



DRAFT

DATA SHARING AGREEMENT

Between

**National Transport Authority (“NTA”)
and
National Standards Authority of Ireland Legal Metrology
Service (“NSAI LMS”, “NSAI” and “LMS”)**

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

Allowing LMS to check if a Small Public Service Vehicle (“SPSV”) is licensed ahead of taximeter verification AND allowing NTA to confirm taximeter verification.



Table of Contents

Glossary	2
Interpretation Table	2
Data Sharing Agreement.....	6
1. Evaluation for a Data Protection Impact Assessment (DPIA).....	7
2. Purpose of the Data Sharing	9
3. Data to be shared	12
4. Function of the Parties.....	14
5. Legal Basis.....	15
6. Impetus for Data Sharing.....	19
7. Categories of Data Shared	20
8. Duration and Frequency	21
9. How data will be processed	22
10. Restrictions.....	23
11. Security Measures	24
12. Retention	31
13. Methods Used to Destroy/Delete Data.....	32
14. Withdrawal from Agreement.....	33
15. Other Matters.....	34
16. Schedule A - Data Protection Impact Assessment.....	36
17. Schedule B	39
18. Schedule C	41
19. Authorised Signatory	42
Data Protection Officers Statement	43



Glossary

Provide a plain English description of terms, phrases, acronyms or abbreviations consistently referenced throughout the agreement.

It is advised to include rare, unfamiliar, specialised or technical terms that are content-specific in the table below.

The purpose of this glossary is to serve as a dictionary for the reader.

Term/Phrase/ Acronym/Abbrev	DESCRIPTION
API	Application Programming Interface
BaaS	Banking as a Service
DGB	Data Governance Board
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DR	Data Retention
DSA	Data Sharing Agreement
DSGA	Data Sharing and Governance Act
EU	European Union
GDPR	General Data Protection Regulation
IP	Internet Protocol
ISO	International Organisation for Standardisation
IT	Information Technology
LMS	Legal Metrology Service
MoU	Memorandum of Understanding
NSAI	National Standards Authority of Ireland
NTA	National Transport Authority
OGCIO	Office of the Government Chief Information Officer
PC	Personal Computer
PSB	Public Service Body
SI	Statutory Instrument
SPSV	Small Public Service Vehicle
TOMs	Technical & Organisational Measures
VPN	Virtual Private Network
WAF	Web Application Firewall



--	--



Interpretation Table

DEFINITION	MEANING
Data controller	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Party disclosing data	Shall mean the Party transferring personal data to the receiving Party or Parties.
Party receiving data	Shall mean the Party receiving personal data from the Party disclosing data.
Data Protection Impact Assessment (DPIA)	Means an assessment carried out for the purposes of Article 35 of the General Data Protection Regulation.
GDPR	Shall be taken as a reference to the General Data Protection Regulation (2016/679) including such related legislation as may be enacted by the Houses of the Oireachtas.
Lead Agency	Refers to the Party to this agreement who is responsible for carrying out the functions set out in 18(2), 18(3), 21(3), 21(5), 22(1), 55(3), 56(1), 56(2), 57(4), 58, 60(1) and 60(4) of the Data Sharing and Governance Act 2019.
Personal Data	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Personal data breach	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Processing	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Public Service Body (PSB)	Means a Public Body as defined by section 10 of the Data Sharing and Governance Act 2019.
Shared personal data	Means data shared pursuant to this agreement.

Table 1.0



Data Sharing Agreement

BETWEEN

Insert name of Lead Agency, having its registered address at:

LEAD AGENCY NAME	ADDRESS
National Transport Authority	National Transport Authority, Haymarket House, Smithfield, Dublin 7, Ireland D07 CF98

AND

Insert name(s) of Other Party/Parties to the agreement, having its registered address at:

PARTY NAME	ADDRESS
National Standards Authority of Ireland Legal Metrology Service	National Standards Authority of Ireland, 1 Swift Square, Northwood, Santry, Dublin 9, Ireland D09 A0E4

The Parties hereby agree that the National Transport Authority will take the role of Lead Agency for the purpose of this Data Sharing Agreement.

Each of the Parties to this agreement are data controllers in their own right when processing personal data on their own behalf, for their own purposes.



1. Evaluation for a Data Protection Impact Assessment (DPIA)

The completion of a DPIA can help data controllers to meet their obligations in relation to data protection law. [Article 35](#) of the GDPR sets out when a DPIA is required.

Data controllers should periodically re-evaluate the risk associated with existing processing activities to understand if a DPIA is now required.

1.1 Identifying if a DPIA is required

The below checklist can assist organisations to understand if they require a DPIA pursuant to Article 35 GDPR to support their data sharing agreement. The questions should be answered in relation to the entire project that the data share corresponds to. This ensures that Public Service Bodies (PSBs) have the opportunity to be transparent in the evaluation of risks in relation to the data required for this process.

The completion of a DPIA is relevant to this data sharing agreement as you will be asked to provide a summary of any DPIA carried out in [Section 16](#) of this document.

The questions below should be completed by the Lead Agency together with the Other Parties involved in this data sharing agreement. Please contact your DPO in relation to the requirement to carry out a DPIA.

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.1	Processing being carried out prior to 25th May 2018?	YES

Table 1.1

If 'Yes' proceed to [1.2](#)
If 'No' proceed to [1.1.2](#)

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.2	A new purpose for which personal data is processed?	NO
1.1.3	The introduction of new types of technology?	NO

Table 1.2

If 'Yes' to either of the last two questions, proceed to [1.1.4](#).
If 'No' to both of the last two questions, proceed to [1.2](#).

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.4	Processing that is likely to result in a high risk to the rights and freedoms of natural persons?	NO

Table 1.3

If 'Yes', then you are likely required to carry out a DPIA under [Article 35](#) GDPR.
If 'No' proceed to [1.2](#).



1.2 Further Considerations

There are limited circumstances where a mandatory DPIA should be carried out, even where processing was underway prior to the GDPR coming into effect¹.

	DOES THE PROCESS INVOLVE:	YES/NO
1.2.1	A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect individuals.	NO
1.2.2	A systematic monitoring of a publicly accessible area on a large scale.	NO
1.2.3	<p>The Data Protection Commission has determined that a DPIA will also be mandatory for the following types of processing operation where a documented screening or preliminary risk assessment indicates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals pursuant to GDPR Article 35(1):</p> <p><u>Lists of Types of Data Processing Operations which require a DPIA.</u></p> <p><i>(if this hyperlink does not work, use the following url: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf)</i></p>	NO

Table 1.4

If 'Yes' to any then you are likely required to carry out a DPIA under [Article 35](#) GDPR.

If 'No', to all then a DPIA may not be required.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>



2. Purpose of the Data Sharing

2.1 Framework

This Data Sharing Agreement sets out the framework for the sharing of personal data between the Parties and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to one another.

This agreement is required to ensure that any sharing of personal data is carried out in accordance with the GDPR and the Data Sharing and Governance Act 2019, and each Party agrees to be bound by this agreement until such time as the agreement is terminated, or the Party withdraws from the agreement.

The Parties shall not process shared personal data in a way that is incompatible with the relevant purposes and this agreement.

The Parties will ensure that the Data Sharing Agreement remains fit for purpose, accurate and up to date.

The Parties will actively monitor and periodically review the data sharing arrangement to ensure that it continues to be compliant with data protection law, that it continues to meet its objective, that safeguards continue to match any risks posed, that records are accurate and up to date, that there is adherence to the data retention period agreed and that an appropriate level of data security is maintained.

The Parties must address all recommendations made regarding this Data Sharing Agreement by the Data Governance Board.



2.2 Performance of a Function

Where a public body discloses personal data to another public body under this agreement, it shall be for the purpose of the performance of a function of the public bodies mentioned, and for one or more of the following purposes (please select):

No.	DESCRIPTION	Select
I	To verify the identity of a person, where one or more of the public bodies are providing or proposing to provide a service to that person	<input type="checkbox"/>
II	To identify and correct erroneous information held by one or more of the public bodies mentioned	<input type="checkbox"/>
III	To avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered by one or more of the public bodies mentioned where one of mentioned public bodies to collect the personal data directly from that person	<input checked="" type="checkbox"/>
IV	To establish the entitlement of a person to the provision of a service being delivered by one or more of the public bodies mentioned, on the basis of information previously provided by that person to one or more of the public bodies mentioned (or another public body that previously disclosed the information to one or more of the public bodies mentioned)	<input checked="" type="checkbox"/>
V	To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input type="checkbox"/>
VI	To facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input type="checkbox"/>
VII	To enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input type="checkbox"/>
VIII	To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned	<input type="checkbox"/>

Table 2.2

2.3 Details about the Purpose

Provide details of the particular purpose of this Data Sharing Agreement.

PURPOSE	DESCRIPTION
III - To avoid the financial or administrative burden that would otherwise be imposed...	<p>The overarching purpose of this Data Sharing Agreement is to provide the NTA and LMS with a lawful basis to share details of SPSV licences for the purposes of carrying out their respective functions of regulating small public service vehicles (“SPSVs”) services and upholding and enforcing accuracy and transparency in trade measures.</p> <p>NTA provides data directly to and receives data directly from LMS.</p> <p>III - In order to carry out its function as licensing and regulatory authority for SPSVs, the NTA must ensure that taximeters have been verified and sealed in compliance with the below referenced taxi regulations. NTA therefore provides SPSV licence data to LMS to allow SPSVs to have their taximeters verified and sealed by LMS and</p>



IV - To establish the entitlement of a person to the provision of a service...	<p>it receives data regarding taximeter verification directly from LMS to support SPSV licensing and compliance checks.</p> <p>In both instances, this avoids the need for SPSV licence holders to print, share or post such information, thereby removing any financial and/ or administrative burden on the licence holder. This information is therefore shared <i>“to avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered”</i> by NTA or LMS, were the public body receiving the information to collect the personal data directly from that person as set out under S.13(2)(a)(ii)(III) of the Data Sharing and Governance Act 2019 (“DSGA 2019”).</p> <p>IV: NTA shares SPSV licence data with LMS to enable LMS to verify the entitlement of a person to a booking to have their taximeter verified and sealed. Pursuant to Regulation 39(1) of S.I. No. 323 of 2008 - Legal Metrology (General Regulations), only persons with an SPSV licence are entitled to this service. Only NTA, as licensing authority for SPSVs and the authority responsible for maintaining the “Register of Licences” under the Taxi Regulation Act 2013 (as amended), can verify this SPSV licence information. This information is therefore shared to establish “the entitlement of a person to the provision of a service being delivered” by NTA or LMS as set out under S.13 (2) (a) (ii) (IV) of the DSGA 2019.</p>
---	--

Table 2.3



3. Data to be shared

3.1 Quality

The Parties will take all reasonable steps to ensure that any personal data processed under this agreement is accurate, kept up to date, and that data which is inaccurate, having regard to the purposes for which it was processed, is erased or rectified as soon as is practicable.

Shared personal data shall be limited to the personal data described in [table 3.4](#) to this agreement and will be shared only in the manner as set out in [table 11.2](#) therein. Where a party receiving data is notified of inaccurate data by the data subject, this party is obliged to notify the disclosing Party/Lead Agency.

3.2 Subject Rights

In so far as the shared personal data is processed by the Party/Parties receiving data, as a data controller, the Party/Parties receiving data will deal with data subjects in their exercising of rights set out in the GDPR, including but not limited to, the right of access, the right of rectification, erasure, restriction of processing and to data portability.

Data subjects have the right to obtain certain information about the processing of their personal data through a data subject access request.

Data subject access requests in relation to data processed by the Party/Parties receiving data will be dealt with by them directly. Data subject access requests in relation to data processed by the Party/Parties disclosing data prior to the transfer will be dealt with by them directly.

3.3 Sharing with Third Parties

The Party/Parties receiving data shall not share the shared personal data with any person who has not been authorised to process such data.

3.4 Detail of the information to be disclosed

Provide details of the personal data set to be disclosed and the detail of any non-personal data.

Note:

If the non-personal data and personal data are linked together to the extent that the non-personal data becomes capable of identifying a data subject then the data protection rights and obligations arising under the GDPR will apply fully to the whole mixed dataset, even if the personal data represents a small part of the set.

	DESCRIPTION
Shared Personal Data	<p>Data shared by NTA:</p> <ol style="list-style-type: none">1. SPSV LICENCE NUMBER: unique licence number for the holder of an SPSV vehicle licence. This is the search term to allow NTA to pull back LMS meter seal information2. VEHICLE_REG_NO: unique registration number for the vehicle licensed as an SPSV3. VL HOLDER_NAME: the full name of the licence holder4. STATUS: the status of the SPSV vehicle licence; only active licences will be returned/shared5. EXPIRY_DATE: the expiry date of the SPSV vehicle licence



	<ol style="list-style-type: none">6. ADDRESS_1: the postal address of the licence holder (1/6)7. ADDRESS_2: the postal address of the licence holder (2/6)8. ADDRESS_3: the postal address of the licence holder (3/6)9. TOWN: the postal address of the licence holder (4/6)10. COUNTY: the postal address of the licence holder (5/6)11. POST_CODE: the postal address of the licence holder (6/6)12. TEL: the main telephone contact number for the licence holder13. EMAIL: the email address for the licence holder14. OPERATOR_NAME: the full name of the SPSV driver linked to that vehicle; i.e. the operator of the licensed vehicle as notified to the Authority15. DRIVER_LICENCE_NO: the unique licence number for the holder of an SPSV driver licence16. DRIVER_LICENCE_STATUS: the status of the SPSV driver licence; only active licences will be linked <p>Data shared by LMS:</p> <ol style="list-style-type: none">17. SPSV LICENCE NUMBER: unique licence number for the holder of an SPSV vehicle licence. This is the search term to allow NSAI to pull back SPSV licence details18. TRAMS_REG: unique registration number for the vehicle held by NSAI for the SPSV Licence searched for. As NSAI do not have a live feed, this may be different to the reg currently on the licence (Vehicle_Reg_No). Appears in NTA systems as 'LMS Registration Number'
Non-personal Data	<p>Data shared by NTA:</p> <ol style="list-style-type: none">1. ADDED_DATE: the date the SPSV vehicle licence was added to the system, i.e. the date of first licensing2. VEHICLE_MODEL: the model of the licensed vehicle3. VEHICLE_COLOUR: the colour of the licensed vehicle <p>Data shared by LMS:</p> <ol style="list-style-type: none">1. TEST DATE: the date the taximeter was verified2. RESULT: the result of the taximeter verification test3. BOOKING DATE: the data the taximeter verification test was booked4. SOFTWARE IN DATE: Yes/No result showing whether taximeter software is in date or has expired5. SEAL SECURITY/VERIFICATION: confirmation that the meter is properly sealed

Table 3.4



4. Function of the Parties

4.1 Function of the Parties

In table 4.1 below:

- i. Specify the function of the party disclosing data to which the purpose (as defined in [table 2.3](#)) of the data sharing relates
- ii. Specify the function of the party receiving data to which the purpose (as defined in [table 2.3](#)) of the data sharing relates.

PARTY	FUNCTION
i. National Transport Authority	<p>The NTA is a statutory non-commercial body, which operates under the aegis of the Department of Transport, Tourism and Sport. Established in 2009 under the Public Transport Authority Act, the NTA is responsible for developing and implementing strategies to provide high quality, accessible, sustainable transport across Ireland which, following the dissolution of the Commission for Taxi Regulation in 2003, includes the principal function of developing, operating and maintaining a regulatory framework for the licensing and regulation of the standards to be applied to small public service vehicles and their drivers.</p> <p>In accordance with the Taxi Regulation Act 2013 (as amended) (the “2013 Act”), the NTA is the licensing authority for SPSVs. Pursuant to section 20 of the 2013 Act, the NTA has made the Taxi Regulations (Small Public Service Vehicle) Regulations 2015 (the “2015 Regulations”) which set out certain requirements in relation to the licensing of SPSVs and the drivers of SPSVs. In particular, in accordance with Regulations 53(2) and 54 of the 2025 Regulations, SPSVs are required to be fitted with a taximeter which has been calibrated and verified by LMS as being correctly calibrated.</p>
ii. National Standards Authority of Ireland Legal Metrology Service	<p>The Legal Metrology Service (LMS) is a division within the National Standards Authority of Ireland (NSAI). The NSAI, established under the National Standards Authority of Ireland Act 1996 (the “1996 Act”), is Ireland’s official standards body. The NSAI is empowered under the 1996 Act to develop and adopt Irish standards supported by the advice of technical experts and its Consultative Committees. The NSAI operates the LMS, which is a national and EU conformity assessment body established under the Metrology Act 1996 and notified for Directives 2014/31/EU (Non-automatic Weighing Instruments) and 2014/32/EU (Measuring Instruments). LMS is responsible for upholding and enforcing accuracy and transparency in trade measures by certifying and inspecting measuring instruments used by traders and by inspecting pre-packaged goods to ensure correct quantity. The Metrology Act 1996 and associated regulations provide significant protections to ensure fair trading conditions for businesses and the protection of consumers.</p>

Table 4.1



5. Legal Basis

5.1 Legal Grounds

For the purposes identified in this Data Sharing Agreement the Parties confirm that the sharing and further processing of the defined personal data is based on the legal grounds set out in 5.1.1 and 5.1.2.

5.1.1 Appropriate Legislative Provisions for Sharing

Define the appropriate legal provision for sharing based on the following:

- i. 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 (GDPR Art 6. 1 (e))

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
S.13(2)(a)(i) S.13(2)(a)(ii)(III) S.13(2)(a)(ii)(IV)	<p>Pursuant to Section 13(2)(a)(i) of the DSGA a public body may disclose personal data to another public body, in a case in which this section applies to such disclosure, only where – <i>the personal data concerned is disclosed for the purposes of the performance of a function of the first or second mentioned public body, and for one or more of the following purposes.</i></p> <p>Pursuant to Section 13(2)(a)(ii)(III) of the DSGA a public body may disclose personal data to another public body, in a case in which this section applies to such disclosure, only where the personal data concerned is disclosed “<i>to avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered by one or more of the public bodies mentioned where one of the mentioned public bodies collect the personal data directly from that person</i>”.</p> <p>Pursuant to Section 13(2)(a)(ii)(IV) of the DSGA a public body may disclose personal data to another public body, in a case in which this section applies to such disclosure, only where the personal data concerned is disclosed “<i>to establish the entitlement of a person to the provision of a service being delivered by the first mentioned public body (or another public body that previously disclosed the information to the first mentioned public body.</i></p>

Table 5.1.1



5.1.2 Appropriate Legislative Provisions for Further Processing

Specify the appropriate legal provision for further processing based on the following:

- ii. 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 (GDPR Art 6. 1 (e))

LEGISLATION	DESCRIPTION
Legislative Provision for Processing by NTA	<p>Legislative Provision for Processing By NTA</p> <p>The processing of personal data received by NTA from LMS is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NTA, i.e. such processing is necessary to enable NTA (as the licensing authority for SPSVs) to ensure that a vehicle is licensed properly in accordance with the 2013 Act and the 2015 Regulations (relevant provisions set out below).</p> <p>For completeness, it is worth noting that where licensing and compliance checks are completed and it is found that an SPSV licence holder is non-compliant with the below legislation (in that they were caught operating with an unsealed/unverified taximeter), the operator may be subject to a Fixed Penalty Notice and/or prosecution. This occurs in less than 10% of cases on average. The processing of personal data received by NTA from LMS for this purpose falls under the Law Enforcement Directive and is not the principal purpose for which LMS shares this data with NTA. As such, it falls outside the scope of this data sharing agreement.</p> <p>Relevant statutory provisions</p> <p><u>Section 20 of the Taxi Regulation Act 2013</u></p> <p>(1) The Authority may make regulations, to be known in this Act as small public service vehicle regulations (“SPSV regulations”) in relation to the following:</p> <p>(b) the vehicle standards to be complied with regarding the roadworthiness and suitability of a small public service vehicle, including standards relating to the following:</p> <p>(iii) the standards relating to any equipment carried in the vehicle, including requirements in relation to evidence of verification of</p>



	<p>taximeters or taximeter systems in accordance with regulations made under the Metrology Act 1996.</p> <p>S.I. No. 33/2015 – Taxi Regulation (Small Public Service Vehicles) Regulations 2015</p> <p>53 (2) A person shall not drive or operate a taxi for the carriage of persons for reward unless - ... (b) the taximeter so fitted to the vehicle has been calibrated in accordance with Regulation 54</p> <p>Calibration of taximeters to reflect maximum fares order 54. (a) A taximeter fitted in a taxi shall be calibrated such that that taximeter calculates all fares in accordance with the maximum fares order.</p> <p>NTA collects personal data from licence applicants under the Taxi Regulation Act 2013 (as amended) and the Taxi Regulation (Small Public Service Vehicle) Regulations 2015.</p> <p>The NTA and NSAI data sharing relationship is Controller-Controller during in sharing of personal data, in that NTA is the Controller of the data shared with NSAI, and NSAI is the Controller of data shared with NTA.</p>
Legislative Provision for Processing by LMS	<p>Legislative Provision for Processing by LMS</p> <p>The processing of personal data received by LMS from NTA is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in LMS, i.e. to enable LMS to verify the entitlement of a person to a booking to have their taximeter verified and sealed in accordance with the 1996 Act, the Metrology Act 1996 and the Legal Metrology (General Regulations) 2008 (relevant provisions set out below).</p> <p>Relevant statutory provisions</p> <p>Sections 13 and 14 of the Metrology Act 1996</p> <p>13. (1) Every person who makes, sells, imports or causes to be made or sold, any instrument intended for use for trade or any prescribed purpose, or who uses or has in his or her possession for use any instrument for any such purpose, shall ensure that the relevant conformity assessment procedure referred to in section 14 has been applied to it.</p> <p>14. (1) Instruments intended for use for any prescribed purpose, including public weighing and measuring equipment referred to in section 26, shall be subject to the procedures ("conformity assessment procedures") prescribed by the Director.</p> <p>Regulations 11, 39 and 40 of S.I. No. 323 of 2008 – Legal Metrology (General Regulations) (as amended)</p> <p>11. (1) Except where otherwise provided, the application of a verification or non-conformity mark under these Regulations shall be</p>



	<p>deemed to invalidate all previously applied prescribed marks and shall continue in effect until such time as the instrument is again stamped with the verification mark or the non-conformity mark as the case may be.</p> <p>11. (4) Interference with or tampering with or removal of any security mark or any security device or seal shall be deemed to invalidate any previously applied verification mark.</p> <p>39. (1) An inspector or authorised person may apply the verification mark to a taximeter system where:</p> <p>(a) a taximeter has been installed in a public service vehicle as required by Regulations made under the Taxi Regulation Act 2003 (No. 25 of 2003),</p> <p>(b) such a taximeter is the subject of a certificate of type approval granted, or taken to be granted as part of a taximeter system, under Regulation 4 (4) of S.I. No.4 (Type Approval) Regulations 2006, or</p> <p>(c) the taximeter has been marked with the CE marking and the supplementary metrology marking in accordance with the provisions of Regulations 19, 20 and 21 of S.I. No.2 of 2018 (European Conformity Assessment of Measuring) Regulations (as amended).</p> <p>(d) as required by Reg 12 of S.I. No. 323 of 2008 Legal Metrology (General) Regulations 2008 (as amended)</p> <p>40. The transfer of a taximeter from one vehicle to another is deemed to invalidate the verification mark notwithstanding that any sealing or security arrangement remains unbroken or that the verification mark remains affixed or intact</p>
--	--

Table 5.1.2



6. Impetus for Data Sharing

Specify the impetus (the motivation or where benefits will be realised) in relation to the data shared under this agreement.

THE IMPETUS FOR THE DISCLOSURE OF DATA WILL COME FROM:	TICK AS APPROPRIATE
i. Data subject	<input type="checkbox"/>
ii. Public Body	<input checked="" type="checkbox"/>

Table 6.0



7. Categories of Data Shared

The personal data shared may be in relation to individual data subjects and/or classes of data subjects. Classes of data subject may be defined by the parties involved and some examples might be customers, vendors, suppliers, visitors, etc.

Aggregated data is information gathered and expressed in a summary form for purposes such as statistical analysis, and so is not personal data for the purposes of data protection law and GDPR and is not the same as classes of data subject.

Select from the below table and comment as appropriate.

CATEGORY		COMMENT
Individual Data Subject	<input checked="" type="checkbox"/>	Both parties carry out individual checks by licence number and review the data shared to enable an action to be carried out, i.e. a service offered or a function completed.
Classes of Data Subjects	<input type="checkbox"/>	

Table 7.0



8. Duration and Frequency

8.1 Duration

Define the start and end dates of the information transfer:

- i. NTA has been sharing data with LMS for the specified purpose since 2010 under a Memorandum of Understanding and will now continue to do so under this Data Sharing Agreement until the parties agree to terminate this agreement.

8.2 Frequency

Indicate the type of transfer that will be required with a description.

TYPE		DESCRIPTION
Once off	<input type="checkbox"/>	
Frequent/regular updates	<input checked="" type="checkbox"/>	LMS exposes a database dataset that is synchronised with their internal system. NTA's API consumes this data over a protected network. LMS shares data with NTA in real time. NTA shares data with LMS daily. The same technology is used for sharing NTA data with LMS.
Other frequency	<input type="checkbox"/>	

Table 8.2



9. How data will be processed

9.1 Obligations of the Parties in Respect of Fair and Lawful Processing

Each Party shall ensure that it processes the shared personal data fairly and lawfully. Each will comply with the requirements of the Data Protection Act 2018, GDPR and any legislation amending or extending same, in relation to the data exchanged.

Each Party undertakes to comply with the principles relating to the processing of personal data as set out in Article 5 GDPR, in the disclosing of information under this Data Sharing Agreement.

Both Parties shall, in respect of shared personal data, ensure that they provide sufficient information to data subjects in order for them to understand what components of their personal data the Parties are sharing, the purposes for the data sharing and either the identity of the body with whom the data is shared or a description of the type of organisation that will receive the personal data.

9.2 Description of Processing

Include a description of how the disclosed information will be processed by each receiving party.

DESCRIPTION OF PROCESSING	
Both parties	<p>LMS data is pulled by NTA based on individual SPSV licence search. The search can be carried out (electronically) in two places: in the electronic CABS vehicle licensing module and in the iCABS mobile application. Real-time LMS data is pulled in when a licence number is searched, and is used to carry out a licensing and compliance check on the vehicle and its operator. (In the case of non-compliance, the data may form part of further processing for law enforcement purposes, but this represents a small proportion of checks.) The data is never stored in the CABS database: it appears in read-only format on the user interface for the time that the screen remains open.</p> <p>The sharing of vehicle licence holder data with LMS is covered in the SPSV Privacy Notice, shared with SPSV operators and available on the NTA website: https://www.nationaltransport.ie/further-information/spsv-privacy-statement/</p> <p>LMS: LMS populate the TRAMS Taximeter owner/operator information using data provided by NTA once per day via an upload to a secured database table. The collection, use and management of this data is necessary to provide management of oversight for the function and accurately plan, coordinate and rollout inspection and compliance campaigns.</p> <p>The sharing of vehicle licence holder data with the NTA is covered in the NSAI Privacy Notice, available on the NSAI website: https://www.nsai.ie/about/publications/privacy-statement/</p>

Table 9.2



9.3 Further Processing

- i. Specify any further processing by the Party or Parties receiving data of the personal data disclosed by the disclosing body under this Data Sharing Agreement.

	SPECIFY FURTHER PROCESSING
[Insert Party Name]	N/A

Table 9.3.1

10. Restrictions

Specify any restrictions on the disclosure of information after the processing by the Party or Parties receiving data to the personal data disclosed by the disclosing body under this Data Sharing Agreement. Give a description of the restrictions, if any, which apply to the further disclosure of the information in table 10.0 below.

	RESTRICTIONS ON DISCLOSURE AFTER PROCESSING
Both parties	<p>Data will not be disclosed to any parties other than the parties to this Agreement, except to the extent otherwise required by applicable law.</p> <p>No data is processed other than for the purposes set out in this Agreement.</p> <p>Data cannot be accessed by any person in NTA or LMS unless they are securely logged in and have been granted the relevant permissions.</p> <p>Data retention rules for both parties are applied to delete the data in accordance with the parties' data retention policies.</p>

Table 10.0



11. Security Measures

11.1 Security and Training

Both Parties shall adhere to the procedures set out in [table 11.2](#) below, regarding the transfer and receipt of data.

The Party/Parties receiving data agree, in accordance Article 32 of the GDPR, to implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data transmitted, stored or otherwise processed.

This may include, but is not limited to:

- Policies, guidelines and procedures governing information security.
- Password protection for computer access.
- Automatic locking of idle PCs.
- Appropriate antivirus software and firewalls used to protect integrity and security of electronically processed data.
- Unique identifiers for every user with access to data.
- Employees have access only to personal data required for them to do their jobs.
- Appropriate security where remote access is allowed.
- Encryption of data held on portable devices.
- Data breach procedures.
- Appropriate physical security.
- Staff training and awareness.
- Monitoring of staff accessing data.
- Controlling physical access to IT systems and areas where paper-based data are stored.
- Adopting a clear desk policy.
- Appropriate techniques for destruction of data.
- Having back-ups of data off-site.

Both Parties shall ensure that the security standards appropriate to the transfer of personal data under this agreement are adhered to.

The Party/Parties receiving data shall ensure that all persons who have access to and who process the personal data are obliged to keep the personal data confidential.

The Party/Parties receiving data shall ensure that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data.

Access to the data supplied by the Party disclosing data will be restricted to persons on the basis of least privilege, sufficient to allow such persons carry out their role.

Each Party will keep the data secure and ensure that it is transferred securely in accordance with the procedures of this agreement.



11.2 Security Measures

For the purpose of this agreement, particular regard should be given to the data safeguards outlined in the following sections and subsections:

- 11.2.1 – Lead Agency/Party Disclosing Data
- 11.2.2 – Party/Parties Receiving Data
- 11.2.3 – Data Breaches and Reporting

11.2.1 Lead Agency/ Party Disclosing Data

The following questions should be completed by the Lead Agency/ party disclosing data in the data sharing arrangement.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.1.1	TRANSMISSION	COMPLIES	DOES NOT COMPLY
	When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Please provide details.	NTA pushes data to an LMS database. A series of IPs whitelisted on each side allow the communication between machines, overlaid with a suite of Firewall and WAF settings. Data Sync is used to secure LMS data being transmitted from NSAI TRAMS database to NTA Azure database and it is encrypted.	

Table 11.2.1

11.2.1.2 – SECURITY STATEMENT

Give an outline of the security measures to be deployed for transmission of personal data, in a manner that does not compromise those security measures.

You may also provide details of additional measures in place for the sharing of data that are relevant to this arrangement.

**NTA Security Statement:**

All SPSV data is housed in a be-spoke electronic licensing system called CABS, which is protected by robust WAF policies, is actively monitored by IT Security and is patched regularly. Access to CABS is restricted to registered users under the CABS access policy and an annual audit is completed. CABS is used by internal staff and a number of contracted service providers, with views based on the principle of least privileges implemented ensuring employees have access only to data required to do their Jobs. There is a 'Technical & Organisational Measures' (TOMs) policy in place for each service provider, reviewed annually. All technical changes to CABS are reviewed by the security team, and user access cannot be granted without approval from the business team.

As per the TOMs policy:

- All PCs accessing CABS must be password protected in accordance with NTA Password policy
- Idle PCs are automatically locked
- Appropriate antivirus software and firewalls are used to protect integrity and security of electronically processed data
- Unique identifiers are applied for every user with access to data
- Remote access is allowed only through VPN
- USB access is blocked by default.
- Logging and monitoring capabilities should be enabled.
- Data breach procedures apply
- Access to offices is managed by security staff
- Annual data protection and security training is completed
- Data retention rules are applied for both electronic and hard-copy data
- A clear desk policy is applied
- Data is backed-up using BaaS for virtual servers and a DR copy of the database is completed daily

Regarding the export of data from NTA to LMS, an extract of SPSV data is created five times daily and is pushed electronically to the LMS database. LMS IPs are whitelisted by the NTA WAF policy, ensuring the data cannot be sent anywhere else erroneously.

Regarding the import of data from the LMS database, data is pulled for individual licences when they are searched. The data appears in two internal electronic modules only; Vehicle Licensing and iCABS. As per the CABS access policy only users with the relevant system permissions can pull or view this data and this data cannot be downloaded or stored outside of CABS - it is read only access. A technical specification exists for each set of data shared.

NSAI Security Statement**Traders and Economic Operators**

Where we have enforcement functions, we collect personal information about people who are responsible for compliance with law. This information may be shared where we determine it necessary to uphold the law and it may also be shared where we have a written agreement with another public body for such arrangement. Your rights to access, restrict and delete your personal data may be subject to exceptions when it is processed for these purposes.

Security of Personal Data

NSAI has organisational, physical, administrative and technical measures in place to protect the personal data we collect and process. We monitor the measures to ensure information is secure and operating in a manner to reasonably protect the collected and processed information. The information security systems and measures are upgraded from time to time to limit risks of unauthorised disclosure. NSAI is accredited to ISO 27001 (international standard for information security management).

A procedure runs on a scheduled basis that builds relevant tables and populates data from TRAMS to NSAI Sync table in a separate database.

- Data sync tool installed on NSAI server that syncs changed data from on premise table to Azure



- Standalone NTA sync database located in Azure
- NTA provided with username/Password to connect into Azure database
- Read only access given
- NTA can only connect via supplied IP address that has been provided to NSAI and whitelisted, all other connections blocked

11.2.1.3 SECURITY SPECIALIST FOR LEAD AGENCY**YES/NO**

Please confirm your security specialist has reviewed this Data Sharing Agreement and that their advice has been taken into consideration.

YES

Table 11.2.2



11.2.2 Party/Parties Receiving Data

The following questions should be completed by the Party receiving the disclosure of data as part of this Data Sharing Agreement.

Where a 'not applicable' response is included, ensure information is provided as to why.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1	<p>In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.</p> <p>Please provide details for all non-complying or 'not applicable' statements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2.2	<p>Appropriate controls are in place if the disclosed data is accessed remotely.</p> <p>Please provide details.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2.3	<p>A least privileged principle (or similar) is in place to ensure that users are authenticated proportionate with the level of risk associated to the access of the data.</p> <p>Please provide details.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2.4	<p>Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).</p> <p>Please provide details of the protections in place and how they are managed.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



11.2.2.5	Data is encrypted at rest on mobile devices such as laptops and removable media. Please provide details for all non-complying or 'not applicable' statements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2.6	There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location. Please provide details.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		NTA has "read-only" access to the LMS data. LMS data cannot be downloaded or saved by the NTA. LMS access to stored data is restricted to authorised users only and this policy is reviewed periodically. A least privilege access policy applies.		
11.2.2.7	Do you have policy in place that protects data from accidental erasure or other loss? Please provide details.	NTA and NSAI IT Backup policy		
11.2.2.8	Is data stored in a secure location only for as long as necessary and then securely erased? Please provide details.	NTA has "read-only" access to the LMS data on a per licence search basis. LMS data is not stored by the NTA. It is deleted from the CABS user interface as soon as the user leaves the screen. LMS: Please refer to Section 10 above. Data clear down is built into the data update procedure whereby new data overwrites old data.		

Table 11.2.3

**11.2.2.9 – SECURITY STATEMENT**

Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures.

You may also provide details of additional measures in place that are relevant to this arrangement.

All existing security measures are covered in detail in the sections above. LMS's DPIA was completed and used as input to this section.

Regular internal and third-party audits are conducted on an annual basis to support certification to ISO: 9001 and to manage IT Security Controls.

NSAI have received ISO 270001 certification

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA**YES/NO**

Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.

YES

Table 11.2.4

11.3 Data Breaches and Reporting

If a personal data breach occurs after the data is transmitted to the Party/Parties receiving data, the Party/Parties receiving data will act in accordance with the Data Protection Commission's Breach Notification Process and in accordance with GDPR requirements.



12. Retention

Define the retention requirements for the disclosed information for the duration of the Data Sharing Agreement and in the event the agreement is terminated, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

INFORMATION TYPE	RETENTION REQUIREMENTS
1. Information to be disclosed	NTA data imported into the LMS system: data clear down is built into the data update procedure whereby new data overwrites old data monthly. NTA has “read-only” access to the LMS data on a per licence search basis. LMS data is not downloaded or retained by the NTA. It is deleted from the CABS user interface as soon as the user leaves the screen.
2. Information resulting from the processing of the data	None

Table 12.0



13. Methods Used to Destroy/Delete Data

Detail how information will be destroyed or deleted at the end of the retention period as defined in the Data Sharing Agreement, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

INFORMATION TYPE	DESCRIPTION
1. Information to be disclosed	<p>The deletion of retained data is determined by the active status of the data subject's licensing information and, where applicable, any outstanding legal non-compliance notifications.</p> <p>LMS retains NTA data in the TRAMS database only while the data subject—whether as an owner (primary data subject) or operator (secondary data subject)—possesses Type Approved instruments for trade or has outstanding non-compliance notifications related to those instruments. The owner and operator may be the same individual.</p> <p>All personal data will be deleted once the data subject's licensed status is marked as 'dead' in the NTA shared data or when they cease to be the owner/operator. If applicable, any retained information related to non-compliance will be deleted once outstanding notifications are resolved.</p> <p>If non-compliance remains unresolved, LMS will continue to retain the primary data subject's information until the issue is resolved.</p> <p>Retained data is periodically reviewed to ensure only relevant personal information is kept. Any data deemed non-relevant is automatically deleted through the TRAMS system.</p> <p>LMS data is not retained by NTA in the CABS database at all. It is deleted from the user interface as soon as the user leaves the screen</p>
2. Information resulting from processing of the data	None

Table 13.0



14. Withdrawal from Agreement

14.1 Procedure

Each Party commits to giving a minimum of 90 days' notice of its intention to withdraw from or terminate this Data Sharing Agreement.

Each Party disclosing personal data pursuant to this Agreement reserves the right to withdraw, without notice, access to such data where that Party has reason to believe the conditions of this Data Sharing Agreement are not being observed. Each Party disclosing data will accept no responsibility for any consequences arising from the exercise of this right.

Where the disclosing Party is subsequently satisfied that the conditions of the Data Sharing Agreement are being observed, access will be restored forthwith.

Where access to shared personal data is withdrawn, the withdrawing Party shall provide to the other Party reasons for that withdrawal as soon as is practicable thereafter. Where there are only 2 Parties, withdrawal by either one shall be considered a termination of the agreement. Where an agreement has multiple Parties and one withdraws, the Lead Agency should update the schedule and inform the other Parties to the agreement.

Where a Data Sharing Agreement expires or is terminated, the Lead Agency shall notify the Minister in writing within 10 days of the withdrawal. The Lead Agency shall also notify the Data Governance Board as soon as practicable after such expiration or termination, as the case may be.

14.2 Severance

If any provision of this agreement (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this agreement, and the validity and enforceability of the other provisions of this agreement shall not be affected.



15. Other Matters

15.1 Variation

No variation of this agreement shall be effective unless it is contained in a valid draft amendment agreement executed by the Parties to this Data Sharing Agreement in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.2 Review of Operation of the Data Sharing Agreement

The Parties shall review the operation of the Data Sharing Agreement on a regular basis, with each such review being carried out on a date that is not more than 5 years from:

- i. in the case of the first such review, the date on which the Data Sharing Agreement came into effect, and
- ii. in the case of each subsequent review, the date of the previous review. A review under s.20(1) shall consider the impact of the technical, policy and legislative changes that have occurred since the date of the previous review under s.20(1).

Where the Parties to the Data Sharing Agreement consider that it is appropriate following completion of a review they shall prepare an amended Data Sharing Agreement to take account of the technical, policy and legislative changes that have occurred since the date of the previous review or the effective date. The amended agreement will be executed by the Parties in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.3 Jurisdiction

This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of the Republic of Ireland.

15.4 Indemnity

The Party/Parties receiving data shall indemnify and keep indemnified the Party/Parties disclosing data, in full, from and against all claims, proceedings, actions, damages, losses, penalties, fines, levies, costs and expenses, whether direct or indirect and all consequential or indirect loss howsoever arising out of, in respect of or in connection with any breach by the Party/Parties receiving data, including their servants, of data protection requirements.

15.5 Publication

15.5.1 Public Consultation and publishing a Notice

Public Consultation is managed on behalf of the parties by the Data Governance Unit in OGCI. Each of the proposed parties will be required to publish, on the same date as the consultation, a notice on their website that they are proposing to enter into the DSA. They should state the documents that are accessible to the public and link to their relevant DSA and DPO statements published on the public consultations website. This notice should invite submissions and include the date of publication of the notice.



15.5.2 Publishing Executed DSA

After each of the Data Governance Board recommendations have been addressed by the parties and after this Data Sharing Agreement has been signed by appropriate Authorised Signatories, the Lead Agency in respect of this Data Sharing Agreement shall publish a copy of the final agreement on a website maintained by it as soon as practicable after sending a copy of the agreement to the Data Governance Unit who will accept it on behalf of the Minister.

15.6 Base Registries

In respect of this Data Sharing Agreement, where the personal data disclosed is contained in a Base Registry, the Base Registry owner will take on the role of Lead agency.



16. Schedule A - Data Protection Impact Assessment

If a data protection impact assessment (DPIA) has been conducted in respect of the data sharing to which this Data Sharing Agreement relates, a summary of the matters referred to in [Article 35\(7\)](#) of the GDPR is required to be filled in the table below.

OR

If a data protection impact assessment has not been conducted as it is not mandatory where processing is not “likely to result in a high risk to the rights and freedoms of natural persons” ([Article 35](#) of the GDPR), outline the reasons for that decision in the table below.

DPIA	Select	SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT
Has been conducted	<input type="checkbox"/>	
Has not been conducted	<input checked="" type="checkbox"/>	<p>NTA, as Lead Agency and in accordance with its own policies and procedures as a Data Controller, has conducted an evaluation in order to determine whether a DPIA is necessary. A separate DPIA was not deemed to be necessary as the processing of this data does not adversely impact on the rights and freedoms of the data subject. As part of this evaluation, it considered that the sharing of SPSV data with LMS was in place prior to 25 May 2018, that data is not being processed for a new purpose and no changes to how this data is processed have been made.</p> <p>That said, the sharing of SPSV licence data by NTA with LMS is included in NTA's main DPIA for SPSV vehicle licensing, as one of the ways in which personal data is processed, and this processing is covered in the SPSV Privacy Notice available on the NTA website. When NTA began receiving LMS data in 2022, the DPIA for SPSV vehicle licensing was reviewed and the process and data was included.</p> <p>In accordance with Article 32 of the GDPR, NTA and LMS will implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data transmitted, stored or otherwise processed. NTA and LMS will keep the data secure and ensure that it is transferred securely in accordance with the procedures of this agreement.</p> <p>Shared personal data shall be limited to the personal data described in this agreement and will be shared only in the manner as set out in this agreement and only for the purposes specified in the agreement.</p>



	<p>Both parties have the appropriate data protection policies in place and have taken the measures to ensure data subjects can exercise their rights under Articles 12 to 22 of the GDPR.</p> <p>Note: LMS as Other Agency has completed a DPIA to cover the data shared. NSAI took the view that as this process is moving under a DSA, it was appropriate to carry out a DPIA under the category of 'new process', notwithstanding the process has been governed under an MoU previously. The preliminary findings of the draft DPIA indicate very low risks.</p> <p>In reaching this finding, NSAI considered whether the data shared posed risks to the rights and freedoms of the data subjects. NSAI had regard to certain potential risks to data subjects, including but not limited to:</p> <ul style="list-style-type: none">• evaluation or scoring, including profiling and predicting using information about an individual (recitals 71 and 91)• automated decision making which has a legal or similar legal effect on an individual (Article 22 and Article 35(3)(a))• systematic monitoring, that is, processing used to observe, monitor or control individuals, including data collected through networks (including monitoring of a publicly accessible area on a large scale) (Article 35(3)(c))• sensitive/special data about individuals of a kind particularly likely to raise privacy concerns or expectations (Articles 9 and 10 and 35(3)(b))• data being processed on a large scale (recital 91)• matching or combining of datasets (recital 91)• data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? (recital 75)• innovative use or applying new technological or organisational solutions (Article 35(1) and recitals 89 and 91)• processing in itself 'prevents the data subject from exercising a right or using a service or a contract' (Article 22 and recital 91) <p>Having regard to the nature of the above referenced risks, the view taken that none of the factors outlined in Art 35(3) of the GDPR, NSAI reached the conclusion that the data shared poses a very low risk to the rights and freedoms of data subjects.</p>
--	--

Table 16.0

Note: If the Data Sharing Agreement is amended to reflect a change in the scope, form or content of the data processing, then there is an obligation on the data controllers to consider whether the



changes give rise to a high risk to the rights and freedoms of natural persons, such that a DPIA should be carried out.

Under [S.20](#)(4) of Data Sharing and Governance Act, an amended draft agreement must be submitted for review to the Data Governance Board in accordance with Part 9, Chapter 2 of the Data Sharing and Governance Act.



17. Schedule B

17.1 Necessary for the Performance of a Function

Outline the reasons why the disclosure of information under this agreement is necessary for the performance of the relevant function and explain why it is proportionate in that context.

The disclosure of information under this agreement is necessary to allow the NTA, as licensing and regulatory authority for SPSVs, to perform its legal and administrative functions in accordance with the provisions of the 2013 Act (as amended), and to provide the LMS with the relevant information to perform its function of inspection, testing and verification (under secure seal) of taximeter systems pursuant to the Metrology Act 1996.

Necessary and Proportionate for the NTA:

A stated function of the NTA is to operate and maintain a regulatory framework for the licensing and regulation of the standards to be applied to SPSV vehicles and their drivers. In order to carry out this function, the NTA need to share and receive certain SPSV data with the appropriate statutory public bodies, including the LMS. Pursuant to the relevant taxi legislation, all SPSV's must have their taximeters verified and sealed by the LMS. It is therefore necessary and proportionate that SPSV licence information is provided by the NTA to LMS to enable persons with an active SPSV vehicle licence to have their taximeter verified and sealed by the LMS. Equally, it is necessary and proportionate that the NTA receives the results of this verification and sealing from the LMS to ensure that persons with an active SPSV licence are operating with a taximeter which has been verified and sealed by the LMS. Data minimisation principles have been applied to this process and no superfluous personal information is shared for this purpose.

Necessary and Proportionate for the LMS:

Pursuant to Regulations 7 and 8 of the 2008 Regulations:

- A taximeter used for the purpose of trade shall be legally inspected in accordance with the 2008 Regulations. The outcome of these inspections may result in the instrument being taken out of service or allowed to continue in use.
Upon statutory inspection and where an instrument has been found to be in breach with any of the requirements as described with the subsections and regarding the severity of the non-compliance, an inspector may allow the instrument to continue in use but shall issue the operator with a notice covering a period not exceeding 20 working days. The non-conformance should be rectified within this notice period. Where the notice period expires without the necessary follow up action the inspector shall remove the instrument from trade-use and the non-conformity mark shall be applied to the instrument. The active status (compliance) of a taximeter relating to inspection activities of this nature shall be made available to NTA to ensure each taximeter is currently verified and sealed by LMS.

Regulation 39(3) of the 2008 Regulations prohibits the testing of a taximeter system “*unless the taximeter has a software programme installed that has been found by the Legal Metrology Service to comply with the maximum fares order in force under the Taxi Regulation Act 2013*”. It is therefore necessary that the LMS obtain such information from NTA (the regulatory body for SPSVs) prior to carrying out testing.

Following the inspection, verification, and sealing of an SPSV taximeter, the LMS then share this resulting data with the NTA. It is necessary that this information is shared with NTA as only LMS can verify this data. Data minimisation principles have been applied to this process and no superfluous personal information is shared for this purpose



17.2 Safeguards

Summarise the extent to which the safeguards applicable to the data shared under this agreement are proportionate, having regard to the performance of functions by the Parties and the effects of the disclosure on the rights of the data subjects concerned.

See above Security Statement for relevant safeguards. It is critical that this data be safeguarded against unintended disclosure or erasure, and each of the safeguards in place mitigates against the risk of this occurrence.

Since 2010 no data breaches have occurred.

NTA has a data breach policy in place which can be implemented if required. NSAI has a suite of policies and security measures in place to safeguard data and respond to data breaches.



18. Schedule C

18.1 List of Parties to this Agreement

Set out the names of all the Parties to the agreement.

As required under [S.21](#) (3)(a), (b) and (c) of the Data Sharing and Governance Act 2019, this Schedule must be updated by the Lead Agency to include any Parties who have joined the agreement by way of an Accession Agreement, and to remove any Party that has withdrawn from the agreement. The Lead Agency must notify the other Parties of any amendments to this Schedule and the Data Governance Board.

- | |
|---|
| <ol style="list-style-type: none">1. National Transport Authority2. NSAI Legal Metrology Service |
|---|



19. Authorised Signatory

An authorised signatory is required to sign this Data Sharing Agreement after all recommendations made by the Data Governance Board have been addressed and before the Data Sharing Agreement can be executed.

This signatory has the role of accountability for the data sharing defined in this Data Sharing Agreement and holds the post of Principal Officer (equivalent) or above.

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

19.1 Lead Agency

LEAD AGENCY			
Signature:		Date:	
Print Name:			
Position held:			
Email:			
For and on behalf of:			

Table 19.1

19.2 Other Party/Parties

OTHER PARTY			
Signature:		Date:	
Print Name:			
Position held;			
Email:			
For and on behalf of:			

Table 19.2

[Append further Authorised Signatory sections for each additional Party, use same format as above table 19.2.]



Data Protection Officers Statement

This Statement is separate to the Data Sharing Agreement. It is required by law under section 55(1)(d) of the Data Sharing and Governance Act 2019. The Data Protection Officers in each proposed Party must sign and complete this statement before the Data Sharing Agreement is submitted to the Data Governance Unit for Public Consultation and again at execution stage. This statement will be published on a public website.

The Data Protection Officers in each proposed Party to this Data Sharing Agreement must ensure that they:

- i. have reviewed the proposed agreement, and
- ii. are satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law,
- iii. are satisfied that the agreement is consistent with Article 5(1) of the GDPR

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

Lead Agency DPO Statement

LEAD AGENCY DATA PROTECTION OFFICERS STATEMENT			
I have reviewed the proposed agreement			<input checked="" type="checkbox"/>
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			<input checked="" type="checkbox"/>
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			<input checked="" type="checkbox"/>
Signature:	Deirdre Glennon	Date:	14 May 2025
Print Name:	Deirdre Glennon		
Position:	Data Protection Officer		
Email:	Privacy@nationaltransport.ie		
For and on behalf of:	National Transport Authority		

Table 20.1



Other Party/Parties DPO Statement

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			<input checked="" type="checkbox"/>
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			<input checked="" type="checkbox"/>
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			<input checked="" type="checkbox"/>
Signature:	Francis Monds	Date:	14 May 2025
Print Name:	Francis Monds		
Position:	Data Protection Officer		
Email:	dataprivacy@nsai.ie		
For and on behalf of:	National Standards Authority of Ireland]		

Table 20.2