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.