# 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: | Daniel Knight | Date DPIA completed | 27/01/20 |
| Job title: | Infrastructure Manager | Proposed launch date | 31/01/2020 |

| | | | | | |
|---|---|---|---|---|---|
| Name and description of the project: | This is a project to trial the use of GPS tracking technology on Santander Cycles. The initial trial will include approximately 500 cycles for a period of up to 12 months.<br>The initial purpose of using GPS tracking is to aid the recovery of lost or stolen bikes (only), although the use of GPS may be have subsequent applications (which would be considered under individual DPIAs as they arise). The police have indicated that they may request journey data where it is necessary for the investigation of crimes that involve a Santander Cycle in some way. | | | | |
| Personal Information Custodian (PIC) | David Eddington | Is PIC aware of this DPIA? | Y | Project Sponsor | Lee Blakeman |

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. | **X** | 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. | **X** |
| 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.<br><br>You may find it helpful to refer or link to other documents, such as a project proposal.<br><br>Summarise why you identified the need for a DPIA. | Project to add GPS trackers on the new model of Santander bikes. It is anticipated the initial trial will be for 500 bikes.<br><br>The data required is to know the exact location of a bike at any moment in time. At present TfL knows the start and end points of a journey (where a bike is undocked and docked) but not where the bike travels in between.<br><br>Requirement for GPS trackers is primarily for loss prevention. (It may also be useful in resolving disputes concerning whether a bike been returned correctly and where a customer has been charged late return fees or charged for a lost/stolen bike.) Due to the significant cost of a bike, GPS tracking will provide the opportunity to locate and retrieve abandoned or stolen bikes, reducing costs of replacing bikes and minimising reputational impact. (If TfL/Sponsor branded bikes are found abandoned in a canal or river for example,<br><br>21% of the fleet has been decommissioned as lost since the beginning of the scheme in 2010, which is approximately 400-500 bikes per year, at a cost of in excess of £500k annually.<br><br>Subject to the success of this trial, other uses of GPS tracking may be considered, including<br><br>a) Installation of GPS trackers will provide our customers with real-time information on the Santander Cycles Mobile App, allowing users to locate and hire bikes<br><br>b) Tracking the route a bike has taken anonymously can provide unique insight into the flow of traffic, routing data, etc. to help TfL when planning for new cycle routes and cycle lanes. Suppliers responsible for bike tracking data (Serco/Beryl) do not have access to customer personal data. They only track the asset (bike). Suppliers responsible for customer personal data (Cubic/Journey Call) will not have access to bike tracking. Only TfL has access to both bike tracking data and personal data.<br><br>Both of these uses will require the completion of DPIA before proceeding.<br><br>The police have indicated that they may request journey data where it is necessary for the investigation of crimes. |

| Step 2: Describe the nature of the processing | |
|---|---|
| How will you collect, use, and delete data? What is the source of the data?<br><br>Will you be sharing data with anyone?<br><br>Are you working with external partners or suppliers?<br><br>Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)<br><br>Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?<br><br>How and where will the data be stored?<br><br>Will any data be processed overseas?<br><br>You might find it useful to refer to a flow diagram or other way of describing data flows. | GPS data collected within this trial will be used for the purpose of tracking our assets only (bikes) and will not be used to track people.<br><br>For example, if a bike is not docked at the station and has been missing for a set period of time (classified as missing), we will use the GPS data of that bike to track its last known location. On-street operatives will be sent to last known location to attempt bike retrieval. Suppliers responsible for bike tracking data (Serco/Beryl) do not have access to customer personal data. They only track the asset (bike). Suppliers responsible for customer personal data (Cubic/Journeycall) will not have access to bike tracking data. Only authorised employees in TfL have access to both bike tracking data and personal data.<br><br>The source of the data will be the GPS tracker located securely within the frame of the bike, via a SIM card.<br><br>Bike tracking data will be sent from the GPS tracker to our bike tracking supplier (Beryl) who use a Google Platform. Data will be pushed to the Beryl Database which will provide real-time bike information, together with an event based alert system to schedule work. The real-time Beryl platform will be shared with authorised TfL employees for information purposes and with Serco to actively monitor and schedule resource to retrieve abandoned bikes.<br><br>GPS data won't be shared externally; however, there could be occasions where we work closely with the police to ascertain the last known location of a bike to assist in solving a crime. (There is an established process for sharing data with the police for this purpose and requests will be made through CPOS).<br><br>Serco manages the BMS (Bike Management Supply) contract for TfL and is responsible for delivering new bikes, maintaining existing and rebalancing bikes across the estate. TfL will ensure Serco/Beryl both comply with data protection obligations and standard clauses are written in the contract. Serco and Beryl shall provide documented/contractual assurances that any data generated from the trial won't be utilised for monetary gain or other commercial purposes.<br><br>GPS data won't be combined with or analysed alongside other datasets held by TfL without a further DPIA. Usage of the system will be controlled by access rights only being given to authorised personnel. The data is physically separated and held in different systems. Staff have been instructed never to combine customer data with GPS data, unless it is for the purpose of responding to data subject rights requests or police requests. Regular access monitoring will be carried out by the Head of Cycle Hire to ensure that this remains the case. Beryl has confirmed data will be stored in Google Cloud, which will be stored on UK based servers. Beryl currently provides the Blaze Laser light on Santander Cycles and their BILS unit has capability to accept tracking devices. . |

| Step 3: Describe the scope of the processing | |
|---|---|
| Who does the data relate to?<br><br>How many individuals are affected?<br><br>Does it involve children or vulnerable groups?<br><br>If children's data is collected and used, are they aged under 13?<br><br>What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*)<br><br>Specify which special category data or criminal offence data are to be processed?<br><br>Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?<br><br>How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?<br><br>Is the data limited to a specific location, group of individuals or geographical area? | We have approximately 25,000 members and also casual users (tourists, etc.) There were 10.5 million hires in 2018.<br><br>You have to be over the age of 14 to be able to use our scheme and over the age of 18 to purchase an access period.<br><br>However, for the purposes of this trial, the data will only be used for establishing GPS location of an individual bike, as opposed to tracking the location of an individual person. Personal data will not be accessed by Serco or Beryl as part of bike tracking. Only the asset is being tracked to aid the recovery of stolen bikes. Serco does not have access to DBOS (the current 'back office' system for Cycle Hire, where customer personal data is also stored). A partial DBOS feed, which only contains operational data, is sent to the SPI (Service Provider Interface) which doesn't include customer personal data, as set out in the contract.<br><br>Proposed data fields: Device ID, Last known location: Latitude and Longitude, Date and Time.<br><br>The trial does not involve any special category data.<br><br>The retention period will be reviewed 1 month after the trial commences and throughout the trial as required. The retention period for the data will not be fixed at the time the trial commences, while the project team assesses the utility of the data.<br><br>At the end of the trial any remaining GPS data will be depersonalised (by deleting the bike number) and will be handed back to TfL in digital form by secure transfer. This clause will be written into the contract.<br><br>TfL will then retain the data collected on SharePoint– in an access-restricted folder for the purpose of benefits realisation and retain it in accordance with GDPR provisions and the local Cycle Hire retention schedule. TfL will use a specific folder with restricted access to permissions to store the data returned to TfL so only those with a business need can access it.<br><br>TfL will not be processing bike location data in connection with criminal offences, but disclosures may be made to police where Schedule 2 Part 1 Section 2 of the 2018 Data Protection Act applies (prevention and detection of crime, or apprehension or prosecution of offenders).<br><br>Data is not limited to a specific location, group of individuals or geographical area. Bikes enabled with GPS devices will be randomly deployed at docking stations across London. |

| | |
|---|---|
| | It is proposed to update the Privacy Policy for Santander Cycles on the TfL website to advise customers that bikes are being tracked.<br><br>It is proposed to apply GPS stickers to terminals (and individual bikes) to advise customers that bikes are being tracked using GPS technology.<br><br>Wording for bikes:<br><br>TfL uses GPS to retrieve lost bikes<br><br>It is proposed to add stickers to the whole fleet (approx. 12,000 bikes) to act as a deterrent for criminals intent on stealing bikes.<br><br>Wording for terminals:<br><br>TfL uses GPS to support the retrieval of lost or stolen bikes. For more information visit tfl.gov.uk/privacy<br><br>Stickers will be added to terminals across the whole estate (approx. 800 terminals) |

| Step 4: Describe the context of the processing | |
|---|---|
| Is there a statutory basis or requirement for this activity?<br><br>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.)*<br><br>How much control will individuals have over the use of their data?<br><br>Would they expect you to use their data in this way?<br><br>Are there prior concerns over this type of processing or security flaws?<br><br>Is it novel in any way, or are there examples of other organisations taking similar steps?<br><br>What is the current state of technology in this area?<br><br>Are there any security risks?<br><br>Are there any current issues of public concern that you should factor in?<br><br>Are you or your delivery partner signed up to any code of conduct or certification scheme? | 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. Using GPS tracking to assist with loss prevention activities contributes to the provision of '*economic*' transport facilities.<br><br>Users of the Santander Cycles scheme can either be registered members (where personal information has been provided) or casual users, by hiring a bike using a payment card (ie 'turn up and go').<br><br>The Santander Cycles scheme already tracks journeys of all customers in limited way - due to the nature of the scheme infrastructure. As bikes are undocked and docked in a station, this creates a record and as a result all journeys taken will have a start and end location.<br><br>Adding GPS trackers will provide additional data showing all journeys taken, but with an extra benefit of providing last known location when a bike hasn't been docked at a station. Cycle hire had previously trialled RFID trackers on bikes to enable tracking of bikes on vehicles and in depot, but this was unsuccessful and discontinued.<br><br>While the use of GPS tracking within the Santander Cycles scheme is new, it is already deployed routinely across other public cycle hire schemes that have operated in the UK, including Lime, Mobike and Jump<br><br>Data will be transferred via encrypted VPN. Data will be stored in Google Cloud, which will be stored on UK based servers.<br><br>There may a public perception that this introduces a new level of 'surveillance' to journeys made by individuals in London. This will need to be addressed by being transparent about the use of GPS and the purposes it will be deployed for.<br><br>In terms of delivery partners, Serco and Beryl both have ISO27001 accreditation. |

| Step 5: Describe the purposes of the processing | |
|---|---|
| What do you want to achieve?<br><br>What is the intended effect on individuals?<br><br>What are the benefits of the processing – for TfL, for other external stakeholders, for the individuals concerned and for society in general? | The cycle hire scheme experiences loss of bikes due to various reasons, but predominantly customers not docking bikes correctly and this results in bikes being stolen or vandalised. Being able to track stolen/abandoned bikes will give the operational team visibility for the first time since the scheme went live in 2010 to understand what is happening with lost bikes.<br><br>This information will provide a valuable insight into improvements that can be made to the cycle hire infrastructure, quicker retrieval of bikes and criminal prosecutions. We anticipate a 25% reduction in bike loss as a result of this implementation and potential savings of £250,000 per annum.<br><br>It will also improve the availability of bikes to users. |

| Step 6: Consultation process | |
|---|---|
| **Consider how to consult with relevant stakeholders:**<br>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.<br>Who else do you need to involve within TfL?<br>Have you discussed information security requirements with CSIRT?<br>Do you plan to consult with external stakeholders? If so, who?<br>Who will undertake the consultation?<br>What views have been expressed by stakeholders? | The following Stakeholders have been engaged with:<br>Suppliers (Serco/Beryl)<br>Sponsor (Santander)<br>Press Office<br>Mayor's Office<br>All stakeholders currently consulted with have expressed positive comments towards the project.<br>It is not considered necessary for TfL to undertake consultation with Santander Cycles users themselves, particularly as this is a limited trial of GPS usage at this stage.<br>This is an operational change and does not have any customer touch points, therefore no consultation with customers is required. |

| Step 7: Assess necessity and proportionality | |
|---|---|
| **Describe compliance and proportionality measures, in particular:**<br><br>Does the processing actually achieve your purpose?<br><br>Is there another way to achieve the same outcome?<br><br>How will you prevent function creep?<br><br>How will you ensure data quality and data minimisation?<br><br>What information will you give individuals about how their data is used?<br><br>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? | Including GPS tracking on bikes will provide the improved operational visibility required to manage assets when they haven't been docked correctly by users and are subsequently, lost stolen or vandalised.<br><br>Lost bikes result in significant costs for TfL and we believe adding GPS trackers will support in driving this down.<br><br>The basis for this trial is for loss prevention purposes. It is anticipated that further uses of GPS will be developed over time, which may have benefits for TfL and improve the cycle hire scheme for users. A DPIA will be completed for each new potential deployment / use of GPS data.<br><br>For the purpose of data minimisation, there will no combining or data matching with personal information held about cycle hire scheme users, with the exception of processing necessary to respond to Subject Access Requests and/or Police requests for data, which may identify individuals. Police requests for GPS data will be processed by CPOS.<br><br>TfL staff will not have access to both systems. A staff member will not be able to have a DBOS log-in and Beryl log-in, eliminating the possibility of them being able to match data from both systems. Data returned to TfL in de-personalised format after the trial ends will not include bike asset numbers and therefore any data matching will be virtually impossible after the trial.<br><br>Bikes will have stickers attached. All bikes will have stickers irrespective of whether they have GPS enabled or not. Docking station terminals will also display information about the pilot and direct users to the privacy area of the TfL website for more information. The Santander Cycles privacy policy will also be updated.<br><br>The business will need to consider how Subject Access Requests will be handled where customers ask for the GPS data relating to the journeys they have made using the bikes.<br><br>Suppliers will be bound by their contractual obligations. TfL contracts also include audit rights; which will be fully exercised by the business. |

| | |
|---|---|
| **To be completed by Privacy & Data Protection team**<br><br>What is the lawful basis for processing?<br><br>How will data subjects exercise their rights?<br><br>How do we safeguard any international transfers?<br><br>Could data minimisation or pseudonymisation be applied?<br><br>Are data sharing arrangements adequate? | The lawful basis for processing in this case is Article 6 (1) (e) of the GDPR –<br><br>"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."<br><br>There is an existing process within TfL for data subjects to be able to exercise their rights:<br><br>Individuals will be able to exercise their information rights under Articles 15-21 of the GDPR (to be informed, (ii) of access, (iii) to rectification, (iv) to erasure, (v) to restrict processing, (vi) to data portability, (vii) to object and (viii) to automated decision-making including profiling). Each request will be considered on a case by case basis.<br><br>https://tfl.gov.uk/corporate/privacy-and-cookies/access-your-data<br><br>https://tfl.gov.uk/corporate/privacy-and-cookies/your-information-rights<br><br>No international transfers of data are intended<br><br>Measures for data minimisation are covered elsewhere in this DPIA |

| Step 8: Identify and assess risks | | | |
|---|---|---|---|
| **Describe source of risk and nature of potential impact on individuals**. Include risks of damage or distress as well as associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| **TfL or its service providers use the GPS data to match or combine with other customer personal data held to track an individual to a particular location on a given data or time** | Possible | Significant | Medium |
| **At the start of the trial there will be an absence of a fixed retention period for raw data that is no longer required (eg GPS data about successfully docked bikes)** | Possible | Minimal | Low – on the basis that this will be reviewed one month after the start of the trial and the periodically through the remaining trial period. The rationale for not applying this from the outset is that the raw data may be required by the police in order to investigate cycle hire related crime; including robberies and bike thefts |
| **At the start of the trial there will be an absence of an agreed time when the raw data is to be pseudonymized (hashed)** | Possible | Minimal | Low – on the basis that this will be reviewed one month after the start of the trial and the periodically through the remaining trial period. The rationale for not applying this from the outset is that the raw data may be required by the police in order to investigate cycle hire related crime; including street robberies and bike thefts |

| Step 9: Identify measures to reduce risk | | | | |
|---|---|---|---|---|
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| **TfL or its service providers use the GPS data to match or combine with other customer personal data held to track an individual to a particular location on a given data or time** | Proper internal data governance arrangements, including restricted access controls to any raw data during the trial as well as any depersonalised data;<br>Proper use of monitoring and audit rights in relation to service provider activities | Reduced | Low, | Yes |

| Step 10: Sign off and record outcomes | | |
|---|---|---|
| **Item** | **Name/date** | **Notes** |
| Measures approved by Privacy Team: | Lizzie Meadows 27/01/20 | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by Privacy Team: | Lizzie Meadows 27/01/20 | If accepting any residual high risk, consult the ICO before going ahead. |
| Privacy & Data Protection team advice provided: | Lizzie Meadows 27/01/20 | Privacy & Data Protection team should advise on compliance, Step 9 measures and whether processing can proceed. |
| Comments/recommendations from Privacy and Data Protection Team: | **Active, documented steps must be taken by TfL Cycle Hire to ensure Serco/Beryl both:**<br>**i) comply with data protection obligations and standard clauses are written in their respective contracts; and**<br>**ii) provide documented/contractual assurances that any data generated from the trial won't be utilised for monetary gain or other commercial purposes.**<br>**Details of the method of depersonalisation of the GPS tracking data must be recorded**<br>**The TfL privacy web page for Cycle Hire must be updated to include information on the GPS tracking trial (Action for the Privacy and Data Protection team).**<br>**A plan must be implemented to handle Subject Access Requests (SARs) for GPS data.**<br>**Engage with CPOS to ensure that any police requests for data are handled appropriately – and by the Data Disclosures team in the usual way.**<br>**A call or meeting to be set up between Cycle Hire Team and Privacy team one month after go-live to discuss initial findings and to discuss the retention period for the data going forward. Monthly catch ups to take place thereafter.** | |
| DPO Comments: | | |
| 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: | | If your decision departs from individuals' views, you must explain your reasons. |
| Comments: | | |
| This DPIA will kept under review by: | Cujic Branislav / Daniel Knight | 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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Data minimisation must be considered at every stage of the information lifecycle:<br>• when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary;<br>• 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.<br><br>Disclosing too much information about an individual may be a personal data breach.<br><br>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:<br>• The right to be informed;<br>• The right of access;<br>• The right to rectification;<br>• The right to erasure;<br>• The right to restrict processing;<br>• The right to data portability;<br>• The right to object;<br>• 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*."<br><br>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”.<br><br>This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations.<br><br>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.<br><br>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).<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>TfL adopts a layered approach to privacy notices, with clear links to further information about:<br>• Whether the information will be transferred overseas;<br>• How long we intend to keep their personal information:<br>• The names of any other organisations we will share their personal information with;<br>• The consequences of not providing their personal information;<br>• The name and contact details of the Data Protection Officer;<br>• The lawful basis of the processing;<br>• Their rights in respect of the processing;<br>• 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:<br><br>'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.<br><br>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.<br><br>The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes.<br><br>Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability.<br><br>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.<br><br>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:<br>• financial circumstances;<br>• health;<br>• safety;<br>• reputation;<br>• employment opportunities;<br>• behaviour; or<br>• choices |
| **Special Category data** | Special category data consists of information about identifiable individuals':<br>• racial or ethnic origin;<br>• political opinions;<br>• religious or philosophical beliefs;<br>• trade union membership;<br>• genetic data;<br>• biometric data (for the purpose of uniquely identifying an individual);<br>• data concerning health; or<br>• data concerning a person's sex life or sexual orientation.<br>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.<br><br>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:<br>• Traffic signs<br>• Traffic control systems<br>• Road safety<br>• Traffic reduction |

| | |
|---|---|
| | We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs).<br><br>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.<br><br>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:<br><br>• Occurring according to a system<br>• Pre-arranged, organised or methodical<br>• Taking place as part of a general plan for data collection<br>• Carried out as part of a strategy<br><br>Examples of activities that may constitute a regular and systematic monitoring of data subjects include:<br><br>• operating a telecommunications network;<br>• providing telecommunications services;<br>• email retargeting;<br>• data-driven marketing activities;<br>• 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);<br>• location tracking, for example, by mobile apps;<br>• loyalty programs; behavioural advertising;<br>• monitoring of wellness,<br>• fitness and health data via wearable devices;<br>• closed circuit television;<br>• 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. |