Privacy and data protection

A guide for private hire operators

TAXI·PRIVATE HIRE

EVERY JOURNEY MATTERS

Introduction and scope

Transport for London (TfL) introduced a number of changes to the regulation of London private hire vehicle (PHV) operators during 2016. In addition there have been significant changes to the law on data protection.

Some of these changes affect the way you handle personal information, for example the requirement to keep records of customer bookings, complaints and lost property – and obligations to provide TfL with details of the drivers and vehicles available or used by you to carry out private hire bookings.

To help you comply with these responsibilities and legal requirements relating to privacy and data protection, we have created this guide as a summary of obligations and best practice which apply to handling personal information.

It is aimed at the way you handle your customers' personal information, as well as the personal information of any employees or others that may work with you or for you. It is intended to assist those operators putting data protection measures in place for the first time or if you're refreshing existing policies and procedures.

The guide has been prepared for information purposes only and it has no legal effect in or of itself. Further information resources are identified below including where you may go for advice and further guidance.

What is the data protection legislation and who has to comply?

In May 2018, significant changes to data protection legislation were introduced. The Data Protection Act 1998 was replaced by new EU legislation – the General Data Protection Regulation ('GDPR') as well as a new UK Data Protection Act 2018, which supplements the GDPR.

Both of these laws introduce new, higher compliance standards for organisations and businesses that handle personal data – and also give individuals more control over their personal information and how it is used.

If your business collects, stores or handles personal information about customers, employees, drivers (or other people), then you are legally obliged to protect that information, and the data protection legislation applies to you.

If you have a website, or a mobile app, or send your customers marketing messages by email, text or other electronic message, then you also need to take account of the Privacy and Electronic Communications Regulations 2003 (PECR) which contain the rules around using cookies and online marketing/advertising. Please refer to the Help section at the end of this guide for more resources on this.

This guide will generally refer to the GDPR throughout (rather than the term 'data protection legislation'); and also use the terms 'personal information' and 'personal data' interchangeably.

Think Privacy!

It is beneficial to think about privacy in the context of the technology you use, your business practices and even the design of your physical premises or work space. Including privacy considerations in all your activities will help you to minimise risk and build trust with your customers and employees. This is known as 'data protection by design and default' and ensures that data protection is an essential part of the design of your systems, services and business practices.

You should also consider undertaking a Data Protection Impact Assessment (DPIA) to help you assess any privacy risks of any new project or innovation involving personal information. Examples might include using facial recognition, tracking your customers' or drivers' locations, creating new databases or new types of data matching or profiling. Find out more about when and how to carry out a DPIA

If you are considering significant changes to the way you handle personal information – for example new tracking technologies, or using facial recognition or other biometric tools, you should let TfL know in advance of implementing any changes.

What is the Information Commissioner's Office?

The Information Commissioner's Office (ICO) is the UK's independent regulator created to uphold information rights and promote good practice. They deal with privacy related complaints and take action to ensure that businesses and organisations of all kinds comply with their data protection responsibilities. The ICO also publishes practical guidance to help those trying to comply with their obligations.

What is the 'data protection fee'?

It is a legal requirement for organisations and businesses that process personal information to pay a data protection fee to the ICO every year and it is an offence punishable by a financial penalty if you do not. The ICO publishes an online register of the organisations and businesses that have paid the fee. The level of fee you have to pay will vary according to the turnover of your business and the number of members of staff you have.

If you had an old style 'notification' on the ICO Register of Data Controllers, they should contact you near the date it would have been due for its annual renewal, with details of what to do. If you have never notified with the ICO before, you must start paying the data protection fee as appropriate.

You can find out more by reading the ICO guide to the data protection fee.

Personal information and other important definitions

If you collect, use or store information about identifiable individuals using a computer or mobile device, a website or a manual (paper) filing system, then you are likely to be 'processing' personal information – and also be a 'data controller'.

Being a data controller means that you are responsible for making the decisions about **how** and **why** you handle that personal information. A data controller can be an individual (ie a sole trader) or an organisation/business of any size.

In the context of private hire services, 'personal information' includes:

- records about your customers, for example – names, phone numbers, photographs, accessibility/mobility information, collection and destination addresses, booking information such as date and time, payment card or smartphone data, lost property, and complaints; and
- information about people who may work for you or supply your business; such as names, addresses, phone numbers, HR records, payroll and bank account records, other identifiers such as badge, licence or employee numbers, photos, driver licensing data, and vehicle information.

Personal information can be in any format, including paper and computer-based records, audio recordings, CCTV, images such as route maps, location data and expressions of opinion. It also doesn't have to be about an explicitly named person, so if you can identify someone from a description of them, or by putting different pieces of data together, that's also personal information

The term 'processing' has a very wide definition and includes almost anything you would do to personal information, from the moment you collect it, while you store it and until you finally delete it.

Accountability and governance

Accountability is one of the core data protection principles under the GDPR - it makes you responsible for complying with its legal requirements and says that you must keep records so you can provide evidence of compliance. In practice, this means taking the following steps:

- Being proactive about incorporating data protection into all your activities by default;
- Creating (or updating) and implementing data protection policies or procedures for your business;

- Documenting all your activities involving personal information (what data you hold, why you have it, where you get it from, who you share it with, and suppliers you use); and
- Putting written contracts in place with other businesses which provide services that handle personal information on your behalf.

You should also take account TfL's Private Hire Policy Statement, published in February 2018, and which includes measures and obligations relating to good data management in the areas of complaint handling and reporting allegations of crime.

Lawful basis for handling personal information

Under data protection legislation, businesses and organisations are only allowed to use personal information if they have a proper reason or 'lawful basis' to do so. There are six defined 'lawful grounds' listed in the GDPR. You are required to tell people the lawful basis you are relying on to handle their personal data.

In the case of Private Hire operators, there may a number of these 'lawful grounds' you can rely on, depending on the relationships you have with the people concerned and the purposes for handling their personal data. You should seek your own advice on this where necessary, but as guide some examples might include:

- For the 'performance of a contract' in the context of being an employer;
- For the 'performance of a contract' in the context of customers paying you to provide a service to them;
- For the performance of a legal obligation (eg complying with private hire Regulations); and
- Where it is in your legitimate interest (you must document exactly what those legitimate interests are).

Read more about your obligations in the ICO guide to lawful basis for processing.

Collecting personal information

When you collect information about your customers, employees or other people, you need to consider whether they understand what you're going to do with it and why. This applies whether you're collecting hard (paper) copies, taking down information over the phone or capturing it online (using websites or apps).

You should provide a 'privacy notice' which is a statement explaining who you are, what you will do with people's information, and why. It should also include the legal basis for handling their information, the circumstances where you might disclose it to someone else, as well as how long you will keep their information.

Visit www.tfl.gov.uk/privacy to see how TfL presents its own privacy notices.

The notice can be in a number of formats, depending on the way you have collected the information. For example, it could be a leaflet, a statement on a web-form, signage within your booking office or a recorded audio message. The important thing is that you tell people at the time you collect the information in the first place. The privacy notice must be easy to understand and readily available if people want to find it again later.

If you install CCTV cameras in your premises or inside your vehicles, you also need to tell people by putting up appropriate signage. TfL also provides guidance on the requirements for installing CCTV in taxis and private hire vehicles.

You should collect the minimum information possible – ie only that which is strictly necessary for your stated purpose(s). Don't ask for information just because it would be 'nice to know'. You must also take steps to ensure the information you collect is kept accurate and up to date.

You must only use personal information for the purpose(s) for which you originally collected it, so if you collect information about customers wanting to hire a vehicle, don't then use it for something else that is unrelated.

Special categories of 'sensitive' personal information

Some types of the personal information you collect will be more sensitive than others. Examples include information about a person's health or medical condition (or accessibility/mobility needs), race and ethnic origin, trade union membership or their criminal convictions or alleged offences.

If you collect or store information of this nature, then you must only do so with the person's explicit consent or in some cases, where it is necessary for employment purposes.

As part of their operator obligations, operators may require that employees with a public facing role have a 'Basic Disclosure' check - carried out by the Disclosure and Barring Service (DBS). It is essential that you handle and store any information about the results of a basic Disclosure Check securely and in accordance with any guidance issued by the DBS

Security measures

The GDPR requires that all businesses take appropriate technical and organisational measures to protect personal information from being deliberately or accidently compromised or misused.

The ICO can impose a number of sanctions if you fail to adopt adequate measures to protect personal information. In extreme situations, these can include monetary penalties of up to four per cent of your annual turnover or 20 million Euros, (whichever is greater); enforcement action (including ordering you to cease certain business operations); and criminal prosecution.

When protecting information held electronically, there are a number of recognised tools and standards that can help you. A good place to start is the UK Government's 'Cyber Essentials' scheme.

Adequate firewalls and anti-virus software should also be installed and regularly tested and updated. Employee access to information should be managed via role based permissions which only allow them to see the customer details they need to do their job.

We recommend that you implement a policy stating that any sent emails containing sensitive personal data (either in the body of the email or as an attachment) should be encrypted and/or password protected. Any passwords should be sent to the recipient in a separate follow email or by using a different channel, such as by phone or text message. Read more in the ICO guidance on encrypted email.

If you use mobile devices, never leave them unattended to reduce the risk of theft or loss. The device should also be encrypted, so if it falls into the wrong hands, any information stored on it can't be accessed.

If you handle debit or credit card information then additional security requirements may apply. You should refer to sources of help such as the UK Cards Association and recognised standards such as the Payment Card Industry Data Security Standard (PCI DSS).

If you store hard/paper copies of personal information, then you must have appropriate physical security, for example lockable rooms, drawers or filing cabinets - with access limited to only those who are entitled to see it as part of their duties. You should implement a clear desk policy and ensure that documents don't get left lying around on unattended desks, printers or scanners.

You need to ensure that your employees are also aware of their own responsibilities when handling personal information. The ICO produces a range of free training resources that you can use.

Where relevant, employment contracts should contain confidentiality clauses and be clear that misusing personal information will be treated as a disciplinary matter and may constitute gross misconduct.

Retention and disposal

You must not keep personal information for any longer than is 'necessary'. You will need to consider your business purposes, together with any legal or regulatory requirements that will all affect how long you need to keep information, for example:

- private hire operator regulations now require records of bookings, complaints and lost property, as well as driver and vehicle records, to be kept for 12 months;
- the results of Basic Disclosure Checks from the Disclosure and Barring Service should only be kept for as long as is necessary once a recruitment (or other relevant) decision has been made. You can still keep a record of the fact that a check has been completed, and the date on which it was carried out; and

- unsuccessful recruitment applications should only be kept for a maximum of 12 months, to allow for the resolution of any recruitment-related disputes.

In practical terms, the ICO advises that you should also:

- regularly review the length of time you keep personal information;
- securely delete or destroy information that is no longer needed; and
- update or securely delete information if it goes out of date.

Be aware that deletion means permanently and securely destroying that information at the end of its retention period – you should not archive or move it so it can be retrieved again in the future.

The requirement to appropriately store and delete information applies to electronic as well as hard/paper copy formats.

In the case of electronic data, secure destruction means using recognised deletion software, or physically destroying the media itself (eg CDs, DVDs and USB sticks).

For hard/paper copies, you should use shredders or methods such as secure waste bins with a reputable confidential waste collection service. While awaiting destruction, personal information must continue to be stored securely at all times. You should also obtain destruction certificates from suppliers who destroy information on your behalf.

Sharing personal information with TfL

There are a number of circumstances where we may ask you to share information with us about your drivers/employees and your customers. Some of the common scenarios are included below.

TfL Operator uploads

As a private hire operator you are required (under private hire regulations) to provide us with particulars of the vehicles and drivers that were available to or used by you to fulfil private hire bookings on a weekly basis. TfL provides a secure way for you to do this, together with guidance notes on the Operator Upload requirement.

Sharing complaint information

From time to time TfL may ask you to provide information about a particular booking, customer or driver to help us investigate a complaint. If you have received a complaint directly from one of your customers, we may also ask you to share this with us.

You are required to let us know if you dismiss one of your drivers due to misconduct in connection with driving a private hire vehicle. TfL recommends that you adopt secure processes to do this, such as using encrypted email – mentioned earlier in this guide.

You are also encouraged to notify us of any serious complaints that you receive about a driver that is either currently available to work for you or has worked for you. "Available" refers to a driver or vehicle that the operator can call upon to carry out a private hire booking.

This is required to help TfL fulfil its functions as a regulator of private hire services in London and to ensure all licensees remain fit to hold their licence in the interests of public safety.

Private hire vehicles and the Congestion Charge

While most Private Hire vehicles are liable for the Congestion Charge, a limited number of vehicles are exempt (eg wheelchair accessible vehicles). TfL may monitor these private hire vehicles to ensure compliance with the Congestion Charge. We may ask the registered keeper/owner of a licensed private hire vehicle for confirmation that a vehicle was being used for private hire purposes on a particular date and request evidence to verify this e.g. a copy of the booking record and private hire driver's licence. It is the owner's responsibility to provide the information requested to TfL. You should therefore look to assist the owner in providing any information they require to prove that a vehicle was being used for private hire purposes

Other requests to disclose personal information

You may receive requests from other individual or organisations asking for personal information about someone else (often known as a 'third party request');

In the case of a third party asking for someone else's information, then there are only a limited number of circumstances in which you should provide this. These could include:

- requests from the police or other law enforcement bodies
- requests from legal representatives of customers or employees
- requests from insurers or loss adjusters
- requests from other regulators or government agencies
- where there is a court order or other legal obligation.

You should **not** provide information about your customers' journeys in response to casual enquiries from another person. This applies whether or not those people are personally known to you, or whether they indicate they have a personal connection to the person they're asking about. They must also provide you with a valid reason for asking for the information.

You must always verify the identity of the person making the request on each occasion and take care not to disclose personal information about other people not covered by the request.

Subject access requests from customers and employees

Anyone who thinks that your business holds some of their personal information (most likely to be your customers or employees) is entitled under the GDPR to ask you to provide them with a copy of it. Unlike requests from third parties, they do not have to provide a reason for asking for it.

You have a legal duty under the GDPR to provide the information requested - and must do so in a certain time frame, usually within one month. You must provide the information without charging a fee or other costs.

As with requests from third parties, you must always verify the identity of the person making the request on each occasion and take care not to disclose personal information about other people.

More information about this is available from the ICO – see the Help section at the end of this guide.

Other information rights

Individuals also have a number of other 'information rights' in relation to the personal information you hold about them. These include:

- The right to opt out from receiving marketing messages from you
- The right to question any information that they think is wrong or incomplete
- The right to object to how you use their information or to ask you to delete or restrict how you use it
- In some cases, the right to receive a copy of their information in a format that they can easily re-use
- The right to complain to your Data Protection Officer (where you have one)
- The right to complain to the regulator - the Information Commissioner's Office, about the way your handle their personal information

Some of these rights apply in different situations and you should find out more and seek advice from the ICO about how to respond to them.

If things go wrong…

A personal data security breach can happen for a number of reasons. Examples of the types of incidents include:

- Your (or your supplier's) computer systems, website, emails or app are hacked
- hard/paper copies of personal information are stolen or lost
- individuals try to 'blag' information from you, by pretending to be someone else or persuading you that it is okay to hand over the information
- Human error
- employees misusing information, for example by using or sharing it for personal or malicious purposes unconnected to their work

You should develop a process to make sure you know what to do if you suspect a personal data security breach has taken place.

If the breach is serious, the GDPR requires that you also notify the ICO 'without undue delay' and where feasible, no later than 72 hours after becoming aware. Reasons should be provided to the ICO without undue delay in the event that a notification cannot be made within this timescale. If you report a breach to the ICO, you are strongly encouraged to tell TfL, regardless of whether the breach affects your customers or the drivers and vehicles available to you.

You may also have to contact the individuals affected to let them know. Find out more about the GDPR and handling personal data breaches.

TfL's role

We take the security and privacy of personal information very seriously – and this includes the personal data associated with customers and employees of the private hire operators we license and regulate. We work closely with the ICO as part of our regulatory function and report to them on issues of concern.

All of the privacy obligations and best practice mentioned in this summary also applies to us, in the ways that we handle the personal information of our own customers and employees, as well as that of taxi and private hire licensees.

For more information about the ways Transport for London handles the personal information of taxi and private hire licensees please visit www.tfl.gov.uk/privacy.

Changes to this guidance

We will update this guidance from time to time, to make sure it stays up to date.
This guidance was last updated in May 2019.

Help and further information

The ICO offers advice and answers questions by phone, email and live online chat. Find out how to contact the ICO.

The ICO's Guide to GDPR and Self Assessment Toolkit will help you to assess your current level of compliance and highlight what steps you might need to take.

The ICO also produces other self assessment checklists on subjects such as CCTV, direct marketing and information security.

The ICO produces a guide to your accountability under data protection legislation

The ICO also produces a number of resources on a variety of topics including:

- A dedicated GDPR advice service for smaller businesses
- Privacy guidance for small and medium sized businesses
- A quick guide to handling employee information
- A checklist for handling subject access requests

The Think Privacy! Campaign includes a free toolkit to help businesses ensure that their employees are privacy aware.

The Government endorsed Cyber Essentials Scheme helps businesses ensure that they are protecting sensitive information of all kinds, including personal information.

For information on how to comply with the rules around electronic marketing messages, please refer to this ICO guide.

Contact

Taxi and Private Hire
Transport for London

Email tph.enquiries@tfl.gov.uk

Phone 0343 222 4444

Web www.tfl.gov.uk

Twitter @tfltph