F7526 A5 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:		Date DPIA completed	
Job title:		Proposed launch date	

Name and description of the project:					
Personal Information Custodian (PIC) or band 5 lead		Is PIC aware of this DPIA?	Y/N	Project Sponsor	

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.		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.	
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.	
What are the benefits for TfL, the individuals concerned, for other stakeholders and for wider society? How will you measure the impact?	
Will the processing directly affect the individuals concerned?	

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?		
Will you be sharing data with anyone?		
Are you working with external partners or suppliers?		
Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)		
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?		

Will the data be combined with, or analysed alongside, other datasets? If so, which ones?		
Will AI or algorithms be used to make decisions? What will the effect of these decisions be?		
How and where will the data be stored?		
Will any data be processed overseas? Which countries?		
Are you planning to publish any of the data? Under what conditions?		

Step 3: Describe the data		Could there be a privacy risk?
Who does the data relate to?		
How many individuals are affected?		
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		
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		

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?		
Can the objectives be achieved with less personal data, or by using anonymised or pseudonymised data?		
How will you ensure data quality, and ensure the data is accurate? How will you address any limitations in the data?		
How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process? 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?		
Is there any use of Artificial Intelligence or automated decision making?		
Will individuals have control over the use of their data? If so, how can they control it?		
Would they expect you to use their data in this way?		
What information will you give individuals about how their data is used? Is there a privacy notice? Are any risks explained?		
Are there prior concerns over this type of processing or security flaws?		
Is it novel in any way, or are there examples of other organisations		

taking similar steps?		
What is the current state of technology in this area? Is this innovative or does it use existing products?		
What security risks have you identified?		
Are there any current issues of public concern that you should factor in?		
Is the processing subject to any specific legislation, code of conduct or certification scheme?		
Will there be any additional training for employees?		
Does the processing actually achieve your purpose?		
Is there another way to achieve the same outcome?		
Who will own this initiative and ensure there is no function creep without a review of this DPIA?		

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.		
Which business areas have been consulted within TfL?		
Have you discussed information security requirements with CSIRT? If so, who is your contact in CSIRT?		
Do you plan to consult with external stakeholders? If so, who?		
Who will undertake the consultation?		
What views have been expressed by stakeholders?		

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?**

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?**

What is the lawful basis for processing? Are there any Special Category or sensitive data?	**To be completed by Privacy & Data Protection team**	Could there be a privacy risk?
Is this use of personal data compatible with our original purposes for collecting the data?		
Are changes to Privacy Notice required?		
How will data subjects exercise their rights?		
How do we safeguard any international transfers? Is any data being processed outside the UK?		
Could further data minimisation or pseudonymisation be applied?		
Have appropriate security measures been considered, with CSIRT involvement where necessary?		
Are data sharing arrangements adequate? Do they require further documentation?		
Is the data likely to be and remain adequate, accurate and up to date?		

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by Privacy Team:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by Privacy Team:		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, transparency and whether processing can proceed.
Comments/recommendations from Privacy and Data Protection Team:		
DPO Comments:		
PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor):		If overruled, you must explain your reasons below.
Comments:		
This DPIA will kept under review by:		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.
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 individual's 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.