

National Taxi Licensing Information Sharing Agreement

Author

Greg Bickerdike - Licensing Manager, City of Wolverhampton Council

Greg.Bickerdike@wolverhampton.gov.uk 01902 554030

Document Control

Version	Date Modified	Author/Modified by	Summary of change
0.1	23 October 2023	Greg Bickerdike	Document creation
0.2	17 January 2024	Greg Bickerdike	Removal of joint data controller references and requirement for publication.
0.3	27 January 2024	Greg Bickerdike	Made explicit the Reason for processing Special Category Data under Article 9 of UK GDPR.
0.4	13 February 2024	Greg Bickerdike	Included the recommendations of the Information Commissioner's Office on the benefits of agreements. Removed reference to European Union law. Require new signatories to confirm data remains in UK and sub-processors are compliant.

Table of Contents

Introduction	2
Purpose	2
Lawful Basis for Processing Data	3
Lawful basis for sharing of Data	4
Signatories' Responsibilities and Code of Practice	6
Agreement Review	9
Roles	11
Data Categories	11
Process Map for Licensing Authorities Data Sharing Decisions	13
Appendix 1 - Agreement Signatories	14

Introduction

This is an Information Sharing Agreement ('agreement') between all parties working together under the remit of Taxi Licensing to ensure decisions made by licensing authorities are based on the most up to date information to ensure public safety.

This agreement aims to facilitate the lawful and secure sharing of information between the listed partner agencies and designated professionals.

Taxi Licensing is a generic term to refer to the licensing regimes regulating Hackney Carriage Drivers, Hackney Carriage Vehicles, Private Hire Drivers, Private Hire Vehicles and Private Hire Operators.

Purpose

As part of licensing authorities' procedures, authorities are asked to disclose, receive and retain personal, sensitive information. This agreement describes the purposes for which information will be used under the remit of the licensing authority in order to promote the appropriate communication and exchange of information between all authorities working together in the interests of public safety.

The intended outcome of this agreement is improved decision making by licensing authorities and the police, resulting in greater public safety.

All authorities under this agreement will be bound by legislation, guidance and common law which will determine their ability to disclose, receive and process information.

It is important to note that information sharing on a case-to-case basis between professionals should not depend on the existence of an agreement being in place between the relevant agencies. **The absence of a protocol should not prohibit the sharing of information.** However, The Information Commissioner's Office (ICO) recommends having an ISA in place as best practice to set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.

As a minimum, to ensure effective arrangements, this agreement will:

1. Improve the efficiency of information sharing between signatories.
2. Outline the principle for sharing information between agencies, professionals and other statutory bodies in a lawful, fair and transparent manner.
3. Outline the principles and standards of expected conduct and practice of partner agencies and staff working for them; and
4. Provide a framework for the legal, secure and confidential sharing of information between agencies and professionals which concerns protecting members of the public or securing the health and safety of individuals in connection with the action of persons at work, through the taxi licensing regime.
5. Demonstrate the accountability of signatories' and their compliance with the data protection legislation.

Lawful Basis for Processing Data

This agreement intends to build on and expand existing information sharing between the signatories of this agreement. Information is normally shared as a result of one of the following, via an individual data sharing/request:

- An individual has applied to a licensing authority for a taxi licence and has previously been licensed by another licensing authority/authorities. The applicant's licence records, particularly any complaints or decisions (such as revocation), are shared, to inform the decision on whether to grant the new licence.
- The police have received information about, or have arrested, a licence holder. The licensing authority is normally informed via Common Law Police Disclosure and the information is used to review that licence.
- A licensing authority has received a complaint, or has undertaken a compliance operation, where a licence holder with another licensing authority is the subject. This information is shared with the authority; the information is used to review that licence and may be used to prosecute the licence holder.

This agreement seeks to formalise the information sharing practices of the signatories. It is therefore the responsibility of all signatories to this agreement to ensure that any information exchanges are justified and in adherence with the legal basis set out in this agreement.

There is no single source of law that regulates the powers that an organisation has to use and to share personal information. Sharing information between agencies is lawful if it meets one of the criteria set out in Articles 6 (for personal data) and Article 9 (for special category data) of the UK General Data Protection Regulation (UK GDPR). In some cases, the option chosen must also align with an associated condition in UK Data Protection law.

In order to share information legally between partners there must be a defined and justifiable purpose that references the appropriate underpinning legislation and the associated duties and/or powers.

Reason for processing Personal Data under Article 6 of UK GDPR

Processing of data in accordance with this agreement is lawful under UK GDPR Article 6,1. (e) as 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.

Processing of special categories of personal data is lawful under UK GDPR Article 9, 2 (g): processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. As the exercise of this licensing function is conferred on the authority by an enactment or rule of law, this is a lawful basis of significant public interest for

processing Special Category data under Section 6 (2) (a) of Schedule 1 of the Data Protection Act (2018).

The following is a non-exhaustive list of legislation and guidance that may apply to the Processing of Data pursuant to the Agreement:

- A. The DPA (Data Protection Act) 2018, in particular Schedule 1, Part 1, paragraph 1, and Schedule 1, Part 2, paragraph 6 (statutory etc and government purposes).
- B. UK GDPR (General Data Protection Regulation)
- C. The Regulation of Investigatory Powers Act 2000;
- D. Standards and the Policing and Crime Act 2017;
- E. All applicable laws, and regulations relating to the Processing and Sharing of Data and privacy including (where applicable and without limitation) the guidance and codes of practice issued by the Information Commissioner under the UK GDPR, DPA and under any subsequent Data Protection Legislation.

Statutory Duty

Local authorities have a statutory duty under Part II of the Local Government (Miscellaneous Provisions) Act 1976 and the Town Police Clauses Act 1847 to administer a licensing regime for the safe operation of private hire and hackney carriage vehicles.

Statutory Guidance

Sections 4.9 – 4.25 of the Department for Transport's (DfT) 'Statutory taxi and private hire vehicle standards' outline recommendations for partnership working between licensing authorities and the police, including having information sharing agreements. The DfT guidance is statutory and must be regarded.

Lawful basis for sharing of Data

Data protection legislation provides the legal basis for the sharing of data in connection with a local authority's regulatory activities.

The Data Protection Act 2018, Schedule 2, allows adaptations and restrictions of the GDPR mainly relating to an individual's data rights in order to share information for a set of specified reasons. Those which apply to this sharing agreement are:

Schedule 2, Part 1, Paragraph 5, (2) of the Data Protection Act 2018 states that the UK GDPR provisions (again mainly in relation to an individual's data rights) are allowed to be adapted/restricted to allow personal data to be shared or disclosed where it is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of the UK GDPR would prevent the disclosure.

Schedule 2, Part 1, Paragraph 5, (3) of the Data Protection Act 2018 state that the listed UK GDPR provisions do not apply to personal data where disclosure of the data—

- (a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),
- (b) is necessary for the purpose of obtaining legal advice, or
- (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of those provisions would prevent the controller from making the disclosure.

Schedule 2, Part 1, Paragraph 2, (1) of the Data Protection Act 2018 states that communication of personal data breach to the data subject do not apply to personal data processed for any of the following purposes—

- (a) the prevention or detection of crime,
- (b) the apprehension or prosecution of offenders, or
- (c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

Schedule 2, Part 1, Paragraph 2, (2) states that sub-paragraph (3) applies where personal data is processed by a person (“Controller 1”) for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and another person (“Controller 2”) obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

Schedule 2, Part 1, Paragraph 2 (3) states that Controller 2 is exempt from the obligations in the following provisions of the UK GDPR-

- (a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),
- (b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),
- (c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and
- (d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).

Schedule 2, Part 2, Paragraph 7, (2) of the Data Protection Act 2018 states that the listed UK GDPR provisions [in Schedule 2 Part 2 (6), mainly in relation to an individual's data rights] do not apply to personal data processed for the purposes of protecting members of the public against:

- (a) dishonesty, malpractice or other seriously improper conduct,
or
- (b) unfitness or incompetence,
and

The function is conferred on a person by an enactment or is of a public nature and is exercised in the public interest.

Schedule 2, Part 2, Paragraph 7 (4) of the Data Protection Act 2018 applies where:

The function is designed:

- (a) to secure the health, safety and welfare of persons at work,
or
- (b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work,
and

The function is conferred on a person by an enactment or is of a public nature and is exercised in the public interest.

This includes taxi and private hire vehicle licensing. The exemption applies only to information processed for the core regulatory activities of appropriate organisations; it may not be used in a blanket manner. The exemption applies only to the extent that the application of the rights of data subjects to the information in question would be likely to prejudice the proper discharge of the regulatory functions.

Taxi licensing is a function that is designed to protect the public against unfitness or incompetence and is of a public nature and is exercised in the public interest to protect persons other than those at work (i.e. the public) against risk to health or safety arising out of or in connection with the action of persons at work (i.e. a private hire/hackney carriage licence holder).

Common law police disclosure (CLPD) provisions allow police forces to proactively provide personal data or sensitive personal data to a third party using common law powers where there is a "pressing social need" or public protection risk. Any behaviours that question the suitability of a licence holder must be shared with the relevant licensing authorities.

Signatories' Responsibilities and Code of Practice

Role of Signatories

Where personal information is shared under this Procedure, the recipient will become data controller for the information received – for the purposes for which it was shared.

In each case, the disclosing partner shall retain and continue to process the transfer data for its own purposes.

Accuracy

Information shared by the signatories is subject to procedures and validations intended to ensure data quality at the point it is originally input/entered into their own systems. Any inaccuracies should be notified as soon as they are identified to the designated points of contact for this Procedure.

Should the need arise, the signatories will rectify any identified errors, taking into account the nature of the error(s) and the specific information involved in each case.

Where inaccurate data is identified, incorrect information will be confirmed and rectified within 5 working days. Any third party recipients of the information shall also be notified.

Where a data controller has concerns regarding the quality of data, it must ensure that these concerns are accompanied with the data. For example, if a complaint has been made anonymously, or the complainant has refused to make a written statement, this fact should be included with the data.

Breaches

Signatories must inform the Data Controller(s) within 24 hours upon becoming aware of any breach (or potential breach) of the DPA or other relevant legislation, in relation to its processing of the information provided by the Data Controller(s).

Signatories must comply with the requirement of the General Data Protection Regulation (UK GDPR), Article 33 which requires organisations to notify the Information Commissioners Office (ICO) of high-risk breaches without undue delay and within 72 hours. Signatories will also be responsible for notifying their respective relevant internal departments.

Signatories will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and assessing whether the Information Commissioner and/or the information subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the loss, damage or unauthorised disclosure.

Feedback

Action taken by a signatory as a result of information received should be fed-back to the original data controller.

A revocation or refusal on public safety grounds should also be advised to the police.

Mechanisms for sharing

Information should be shared in the following order of preference:

- Information will be generally exchanged by means of secure email
- Depending on the information being shared in each case, and subject to agreement between the partners, the information may be contained within the body of the email itself, or as an email attachment in Word, Excel or PDF format.
- Encrypted Email to a standard in line with governments most up to date guidance.
- Secure website or file transfer, such as a SharePoint or Egress.
- Where appropriate, other channels to transfer information may be required from time to time. Such transfers may take place during planned face to face meetings, by telephone, during the course of specific 'live' operations or campaigns being carried out jointly by the partners. In such cases, each partner will be responsible for subsequently storing the information securely and in compliance with its protective marking or security classification

Information can be requested via telephone but should be shared via one of the above transmission methods.

Signatories will not have any direct access to each other's systems or applications.

National Register of Refusals, Revocations and Suspensions (NR3S)

Licensing authorities must record their decisions to refuse an application for a licence and decisions to revoke or suspend a licence on NR3S.

Licensing authorities in receipt of a new licence application must search for the applicant on NR3S. If another authority has refused or revoked that individual, the information that was considered when making that decision should be requested from them.

Data Subject Rights

Signatories shall respond to requests from data subjects exercising their right of access and/or their right to object to processing, restrict processing and/or erasure, or rectification of their Personal Data - in accordance with the requirements of Data Protection Legislation.

Freedom of Information Requests

Signatories are public authorities for the purposes of the Freedom of Information Act 2000 (FOIA). This means that any information held signatories and their subsidiary companies is accessible by the public on written request, subject to certain limited exemptions.

Signatories shall demonstrate a commitment to openness and transparency regarding information sharing arrangements under this Agreement subject to any limitations posed by security or confidentiality requirements.

In the event that an information access request relating to Information Sharing activities under this Agreement is received and information is identified that may be subject to an exemption, both signatories shall endeavour to consult with the other in accordance with the Code of Practice as implemented by section 45 of FOIA before reaching its conclusion.

Storage

Data must be stored by each data controller securely, in accordance with their privacy policy and in line with their stated data retention periods. After the retention period has expired, the data must be deleted.

It is expected that data relating to a current licence holder would not be destroyed by a data controller, unless the original data controller has requested its destruction or has withdrawn from the information sharing agreement.

The signatories must either have a satisfactory Data Security and Protection Toolkit result or be compliant with ISO27001, Cyber Essentials Plus or Public Sector Network (PSN) current certification.

Sharing

Data should be shared when requested by a signatory within 10 working days. If data will take longer to provide, then this must be advised to the requestor within 10 working days and the data provided within one calendar month from the date the request was received.

Data controllers must record when they share data in accordance with this agreement, so that the recipient can be logged for the purposes of any requests from data subjects.

All information exchanged under this agreement must be:

- Relevant to all necessary actions and procedures applicable to hackney carriage and private hire licensing; and
- Be shared for the specified purpose; and
- Be shared in circumstances justifying the need to share information.

Agreement Review

This agreement shall remain in place indefinitely but will be reviewed by all signatories in January of each year. The following will be considered at a meeting of the signatories:

- Whether the information sharing is having the desired effect; is it resulting in quicker and more accurate licensing or policing decisions?
- Any complaints or questions received regarding the information sharing agreement.

- Whether signatories are compliant with the agreement, particularly that privacy notices are still accurate and any mediation that has taken place following a breach of the agreement.
- Whether data is being stored correctly and the details of any security breaches.
- Whether requests are being administered properly, particularly subject access requests.
- Whether data has been retained correctly, particularly if there has been an erasure request or a signatory has withdrawn from the agreement.

Amendments

Any amendments must be agreed by all signatories before coming into effect.

Joining the Agreement

For a new organisation to join the agreement, an existing signatory must notify all other signatories of the new organisation's:

- Name
- Address
- Data Protection Officer
- Information Commissioner's Office registration number
- Contact email
- Confirmation that data processed under the agreement will remain at all times within the UK, including when processed by any sub-processors working for the Signatory;
- Confirmation that if data is to be processed by a sub-processor, the Signatory is compliant with Articles 28 and 35 in that regard to that processing.

The other signatories must reply within 28 days stating whether they agree that the new organisation be allowed to join the agreement.

If all signatories agree, the new organisation must add their details and signature in the 'Agreement Signatories'. The existing signatory which originally notified the other signatories must then circulate this version of the agreement to all signatories, accompanied by written proof that each signatory agreed to the new organisation joining.

If any signatory disagrees, the new organisation is not permitted to join the agreement and the agreement continues as is.

Leaving the Agreement

Should a signatory wish to withdraw from the agreement at any time, they must formally notify all other signatories using the contact details listed.

Future data requests and sharing with the ex-signatory will not be covered by this agreement.

In the event of termination of this ISA each signatory may continue to hold information originating from another signatory for which they are Controller – for the purposes for which the information was originally collected/received/shared.

Roles

Data Controllers

Signatories in possession of data shared in accordance with this agreement are data controllers for those data.

Data Subjects

1. Applicants, holders and former holders of a:
 - Driver licence for hackney carriages or private hire vehicles;
 - Vehicle licence for a proprietor of a hackney carriage or of a private hire vehicle;
 - Operator licence for private hire vehicles;

regulated under Part II of the Local Government (Miscellaneous Provisions) Act 1976 and the Town Police Clauses Act 1847.
2. Complainants or witnesses where their complaint/statement relates to a data subject listed above.

Data Categories

The following data categories can be requested and shared in accordance with this agreement:

Personal Data

- Applicant/licensee's name
- Address
- Date of birth
- Telephone number
- Email address
- Vehicle registration number
- Licence number
- Details of non-compliance

Special Categories of Personal Data

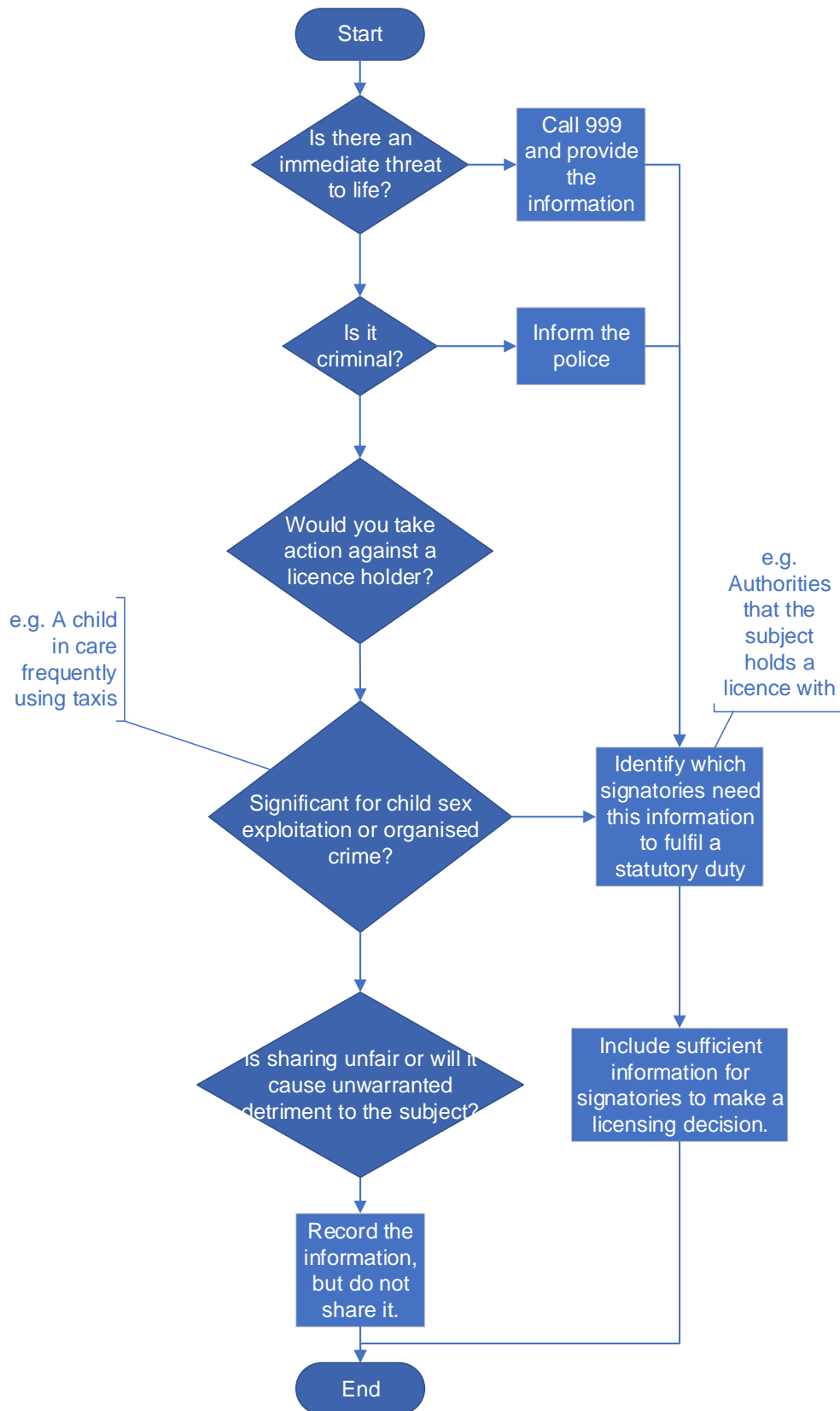
- Ethnicity
- Nationality
- Information about their health
- Criminal offence data

Data required for the performance of Statutory Duties

The following data relating to taxi licensing:


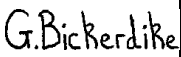
- Licence records
- Complaint details
- Multimedia files to support complaints or compliance investigations
- Complaint records held by Private Hire Operators
- Witness statements
- Information from police investigations where there is a pressing social need to inform a licensing authority
- Authorised officer delegated decision records
- Committee/Sub-Committee/Hearing reports and minutes relating to decisions

Process Map for Licensing Authorities Data Sharing Decisions



Appendix 1 - Agreement Signatories

Signed by the organisation's duly authorised representative:

List of Signatories				
Organisation	Data Protection Officer	Representative Name and Position	Signature	Date
<p>South Derbyshire District Council of Civic Office, Civic Way, Swadlincote, DE13 1AH (Information Commissioner's Office registration number Z5863677). Contactable at licensing@southderbyshire.gov.uk</p>	<p>Anthony Baxter dataprotectionofficer@southderbyshire.gov.uk</p>	<p>Ardip Kaur, Executive Director, Law and People</p>		<p>22/05/2024</p>
<p>Wolverhampton City Council of Civic Centre, St. Peter's Square, Wolverhampton WV1 1SH (Information Commissioner's Office registration number Z5569755). Contactable at licensing@wolverhampton.gov.uk or DriverLic@secure.wolverhampton.gov.uk</p>	<p>Anna Zollino-Biscotti, Information Governance Manager DPO@Wolverhampton.gov.uk</p>	<p>Greg Bickerdike Licensing Manager</p>		<p>15/04/24</p>