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:	[redacted]	Date DPIA completed	26/01/2021
Job title:	Data Scientist	Proposed launch date	

Name and description of the project:	Covid-19: Face Covering Compliance from CCTV Footage of LU Gate lines In June 2020 the Government made it a mandatory requirement for customers travelling on public transport to wear a face covering. However, it has been observed that some customers do not comply with this policy, putting everyone's safety at risk and leading to a perception that TfL isn't managing their safety effectively. This project is an exploratory one-off piece of work that aims to capture the percentage of people that don't comply with the face covering policy.

	CCTV recordings from cameras placed near the ticketing gates (30 stations) will be used to identify if customers are wearing a face covering whilst using public transport. Machine Learning / Deep Learning algorithms will be used to detect face coverings. There is no intention to identify any passengers. The output of the project will be a scorecard showing the overall level of compliance in each station, at a given time period. The processing is not likely to cause substantial damage or distress to passengers and is not carried out for the purposes of measures or decisions with respect to a particular passenger.				
Personal Information Custodian (PIC)	[redacted]	Is PIC aware of this DPIA?	Y	Project Sponsor	[redacted]

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.		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.		Process personal data without providing a privacy notice directly to the individual.	X

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.	

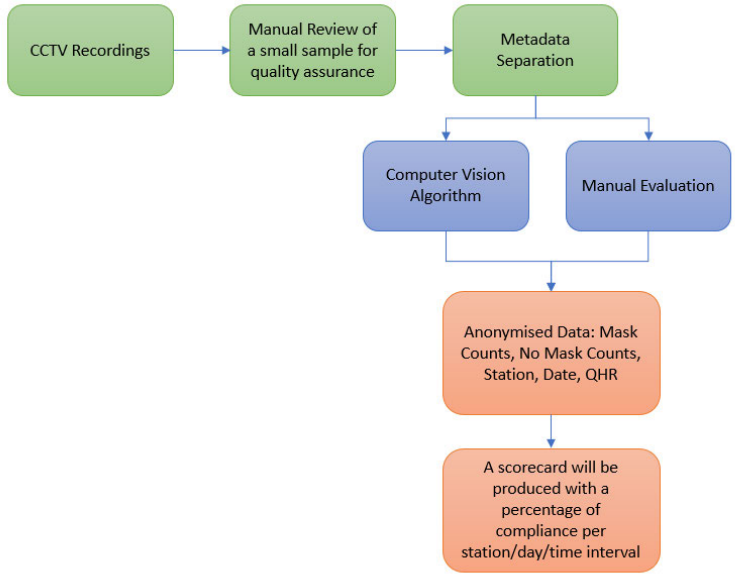
Step 1 – Identify the need for a DPIA	
Explain broadly what your project aims to achieve and what type of data and processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	In June 2020, face covering masks became mandatory on public transport to help reduce the spread of corona virus. It was quickly observed that some customers were not always complying with the rules. As a result, the Data Science team was tasked to identify the level of mask covering compliance and estimate the size of the problem. Because of the unique nature of the problem the Data Science team suggested the usage of footage from TfL CCTV cameras located near the gate lines. These recordings are capturing customers entering and exiting the stations. For the purpose of this exercise, the CCTV footage will be converted to still images and machine learning / deep learning algorithms will be used to detect face coverings. This project doesn't intend to identify any individuals or track their movements/activities within the network. Although the data that will be processed will be personal, the final output will be aggregated, and therefore anonymised, containing no personal identifiable information. At this stage the project is an exploratory piece of work, and this won't affect any individuals directly since we are capturing only the overall rate of mask covering compliance. It is worthwhile noting however, that this work may feed into wider operational decision-making processes in LU/TfL to better safeguard our staff, our customers and ensure compliance levels are high. Finally, if the outcome of the project is promising a second phase might follow and a new DPIA will be resubmitted.

Step 2: Describe the nature of the processing

How will you collect, use, and delete data? What is the source of the data?	**Collection:** The Data Science team will receive CCTV recordings from TfL cameras located near gate lines from approximately 30 stations. The exploratory stage will involve 400hrs worth of CCTV footage (40hrs per station for 10 stations). These recording will be provided by the CCTV Data Manager through a SharePoint site maintained by the corporate TfL OneLondon framework, with restricted permissions to the Data Science Team only and they will be password protected. **Use:** • Once the recordings are collected a member from the Data Science team will manually evaluate a small sample of the data to ensure good quality. • The recordings and the metadata (i.e. Date, Timestamp, location etc.) will be stored separately. This will prevent any user working with the files from having access to any other information about individuals who appear in the video. • The recordings will be converted to mp4 files using python. The conversion will be completed in a dedicated virtual machine with restricted permissions. • A semi-automated face covering detection process will follow. The mp4 files will be converted to still images and they will be labelled. A machine learning / deep learning algorithm will be used to detect face coverings. A member of the Data Science team will evaluate the results manually (they will have to view a small sample of the images) to ensure that the algorithm performs well. • The aggregated output will be joined with the metadata to help us identify any locations, dates or times with high non-compliance rates.

	• The outcome will be an aggregated result, namely counts of people that wear a mask versus those with no masks within a given station and at a given time interval. • The algorithms and outputs will be peer reviewed by a Data Scientist within D&A to ensure we have the lowest possible false positive rates. • Limitations: We won't be able to exclude children, people with mask exceptions and TfL staff. However, a disclaimer will be used when sharing the anonymised information. **Deletion:** This DPIA covers the first phase of the project which is an exploratory piece of work. If we are happy with the outcome it is very likely that a second phase will follow. The algorithm will be built based on the training data therefore the still images will be used in the second phase of the project as well. The raw data will be deleted after the conversion to still images. The still images will be deleted by the completion of the project (phase 1 and phase 2). We will review the DPIA every 3 months to continually assess the completion date of the project.
Will you be sharing data with anyone?	The CCTV recordings will be provided by the CCTV Data Manager and accessed / viewed by 2 members of the Data Science team within Data and Analytics. A technical architect within D&A will support with the data collection and data storage process. A Data Scientist from the D&A team will be assisting in peer reviewing and validating the quality of the output, therefore he will need to view a small sample of the data. The output data, which will be aggregated and contain no personal identifiable information, will be shared with internal stakeholders.

Are you working with external partners or suppliers?	No
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)	We won't share the data with external parties.
Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?	To ensure data integrity and validation, we may have to join the aggregated data with aggregated transactional data such as CPC and Oyster quarterly counts for the specific stations. The video and image files will not be combined with any other data source.
How and where will the data be stored?	The data will be uploaded by the CCTV Manager onto the SharePoint Site with restricted permissions and it will be then transferred to an Azure Storage Account. Once the data has successfully been transferred it will be deleted from the SharePoint site. A dedicated Virtual Machine will be used for the purposes of this project with restricted access to 4 D&A Data Scientists that will undertake the work. We will ensure that the metadata, the recordings and the still images will be stored separately.
Will any data be processed overseas?	No.

You might find it useful to refer to a flow diagram or other way of describing data flows.	 Figure 1: Data Processing Flow Diagram

Step 3: Describe the scope of the processing	
Who does the data relate to?	The data collected is CCTV footage of customers entering and exiting a selected group of LU stations. The footage will also include TfL Station staff.
How many individuals are affected?	Difficult to answer. This would depend on how many individuals were captured at the gateline CCTVs of the 30 stations we will be analysing.
Does it involve children or vulnerable groups? If children's data is collected and used, are they aged under 13?	It is not be possible to control who is in the recordings so, it is likely that children or vulnerable groups might be entering or exiting the stations and therefore will be included. However, they won't be personally identified or categorised as such in the output data.
What is the nature of the data? (Specify data fields if possible; For *example, name, address, telephone number, device ID, location, journey history, etc.*)	Recordings from CCTV cameras that capture customers and staff entering and exiting a selected group of LU stations.
Specify which special category data or criminal offence data are to be processed?	No special category data will be processed. The algorithms won't be able to determine individuals with mask exception.
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?	The data processed will be personal however, the output dataset will be aggregated and therefore anonymised. By separating out the video and associated metadata, we have ensured that even if an individual is identified by one of the project team reviewing the footage it will not be possible to infer when they were at a location, but the project team member reviewing footage for data quality, or reviewing

	a still, may be able to determine whether the individual was travelling with others. There is no way to anonymise or pseudonymise the raw data further and meet the project objectives. In addition, any incidents will be removed from the data.
How long will you keep the data? Will the data be deleted after this period?	This DPIA covers the first phase of the project which is an exploratory piece of work. If we are happy with the outcome it is very likely that a second phase will follow. The raw data will be deleted after the conversion to still images. The still images will be deleted by the completion of the project (phase 1 and phase 2). We will review the DPIA every 3 months to continually assess the completion date of the project.
Who is responsible for this deletion process?	The D&A Data Scientist ([redacted] will be responsible for the deletion process. It will be noted as a task during the project close process so it is carried out efficiently and will be overseen by the D&A Principal Data Scientist ([redacted]). Once the data has been deleted, we will inform the Privacy team and D&A Data Governance Manager ([redacted])
Is the data limited to a specific location, group of individuals or geographical area?	The data will be from LU Station CCTV cameras located at the gate lines of 30 LU stations.

Step 4: Describe the context of the processing	
Is there a statutory basis or requirement for this activity?	The use of face covering within the transport network is a mandatory requirement and aims to reduce the spread of coronavirus and keep both staff and customers safe. TfL has statutory powers to issue enforcement penalties to people who do not wear masks at transport terminals and do not have a valid exemption.
Are you or your delivery partner signed up to any code of conduct or certification scheme?	Not applicable.
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.)*	The individuals recorded are customers and staff
How much control will individuals have over the use of their data?	Our privacy statement for CCTV usage explicitly mentions that we may use this data for research and analysis purposes. CCTV & surveillance usage in TfL is shared with the public on our website and is not something individuals can opt out of: https://tfl.gov.uk/corporate/privacy-and-cookies/cctvThe final output will not contain any personal identifiable information.
Would they expect you to use their data in this way?	TfL makes frequent announcements and shares information on their website to inform the public that CCTV cameras are recording, being monitored and that the footage can be used to identify any incidents including "Protecting the health and safety of employees, customers and members of the public". This exploratory work aims to assist in this area

	by analysing the compliance rate of mask coverings to reduce risk against the Coronavirus.
Are there prior concerns over this type of processing or security flaws?	No. CCTV is being used widely and is a reliable technology. The algorithms we develop to identify face mask coverings will be peer reviewed and validated by a data scientist in D&A. The data storage and access controls will be reviewed by a D&A technical architect.
Is it novel in any way, or are there examples of other organizations taking similar steps?	Various universities have used similar data for similar purposes under academic research agreements with TfL. There have also been various internal projects with similar characteristics.
What is the current state of technology in this area?	Currently face mask coverings at stations is something that is being monitored manually by station staff who are escalating their concerns via management routes. This is not a systematic method as some station staff are more likely to report than others.
Are there any security risks?	See section 8.
Are there any current issues of public concern that you should factor in?	No, TfL informs the public regarding the usage of CCTV cameras within the network. Additionally, the output won't target any individuals. This process is not facial recognition as we won't match the images against any customer databases.

Step 5: Describe the purposes of the processing	
What do you want to achieve?	At this stage we want to understand if the available data will allow us to perform advanced analytical techniques and estimate the level of face covering compliance. If the exploratory work is successful it may feed into a wider operational decision-making process in LU/TfL to better safeguard our staff, our customers and ensure compliance levels are high (i.e. station announcements, posters, enforcement officers etc.)
What is the intended effect on individuals?	No effect.
What are the benefits of the processing – for TfL, for other external stakeholders, for the individuals concerned and for society in general?	By understanding the level of face covering compliance we might be able to inform decisions that will decrease the spread of the corona virus and help people feel safer using the transport network.

Step 6: Consultation process	
Consider how to consult with relevant stakeholders: Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.	Seeking the views from individuals whose data we will be collecting is not necessary for the nature of this work. The output will be aggregated and will better inform on the safety of staff and customers.
Who else do you need to involve within TfL?	It has already been established that we will involve: • D&A Data Science Team - [redacted], [redacted] [redacted] • D&A Data Governance Manager – [redacted] • D&A Build Team • CCTV Data Manager - [redacted] Other key stakeholders include: • Chief Data Officer - [redacted]

	• Privacy and Data Protection - [redacted]
Have you discussed information security requirements with CSIRT?	Yes. We had an outline discussion with CSIRT on 11 March (Deputy CISO, CSIRT Architect, CDO & Data Governance & Architecture Manager). We explained that this was TfL Confidential Data, and the guidance from CSIRT was that our data processing and storage solution must be in line with the safeguards required for TfL Confidential Data. Our technical solution for this activity will reflect this.
Do you plan to consult with external stakeholders? If so, who?	No
Who will undertake the consultation?	Not applicable
What views have been expressed by stakeholders?	The stakeholders believe that this will be a valuable solution in providing pertinent safety information on our network.

Step 7: Assess necessity and proportionality	
Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose?	The processing of CCTV recordings is necessary to achieve the objective of the project. The data will help us understand the face covering compliance levels and the outputs might help in operational decision-making. The analysis will be based on static data – real time data analysis doesn't seem possible for now due to the manual element in collecting the CCTV footage. However, real – time data could provide a more robust solution and depending on the value of the output and the flexibility of the process we might suggest it in the future.
Is there another way to achieve the same outcome?	We don't have any other data and with that coverage that could help with this project.

How will you prevent function creep?	This exploratory work has a tight controlled purpose and we do not envisage any function creep. Should we get enquiries to explore further, related or otherwise, we will notify the Privacy and Data Protection Team. If the research is successful, any further work to expand or modify the process will be subject to a new DPIA setting out appropriate controls for the proposed usage.
How will you ensure data quality and data minimisation?	Access to personally identifiable data will be restricted. The D&A Data Science team will perform data quality checks and make a record of any data cleansing, assumptions and exceptions. These will be peer reviewed and validated by a Data Scientist in D&A. The recordings and the metadata will be stored separately from any output storage locations.
What information will you give individuals about how their data is used?	TfL's privacy page (https://tfl.gov.uk/corporate/privacy-and-cookies/cctv) informs passengers how TfL, including its operating subsidiaries use personal data collected via CCTV across London's transport network.
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?	Not applicable.
To be completed by Privacy & Data Protection team What is the lawful basis for processing?	The Health Protection (Coronavirus, Wearing of Face Coverings on Public Transport) (England) Regulations 2020 (SI 2020/592) is a statutory instrument (SI) brought into force on 15 June 2020 by the Secretary of State for Transport, in response to the COVID-19 pandemic. It requires the wearing of a face covering when travelling on public transport in England. TFL public task to deliver a safe and reliable network that promotes healthy living. TfL ensure compliance with The Health Protection

	(Coronavirus, Wearing of Face Coverings on Public Transport) (England) Regulations 2020 (SI 2020/592) across London's transport network. This project will help estimate the level of face covering compliance. The face coverings have become mandatory within the transport network therefore, non-compliance is an unlawful act and jeopardises people's health safety.
How will data subjects exercise their rights?	TfL's access your data and your information webpage covers how data subject can exercise their right.
How do we safeguard any international transfers?	Non-Applicable
Could data minimisation or pseudonymisation be applied?	The metadata and the recordings will be separated. Any reported (EIRF) incidents will be removed from the recordings. The outcome will be an aggregated result, namely counts of people that wear a mask versus those with no masks within a given station and at a given time interval. Any counts less than five will be excluded.
Are data sharing arrangements adequate?	n/a

Step 8: Identify and assess risks			
Describe source of risk and nature of potential impact on individuals. Include risks of damage or distress as well as associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, Significant or Severe	**Overall risk** Low, medium or high
A third-party accessing SharePoint site.	Remote	Significant	Medium
A Data Scientist recognizing someone from the footage.	Possible	Significant	Medium

A Data Scientist sees an incident such as a crime or injury	Possible	Significant	Low
Public objections to use of data for this purpose	Possible	Significant	Medium

Step 9: Identify measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 8				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced or accepted	**Residual risk** Low, medium or high	**Measure approved** Yes/no
A third-party accessing SharePoint site.	The SharePoint is maintained by the corporate TfL OneLondon framework and permissions will be restricted to the D&A Data Scientists.	Accepted	Low	
A Data Scientist recognizing someone from the footage.	The Data Scientist will stop watching the footage, they will inform the Principal Data Scientist and the footage will be deleted.	Accepted	Low	
A Data Scientist sees an incident such as a crime or injury,	Any reported incidents (EIRFs) will be removed from the recordings prior to collections. The Data Scientist will stop watching the footage, they will inform the CCTV Manager and Principal	Accepted	Low	

	Data Scientist. The footage will be deleted.			
Public objections to use of data for this purpose	TfL informs the public regarding the usage of CCTV cameras within the network. Additionally, the output won't target any individuals. This process is not facial recognition as we won't match the images against any customer databases.	Accepted	Low	

Step 10: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:	[redacted] 23/03/2021	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:	[redacted] 23/03/2021	If accepting any residual high risk, consult the ICO before going ahead.
Privacy & Data Protection team advice provided:		Privacy & Data Protection team should advise on compliance, Step 9 measures and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:	The DPIA will be reviewed every 3 months by [redacted]	
DPO Comments:	Processing is good to proceed – [redacted] on behalf of DPO. 30/03/2021	
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):		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:	[redacted]	The DPO may also review ongoing compliance with DPIA.

Glossary of terms

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

Data minimisation	Data minimisation means using the minimum amount of personal data necessary, and asking whether personal data is even required. Data minimisation must be considered at every stage of the information lifecycle: • when designing forms or processes, so that appropriate data are collected and you can explain why each field is necessary; • when deciding what information to record, you must consider what information is required, what is relevant and whether any information is excessive; • when deciding whether to share or make use of information, you must consider whether using all information held about an individual is necessary for the purpose. Disclosing too much information about an individual may be a personal data breach. When deciding how long to keep information, you must consider what records you will need, and whether some personal data can be deleted or anonymised.
Data Protection Rights	The GDPR provides the following rights for individuals: • The right to be informed; • The right of access; • The right to rectification; • The right to erasure; • The right to restrict processing; • The right to data portability; • The right to object; • Rights in relation to automated decision making and profiling.
Data quality	The GDPR requires that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*." This means you must take steps to ensure that the data you use is sufficiently accurate, up to date and comprehensive for your purposes, and that you take steps to effectively mitigate any detriment to individuals that is likely to result from inadequate data.
Function creep	Function creep describes the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Review and update your DPIA, or undertake a new DPIA to reflect changes in the purpose or the means by which you process personal data.
Genetic data	Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

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

	• The names of any other organisations we will share their personal information with; • The consequences of not providing their personal information; • The name and contact details of the Data Protection Officer; • The lawful basis of the processing; • Their rights in respect of the processing; • Their right to complain to the Information Commissioner; • The details of the existence of automated decision-making, including profiling (if applicable).
Processing	Doing almost anything with personal data. The GDPR provides the following definition: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Profiling is the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymised data	Pseudonymisation separates data held about an individual from information that identifies the individual. This can be achieved by encrypting (hashing) the individuals name, MAC address or ID code, masking an individual's exact location or changing an image to make an individual unrecognisable. TfL can hold the same data in identifiable and anonymous form, provided appropriate controls are in place to prevent re-identification of the pseudonymised data. The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes. Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability. Pseudonymisation is an important security measure and must be considered as part of Privacy by Design and Default approach. If you use pseudonymised data you must ensure that an individual can not be re-identified with reasonable effort. The risk of re-identification is higher when information about the same individual is combined. For example, whilst a post code, a person's gender or a person's date of birth would be very unlikely to identify an individual if considered without other reference data, the

	combination of these three pieces of information would be likely to enable a motivated individual to re-identify a specific individual in most circumstances. If you use a "key" to encrypt or hide their identity you must ensure it is sufficiently protected to prevent the individual being re-identified. A Data Protection Impact Assessment can help you assess whether pseudonymisation is reversible in a given scenario.
Significant effects	A DPIA will be required for processing relating to an individual, or group of individuals that has an effect on their legal status or legal rights, or will otherwise affect them in a significant way. These effects may relate to a persons: • financial circumstances; • health; • safety; • reputation; • employment opportunities; • behaviour; or • choices
Special Category data	Special category data consists of information about identifiable individuals': • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data (for the purpose of uniquely identifying an individual); • data concerning health; or • data concerning a person's sex life or sexual orientation. Information about criminal convictions and offences are given similar protections to special category data under the Law Enforcement Directive.
Statutory basis for processing	TfL is a statutory body created by the Greater London Authority (GLA) Act 1999. This Act gives the Mayor of London a general duty to develop and apply policies to promote and encourage safe, integrated, efficient and economic transport facilities and services to, from and within London. The Act also states that we have a duty to help the Mayor complete his duties and implement the Mayor's Transport Strategy. In particular, we are required to provide or secure the provision of public passenger transport services, to, from or within Greater London. As a highway and traffic authority for GLA roads, we regulate how the public uses highways and we are responsible for: • Traffic signs

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

Vulnerable people	A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or others from harm or exploitation. All children are considered vulnerable by virtue of their age and immaturity.