

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: | Lizzie Meadows | Date DPIA completed | May 2021 | | |
| Job title: | Principal Privacy Adviser | Proposed launch date | Expected to be June/July 2021 | | |
| Name and description of the project: | <p>TfL's participation in a National Register of Taxi and Private Hire driver licence refusals and revocations (known as NR3). It will involve TfL's Taxi and Private Hire Department (TPH) uploading certain fields of driver data which will be accessible to other taxi and private hire licensing authorities across England and Wales. Its purpose is to ensure that information about a driver who has had a licence refused or revoked in the past is available to other licensing authorities if they receive an application from the same individual. This enables a fully informed decision to be made on whether that person is 'fit and proper' to hold a licence in future. TfL will be a provider of information and will also access information added to the register by other taxi and private hire licensing authorities where they have revoked or refused a licence in their area.</p> | | | | |
| Personal Information Custodian (PIC) | Helen Chapman / Graham Robinson | Is PIC aware of this DPIA? | Y | Project Sponsor | |

Printed copies of this document are uncontrolled
 Issue no. A3 Issue date: November 2018



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. | Y |
| 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. | Y |
| Use new technologies or make novel use of existing technologies. | | Process personal data on a large scale or as part of a major project. | Y | 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. | Y | 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.

TfL is required to satisfy itself that those holding a taxi or private hire driver licence are 'fit and proper' to do so. This is done firstly during the application (or renewal) for a licence, and then at any time during the currency of a licence.

Presently, there is no consistent way of establishing whether an individual has had a licence refused or revoked in another area for failing to be 'fit and proper'. It relies on the applicant self declaring the information. This means that information about an applicant's past behaviour may be missed and an individual might be able to obtain a new taxi or private hire driver licence in another area, despite having their licence revoked or refused elsewhere.

The creation of the national NR3 Register will help prevent people found to be not fit and proper in one area from securing a licence somewhere else through deception and non-disclosure.

The National Register of Taxi Licence Revocations and Refusals ('NR3') has been created by the Local Government Association (LGA). It allows taxi and private hire licensing authorities (primarily local councils – but also TfL) to record details of individuals where their taxi or private hire licence application has been refused by that licensing authority or their licence revoked. Licensing authorities will also be able to check the register to see if a new or renewing applicant has previously had a licence refused or revoked elsewhere.

The overall purpose of the Register is to provide a consistent means for all licensing authorities to make decisions on whether an individual is 'fit and proper' and so improving public safety for all users of taxi and private hire services in the UK.

The LGA has commissioned the National Anti Fraud Network (NAFN) to develop and host the Register. NAFN is a shared service, hosted by Tameside Metropolitan council, which supports public authorities to tackle fraud and share intelligence.

In July 2020, the Department for Transport produced Statutory Standards stating that all licensing authorities should participate in the Register. (See sections 4.20 – 4.25 of the [DfT Statutory taxi and private hire vehicle standards](#).)

Basic licensee information will be recorded in the NR3 – it will *not* include the reason for the refusal or revocation.

If the licensing authority requires more detail about the refusal/revocation e.g. to further verify it is the same individual and/or the specific reasons for the previous decision) they will need to make a request for further information directly to that authority.

More information can be found on the LGA website:

<https://www.local.gov.uk/topics/licences-regulations-and-trading-standards/new-national-register-taxi-and-private-hire>

TfL will upload 'current data' to the Register on an ongoing basis (i.e. where an application has recently been refused or licence revoked) – but it will also upload historical revocations and refusals data. When it commences participation (expected to be June/July 2021), TfL intends to upload historical data, dating back to 1 January 2018. This will equate to approximately 4650 records.

The need for a DPIA has been identified because:

- The activity constitutes the processing of personal data on a large scale.
- The retention period for records in the Register will be 25 years. (This is specified by the Local Government Association and TfL has no role in deciding the retention period for the NR3 register).
- TfL's participation in the Register will result in significantly more people (from third party licensing authorities) having access to licensee personal data.

Step 2: Describe the nature of the processing

How will you collect, use, and delete data? What is the source of the data?

Will you be sharing data with anyone?

Are you working with external partners or suppliers?

Is there an agreement/contract in place with the third parties? (If so, please provide a copy with the assessment.)

Will the data be combined with, or analysed alongside, other datasets held by TfL? If so, which ones?

How and where will the data be stored?

Will any data be processed overseas?

You might find it useful to refer to a flow diagram or other way of describing data flows.

The data fields below will relate specifically to individuals who have had taxi and private hire driver applications refused or licences revoked. It does not include individuals who have had their licences suspended, nor does it include operator or vehicle applications or licences:

- a) Name;
- b) Date of Birth
- c) Address
- d) Driving Licence Number
- e) National Insurance Number
- f) Telephone Number
- g) E mail address
- h) Licence Type: (Hackney / Private Hire / Dual)
- i) Licensing action (revocation or refusal)
- j) Date of action / date action took effect

This information will be derived from TPH's licensing database, and is a mix of data provide by the individual in order to apply for the licence, as well as the licensing action which is generated by TfL.

The data fields will be added by TfL to the NR3 Register in respect of revoked or refused TPH licences and will be accessible to the other participating licensing authorities. (There are in the region of 350 taxi and private hire licensing authorities in the UK.)

Equivalent data added by other licensing authorities participating in the Register will be visible to TfL

The NR3 Register will be hosted by Tameside Metropolitan Borough Council of behalf of the NAFN.

There is a data processor agreement between TfL and Tameside Metropolitan Borough Council.

There is a data sharing agreement in place between TfL and the other participating licensing authorities.

Access to the Register is only possible where the licensing authority:

- 1 is a current member of NAFN
- 2 has signed the data processor agreement
- 3 has signed the data sharing agreement

In terms of the physical location of the servers, these are maintained by Rochdale Metropolitan Borough Council under a SLA with NAFN.

There will not be any processing of personal data overseas. Any subsequent processing of the Register outside the EEA is subject to approval from the participating authorities.

TfL – and the other licensing authorities - will use the information in the NR3 Register as the basis for making further enquiries as to the circumstance of a licence revocation or application refusal. This in turn will help inform the decision to award a licence in response to the current application. The information obtained as a result of those further enquiries will be stored against the driver or application record held in the TPH database, or equivalent databases operated by the other licensing authorities.

Step 3: Describe the scope of the processing

Who does the data relate to?
 How many individuals are affected?
 Does it involve children or [vulnerable](#) groups?
 If children's data is collected and used, are they aged under 13?
 What is the nature of the data? (Specify data fields if possible; For example, name, address, telephone number, device ID, location, journey history, etc.)
 Specify which [special category data](#) or criminal offence data are to be processed?
 Can the objectives be achieved with less [personal data](#), or by using [anonymised](#) or [pseudonymised data](#)?
 How long will you keep the data? Will the data be deleted after this period? Who is responsible for this deletion process?
 Is the data limited to a specific location, group of individuals or geographical area?

The data relates to previous Taxi or Private Hire driver licence holders or applicants. TfL will also upload three years' worth (i.e. from 2018-onwards) of previous refusal and/or revocation data on commencement of its participation in the Register. This will equate to information about approximately 4650 individuals.

Subsequently, data will be added on at least a weekly basis; volumes will vary according to the numbers of licence revocations or application refusals in each week.

The processing does not involve children or vulnerable groups.

The data fields stored in the Register are listed in Step 2 of this DPIA

There will be no special category data stored in the NR3 Register itself. Responses received by TfL following subsequent enquiries made about the reason for a licence refusal or revocation to another authority may include some special category data, ie health related information and/or criminal offence data. Similarly TfL may disclose special category information in response to a request made by another licensing authority. TfL will consider all such requests on a case by case basis and in line with existing processes for handling third party requests for personal data.

The objectives (ie the decision whether to award or renew a TPH licence) can only be achieved using personal data. The minimum data necessary will be stored in the NR3 Register itself. Further information will only be provided following a specific request from an individual licensing authority.

The standard retention period for the register is 25 years. This is specified by the Local Government Association and TfL has no role in deciding the retention period for the Register. TfL has the right to request the deletion of records from the NR3 Register at any time

TfL's own retention period for licence applications is 7 years following expiry or refusal or revocation of that licence. (This represents 2 licensing cycles (3 years each) plus one year).

Given that the proposed retention period for the data held within the NR3 Register itself is 25 years. TfL would be unable to respond to enquiries about revocations or refusals where that decision was made more than 7 years previously. This is further considered in the Risk section of this DPIA.

The existence on the NR3 Register of a record of a refusal or revocation without any evidence to support that record means that the record may be inadequate. If the unsupported record has material effect on an applicant who claims it is inaccurate TfL may lack evidence to defend against a claim.

The data held is limited to those people who have held or applied for a TPH driver licence that has been revoked or refused since 1 January 2018. It will not comprise the entire list of licensed taxi and private drivers. The data is not limited by geographical location, as a TfL TPH licensee may reside in any part of the UK.

Step 4: Describe the context of the processing

Is there a [statutory basis](#) or requirement for this activity?

What is the nature of TfL's relationship with the individuals?
(For example, the individual has an oyster card and an online contactless and oyster account.)

How much control will individuals have over the use of their data?

Would they expect you to use their data in this way?

Are there prior concerns over this type of [processing](#) or security flaws?

Is it novel in any way, or are there examples of other organisations taking similar steps?

What is the current state of technology in this area?

Are there any security risks?

Are there any current issues of public concern that you should factor in?

Are you or your delivery partner signed up to any code of conduct or certification scheme?

Participation by licensing authorities in the Register is currently voluntary; however the Government supported the view in the recent [Task and Finish Report](#) (Recommendation 23) that participation in this Register should become mandatory in the future. [Statutory Standards](#) published by the DfT in July 2020 further confirmed that all licensing authorities should participate in the Register.

TfL recognises that the existence of the Register means that intelligence about an applicant's past behaviour can be shared in a controlled manner. It will directly contribute to a licensing authority being able to make an informed decision on an individual's fitness to hold a licence, and therefore contribute directly to maintaining public safety for all users of taxi and private hire services in London (and indirectly, in other licensing areas).

As such it forms part of TfL statutory function as the regulator of taxi and private hire services in London under the following:

- Greater London Authority Act 1999
- Private Hire Vehicles (London) Act 1998
- Private Hire Vehicles (London PHV Driver's Licences) Regulations 2003
- London Cab Order 1934

Individuals will have limited control over the inclusion of their data in the Register by TfL and TfL will not be relying on consent as a relevant processing condition.

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.

This is the first time a national database of this kind has been created for this purpose. As such it is difficult to say whether this processing would be within the legitimate expectation of data subjects. However this is likely to be mitigated by the fact that the purpose of the NR3 Register is to improve public safety and ensure only 'fit and proper' persons are able to obtain a taxi or private hire licence. Statutory standards published by the DfT in July 2020 state: *"An applicant should also be required to disclose if they have had an application for a licence refused, or a licence revoked or suspended by any other licensing authority."*

It is possible that trades unions or other trade bodies may have concerns; particularly relating to the proposed retention period for the Register; however there has been limited evidence of this to date (the Register went live in July 2018) and the NR3 Register is already being used by a large number of licensing authorities. In addition the [DfT Statutory Standards](#) were subject to consultation and the measures/recommendations were found to be

| | |
|--|---|
| | <p>proportionate.</p> <p>The Register will be hosted in a Public Services Network (PSN) compliant environment. The PSN is a government-approved network which helps public sector organisations work together and share/access data securely over the internet. Access itself will be by specifically authorised users, and will require 4 factor authentication: a unique username, password, pin code and 3 co-ordinates from a user grid card.</p> |
|--|---|



Step 5: Describe the purposes of the processing

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the [processing](#) – for TfL, for other external stakeholders, for the individuals concerned and for society in general?

The overall purpose of the NR3 Register is to facilitate more efficient cooperation between the licensing authorities and enable them to share information which will allow them to identify persons that have had a taxi or private hire driver's licence revoked or application refused by another authority. This in turn will improve public safety for users of taxi and private hire services, not just in London, but elsewhere in the UK.

Previously if drivers do not disclose information themselves about a previous revocation or refusal of a licence, there is often no way for an authority to find this information out (without writing to each individual licensing authority for each individual application). This means that information about an applicant's past behaviour would be missed and an individual might be able to get a new licence in another area, despite having their licence taken away elsewhere.

The benefits include:

Improved public safety as additional check can be undertaken to ensure an applicant's fitness to hold a licence;

Enables TfL to better carry out its obligations as regulator of taxi and private hire services in London

Enables other taxi and private hire regulators in England and Wales to better carry out their obligations as regulators

Step 6: Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek views from the individuals whose data you will be collecting – or justify why it's not appropriate to do so.

Who else do you need to involve within TfL?

Have you discussed information security requirements with CSIRT?

Do you plan to consult with external stakeholders? If so, who?

Who will undertake the consultation?

What views have been expressed by stakeholders?

The NAFN / LGA undertook some limited consultation during 2017 (largely with licensing bodies) and sought legal advice.

Information was also available on various driver forums online, for example:

<https://www.taxi-driver.co.uk/phpBB2/viewtopic.php?f=2&t=31327>

The DfT, who produced the Statutory taxi and private hire vehicle Standards (which includes the recommendation to participate in the NR3 register) also consulted prior to formal publication. A [summary of the consultation responses](#) can be found online.

It is not intended that TfL will consult with affected individuals. However, there will be an awareness exercise which may include at least the following:

- Article(s) in 'On Route'
- The Publication of an official TPH Notice
- Updates to the TPH privacy page
- Updates to other TPH correspondence templates
- Letters to historic licence holder / applicants affected
- Highlighting the changes via regular calls that take place with Senior Trade Representatives and larger private hire operators.

Step 7: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

Does the [processing](#) actually achieve your purpose?
 Is there another way to achieve the same outcome?
 How will you prevent [function creep](#)?
 How will you ensure [data quality](#) and data [minimisation](#)?
 What information will you give individuals about how their data is used?
 What measures do you take to ensure suppliers processing personal data on our behalf provide adequate assurances about their ability to process this data safely and lawfully?

The processing does achieve the purpose as it removes the reliance on individuals self-declaring previous revocations / refusals.

All participating licensing authorities will need to guard against function creep. It is possible that such a large repository of taxi and private hire data in a single place will attract requests or proposals for further use or requests to routinely access the data from other bodies such as the police or other statutory law enforcement agencies. Should this be the case, TfL would expect NAFN to consult with all licensing bodies on the privacy / data protection issues this raises and the associated function creep.

TfL will provide records held within the Taxi and Private Hire licensing database which are already subject to internal data quality measures. The minimum data possible will be shared in order to achieve the purpose. All licensing authorities will be sharing the same data fields. All follow up requests from licensing authorities to TfL will be handled on a case by case basis (in accordance with existing processes) to ensure that only the minimum data is disclosed for the purpose.

TfL will take several steps to inform all affected individuals about how their data will be used. This is described in Step 6 of this DPIA.

TfL has sought further information from NAFN as the role of Tameside Metropolitan Borough Council - in particular how they will manage the role of data processor in addition to also being a user of the NR3 Register as licensing authority in their own right. They have responded:

“The system has been designed and developed so that only officers within the same organisation and department can view their own organisation’s records.

- *No organisation is able to search the register unless they have agreed/signed the NR3 Data Sharing Agreement. Tameside MBC have complied with this requirement.*
- *Managers can view their staff and their own licensing authority record entries.*
- *Where a search identifies a match, the only data that is returned to the enquirer is the contact details of the licensing authority which is responsible for the data entry. If the record belongs to the same authority and department conducting the search then the full details of the match are provided.”*

TfL has entered into a written data processor agreement with NAFN in relation to the hosting of the Register. This data processor agreement contains rights of audit as well as the obligation to provide reasonable assistance

To be completed by Privacy & Data Protection team

What is the lawful basis for processing?

How will data subjects exercise their [rights](#)?

How do we safeguard any international transfers?

Could data [minimisation](#) or [pseudonymisation](#) be applied?

Are data sharing arrangements adequate?

to TfL in the completion of any DPIA.

The lawful basis for processing in this case is Article 6 (1) (e) of the GDPR –

“The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

In respect of any special category, or criminal convictions personal information disclosed in response to a further query, the relevant processing conditions are found in Article 9 (2) (g) of the UK GDPR:

“The processing is necessary for reasons of substantial public interest, on the basis of domestic law, which shall be proportionate to the aim...”

Also, Schedule 1 Part 2 of the Data Protection Act 2018:

Paragraph 6: *“The processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law – and is necessary for reasons of substantial public interest”*

There is an existing process within TfL for data subjects to be able to exercise all their information rights:

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.

<https://tfl.gov.uk/corporate/privacy-and-cookies/access-your-data>

<https://tfl.gov.uk/corporate/privacy-and-cookies/your-information-rights>

Pseudonymisation is not an option in this case as the processing requires individuals to be identifiable. The data fields accessible within the Register are the minimum necessary to allow a licensing authority to identify a potential licence applicant of concern. More detailed/sensitive data is only available to licensing authorities upon further request which must demonstrate proportionality and justification.

A data sharing agreement has been drafted by the NAFN for all participants to use and which must be signed up to before access is granted to the NR3 Register.

A data processor agreement has also been drafted by the NAFN for all participants to use and which must be signed up to before access is granted to the Register.

| 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 |
| The retention period for the NR3 is not aligned with TfL's own retention period for TPH licensee data. This could mean that the reasons for a TfL refusal could not be substantiated. | Probable | Significant | High |
| Function creep – whereby use of the NR3 Register is sought for other purposes by other third party organisations or local or central government | 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 |
| The retention period for the NR3 is not aligned with TfL's own retention period for TPH licensee data. This could mean that the reasons for a TfL refusal could not be substantiated | Align the retention period with TfL's own schedule | Eliminated | Low | Not possible as the retention in NR3 register data is outside TfL control. |
| | Seek manual deletion of TfL data from NR3 Register after 7 years | Reduced | Medium | No, on basis of being impractical to implement for a large volume of records. |
| | Consider whether to extend TfL's own retention period for licence information, or to retain at least a skeleton record in the case of revoked or refused licences to enable a summary of the rationale to be disclosed on request if required. | Reduced | Medium (this option would require a DPIA in its own right) | Yes |
| Function creep – whereby use of the NR3 Register is sought for other purposes by other third party organisations or local or central government | No changes to purpose of Register without consultation of all partners, further DPIA, and consultation with trades bodies | Reduced | Low | Yes |

| Step 10: Sign off and record outcomes | | |
|--|--|---|
| Item | Name/date | Notes |
| Measures approved by Privacy Team: | Head of Privacy and Data Protection 11/05/2021 | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by Privacy Team: | Head of Privacy and Data Protection 11/05/2021 | If accepting any residual high risk, consult the ICO before going ahead. |
| Privacy & Data Protection team advice provided: | Head of Privacy and Data Protection 11/05/2021 | Privacy & Data Protection team should advise on compliance, Step 9 measures and whether processing can proceed. |
| Comments/recommendations from Privacy and Data Protection Team: | Approved to proceed, but, Taxi and Private Hire (in conjunction with the Privacy and Data Protection team) must conduct a review of retention in respect of records of refusals and revocations within 12 months, to avoid the possibility of being unable to substantiate data on the NR3 register. Amendment and additions to the current privacy notice also provided by the Privacy and Data Protection team. | |
| DPO Comments: | In addition to the comments above, TPH must maintain active oversight of the operation of the data processor agreement with Tameside MBC and the data sharing agreement with other participating licensing authorities. | |
| PDP Team / DPO advice accepted or overruled by (this should usually be the Project Sponsor): | Yes | If overruled, you must explain your reasons below. |
| Comments: n/a | | |
| Consultation responses reviewed by: | n/a | If your decision departs from individuals' views, you must explain your reasons. |
| Comments: n/a | | |
| This DPIA will kept under review by: | Graham Robinson, General Manager Taxi and Private Hire | The DPO may also review ongoing compliance with DPIA. |

Glossary of terms

| | |
|----------------------------------|---|
| Anonymised data | <p>Anonymised data is information held in a form that does not identify and cannot be attributed to individuals.</p> <p>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.</p> <p>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.</p> <p>If information can be linked to an identifiable individual the data is not anonymous and you must treat it as personal data.</p> |
| Automated Decision Making | <p>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.</p> |
| Biometric data | <p>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.</p> <p>Biometric data is subject to additional safeguards under the GDPR when it is processed for the purpose of identifying individuals.</p> |
| Data breaches | <p>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.</p> |
| Data minimisation | <p>Data minimisation means using the minimum amount of personal data necessary, and asking whether personal data is even required.</p> <p>Data minimisation must be considered at every stage of the information lifecycle:</p> <ul style="list-style-type: none">• 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. |

| | |
|-------------------------------|---|
| | <p>Disclosing too much information about an individual may be a personal data breach.</p> <p>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.</p> |
| Data Protection Rights | <p>The GDPR provides the following rights for individuals:</p> <ul style="list-style-type: none"> • 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 | <p>The GDPR requires that <i>"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."</i></p> <p>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.</p> |
| Function creep | <p>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.</p> |
| Genetic data | <p>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.</p> |
| Marketing | <p>Direct marketing is "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".</p> <p>This covers all advertising or promotional material directed to particular individuals, including that promoting the aims or ideals of not-for-profit organisations.</p> <p>Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects</p> |

| | |
|-----------------------|--|
| | <p>details to use in future marketing campaigns, the survey is for direct marketing purposes and the privacy regulations apply.</p> <p>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).</p> <p>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.</p> |
| Personal data | <p>Personal data is information, in any format, which relates to an identifiable living individual.</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| Privacy notice | <p>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.</p> <p>TfL adopts a layered approach to privacy notices, with clear links to further information about:</p> <ul style="list-style-type: none"> • 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; |

| | |
|---------------------------|--|
| | <ul style="list-style-type: none"> The details of the existence of automated decision-making, including profiling (if applicable). |
| Processing | <p>Doing almost anything with personal data. The GDPR provides the following definition:</p> <p>‘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</p> |
| Profiling | <p>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.</p> |
| Pseudonymised data | <p>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.</p> <p>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.</p> <p>The advantages of pseudonymisation are that it may allow further processing of the personal data, including for scientific, historical and statistical purposes.</p> <p>Pseudonymised data (if irreversible) is not subject to the individuals rights of rectification, erasure, access or portability.</p> <p>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.</p> <p>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.</p> |

| | |
|--|--|
| <p>Significant effects</p> | <p>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:</p> <ul style="list-style-type: none"> • financial circumstances; • health; • safety; • reputation; • employment opportunities; • behaviour; or • choices |
| <p>Special Category data</p> | <p>Special category data consists of information about identifiable individuals':</p> <ul style="list-style-type: none"> • 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. <p>Information about criminal convictions and offences are given similar protections to special category data under the Law Enforcement Directive.</p> |
| <p>Statutory basis for processing</p> | <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Traffic signs • Traffic control systems • Road safety • Traffic reduction |

| | |
|---|---|
| | <p>We are also the licensing authority for hackney carriages (taxis) and private hire vehicles (minicabs).</p> <p>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 11 of the Act.</p> <p>Activities may have a statutory basis related to other legislation, for instance the requirements to publish information under the Local Government Transparency Code.</p> |
| <p>Systematic processing or monitoring</p> | <p>Systematic processing should be interpreted as meaning one or more of the following:</p> <ul style="list-style-type: none"> • 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 <p>Examples of activities that may constitute a regular and systematic monitoring of data subjects include:</p> <ul style="list-style-type: none"> • 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. |
| <p>Vulnerable people</p> | <p>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.</p> |