DRAFT

DATA SHARING AGREEMENT

Between

The Office of the Revenue Commissioners

and

Department of Agriculture, Food and the Marine,
Department of Enterprise, Trade and Employment,
The Road Safety Authority,
Tailte Éireann – Valuation,

Department of Public Expenditure NDP Delivery and Reform – OGCIO.

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

Allowing Revenue to share Unique Business Identifier Number (UBIN) data, enabling consistent identification of businesses and improving the quality and accuracy of business data holdings across the Public Service.

Table of Contents

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

Glossary

Provide a plain English description of terms, phrases, acronyms or abbreviations used within the content of this DSA.

It is advised to include rare, unfamiliar, specialised or technical terms that are content-specific in table 1.1 below.

The purpose of this glossary is to serve as a dictionary for the reader that they can reference throughout.

Term/Phrase/ Acronym/Abbrev	DESCRIPTION
AES	Annual Employment Survey
AWS	Amazon Web Services
BAR	Brexit Adjustment Reserve
CAP	Common Agricultural Policy
CPR	Common Provisions Regulations
CRO	Companies Registration Office
CSO	Central Statistics Office
CVR	Commercial Vehicle Roadworthiness
CVRT	Commercial Vehicle Roadworthiness Testing
DAFM	Department of Agriculture, Food & the Marine
DLP	Data Leaks Protection
DEASP	Department of Employment Affairs and Social Protection
DETE	Department of Enterprise, Trade and Employment
DPENDR	Department of Public Expenditure NDP Delivery and Reform
Driver CPC	Driver Certificate of Professional Competence
EDW	Enterprise Data Warehouse
EPPM	Enterprise Project and Portfolio Management solution
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IPsec	Internet Protocol Security
ISO	International Organisation for Standardisation
IT	Information Technology
MDM	Mobile Device Management
MFA	Multi-Factor Authentication

NACE	A pan-European classification system that groups organisations according to their business activities. It is derived from the French *Nomenclature Statistique des Activites Economiques dans la Communaute Europeenne*
OGCIO	Office of the Government Chief Information Officer
On Prem	On Premise
PREM	Employers (PAYE/PRSI) registration
R&D	Research and Development
Revenue	The Office of the Revenue Commissioners
ROS	Revenue Online Service
RRF	Recovery and Resilience Facility
RSA	Road Safety Authority
SBCI	Strategic Banking Corporation of Ireland
SDC	Statistical Disclosure Control
TPM	Trusted Platform Module
UBIN	Unique Business Identifier Number
USB	Universal Serial Bus
VPN	Virtual Private Network

Table 1.1

Data Sharing Agreement

BETWEEN

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

LEAD AGENCY NAME	ADDRESS
The Office of the Revenue Commissioners	Upper Yard, Dublin Castle, Dublin 2, D02 F342

AND

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

PARTY NAME	ADDRESS
Department of Agriculture, Food and the Marine	Agriculture House, Kildare Street, D02 WK12
Department of Enterprise, Trade and Employment	23 Kildare St, Dublin 2
Road Safety Authority	Moy Valley Business Park, Primrose Hill, Dublin Road, Ballina, Co Mayo
Tailte Éireann – Valuation	Block 2, Irish Life Centre, Abbey Street Lower, Dublin 1, D01 E9XO
Department of Public Expenditure NDP Delivery and Reform – OGCIO	3A Mayor Street Upper, North Wall, Dublin 1, D01 PF72

The Parties hereby agree that The Office of the Revenue Commissioners 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?	NO

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?	YES
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 effect[1].

	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	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): Lists of Types of Data Processing Operations which require a DPIA. (*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)*	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.	☒
II	To identify and correct erroneous information held by one or more of the public bodies mentioned.	☒
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.	☒
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).	☒
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.	☒
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.	☒
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.	☒
VIII	To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned.	☒

Table 2.2

2.3 Details about the Purpose

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

PURPOSE	PARTY	DESCRIPTION
	All parties	Section 35 of the Data Sharing and Governance Act 2019 states that the Minister for Public Expenditure, National Development Plan Delivery and Reform (DPENDR) may, for the purpose of uniquely identifying an undertaking, allocate and issue a number (to be known as the "unique business identifier number") to that undertaking. Also, the Minister may, with the consent of such other Minister of the Government, if any, in whom functions in relation to the public body are vested, by order delegate his or her functions under subsection (1) to a public body. The functions of the Minister for DPENDR under section 35 (1) of the Data Sharing and Governance Act 2019 (No. 5 of 2019) were accordingly delegated to the Revenue Commissioners. The Office of the Revenue Commissioners (Revenue) will uniquely identify an undertaking, allocating and issuing a number, known as the "unique business identifier number" to that undertaking. The role Revenue has in this proposed DSA will be, to make available to other Public Sector Bodies (PSBs)

		a dataset of Irish businesses containing a newly created Unique Business Identifier Number (UBIN) and certain other identifying information. All taxpayers on Revenue systems with: 1) a live CRO number, and/or 2) a live VAT number will be included in the dataset. The purpose of this DSA is to: • Enable the consistent identification of businesses across the public service. • To improve the quality and accuracy of business data holdings in the public service • To facilitate the efficient linking of business data within and across PSBs The first beneficiaries will be the Parties outlined in this notification, that use the UBIN service. The UBIN dataset (as noted in table 3.4, personal and non-personal data, items 1 – 9) will have the following benefits: • It will remove out of date business data held by PSB's. • It will provide up to date business data and validate existing business data held by PSB's, removing duplication of business records, improving public services by harnessing data effectively, leading to better data sharing and interoperability to streamline service delivery, aligning with the principles to deliver a Digital and ICT Strategy for Ireland's Public Service by 2030. • It will allow PSB's to identify business that have entitlements to, or are beneficiaries of, grants or other types of Government and/or European Union (EU) funding. • Where necessary, the cross referencing of business data will lead to more accurate reporting to Government and the EU. • When Revenue is notified by a business of a change in their business name or address etc. (the type of data being shared as noted in table 3.4), this information will automatically be updated to the parties outlined in this DSA and any PSB that is not an original signatory but who has acceded to this agreement, therefore reducing the burden on businesses to update this data with multiple PSB's. • In all, the UBIN dataset will reduce the administrative burden of businesses by providing PSB's with a consistent and reliable source of identification of a business, the type of business that business carries out and the location/s of the business.
I - To verify the identity of a person, where one or more of the public	**RSA**	The data will be accessed by the RSA to verify the identity of a business so as to facilitate the creation of an RSA online business registration account and enable that company avail of an RSA online service.

bodies are providing, or proposing to provide	**DETE**	DETE will use the UBIN webservice to confirm the following details about business entities. 1. Assigned Companies Registration Office (CRO) number. 2. VAT number. 3. Unique Business Identifier Number. 4. Business Name. 5. Business Address. 6. Eircode. 7. PREM number. 8. NACE code. 9. NACE Description. DETE will use the data for the purposes of verification of the identity of a business and may also use the data to verify the identity of a business or a person. This verification process is required for the purposes of producing national statistical publications to inform policy formulation and for research and analysis purposes. The data sets are not published in raw format and will remain unpublished in this format. The data will be accessed by DETE for the purposes of verification of the identity of a business and may be used to identify and correct erroneous information held by DETE. This verification and correction of erroneous data will be used to enhance policy formulation and programme/project formulation by the DETE. The accuracy of these data sets will also enhance the targeting of enterprise support programmes and be used to inform future policy programme-specific funding aimed at maximising productive capacity, employment creation and sustainability which are part of the core functions of the DETE. DETE will use the UBIN data to reduce or avoid the administrative burden of re-collecting identifying information about our business customers to whom we are delivering a service or a scheme. This will assist the DETE in meeting the cross-government objectives set out in the Public Service Data Strategy. DETE will use the UBIN data or information previously provided to establish the entitlement of a person to the provision of DETE schemes and services. The data will be used to ensure value for money for Exchequer funding and to reduce the risk of incidences of fraud. The data sets will also be used to inform the effectiveness of targeted schemes and services and inform future policy formulation. DETE propose to use the UBIN to facilitate the administration, supervision and control of DETE services / schemes to businesses and in the broader development of policy deliverables. The data sets will be used for analysis in the DETE of the effective administration, supervision and control of targeted and sector-specific services and schemes to business and inform future policy formulation aimed at achieving the DETE's mandate. DETE intend to utilise the UBIN to facilitate and enhance the delivery of schemes and services whilst providing data to enhance policy making decisions. The availability of up-to date and accurate data sets is essential in assisting the DETE to more effectively analyse the efficacy of targeted funding and enhancing the design and delivery of schemes and services to

		meet its mission while also providing value for money for the Exchequer. DETE purport to use UBIN data for the evaluation and review of schemes/services and programmes. This will facilitate the development of future programmes/services and policy implementation. The data sets will be used to evaluate and review both existing and future schemes, programmes and services to provide greater insight into the effectiveness of such initiatives and provide qualitative analysis to inform the future formulation of such initiatives. For example, the Ukraine Credit Guarantee Scheme, the Growth and Sustainability Loan Scheme, the Tailored Company Expansion Package. DETE intend to apply the UBIN to support the analysis of its business functions and programmes which is reliant on up-to-date and valid data. Real-time, accurate data sets are essential in assisting the DETE to enhance its quantitative and qualitative analysis of the effectiveness of the delivery of its business functions and ensuring that targeted funding initiatives are meeting enterprise needs to generate sustainable employment creation and sustainability. The personal data received within UBIN data transfer has been assessed to be necessary to assist the DETE in meeting its statutory functions and aligns to the broader government objectives contained within the Public Service Data Strategy.
	DAFM	DAFM will use the UBIN webservice to confirm the following details about business entities registered with the department. 1. Assigned Companies Registration Office (CRO) number. 2. VAT number. 3. Unique Business Identifier Number. 4. Business Name. 5. Business Address. 6. Eircode. 7. PREM number. 8. NACE code. 9. NACE Description. The data will be accessed by DAFM for the purposes of verification of the identity of a business and may be used to verify the identity of a business or a person.
	TE	The data will be used by Tailte Éireann - Valuation for the purposes of cross-validation of the occupier of a commercial property using the UBIN, to improve the accuracy of commercial property records by having access to the most up-to-date information.
	DPENDR	DPENDR will use the UBIN webservice to confirm the following details about business entities that will be beneficiaries of EU Funds including the Common Provisions Regulations, the

		Recovery and Resilience Facility and the Brexit Adjustment Reserve. 1. Assigned Companies Registration Office (CRO) number 2. VAT number. 3. Unique Business Identifier Number 4. Business Name 5. Business Address 6. Eircode 7. PREM number 8. NACE code 9. NACE Description The data will be accessed by DPENDR for the purposes of verification of the identity of a business and may be used to verify the identity of a business or a person.
II - To identify and correct erroneous information held by one or more of the public bodies mentioned.	**RSA**	The data will be accessed by the RSA to correct erroneous information which the RSA may hold in relation to a business entity engaging with the RSA.
	DETE	The data will be accessed by DETE to correct erroneous information which DETE may hold in relation to a business entity engaging with DETE.
	DAFM	The data will be accessed by DAFM for the purposes of verification of the identity of a business and may be used to identify and correct erroneous information held by DAFM.
	TE	The data will be accessed by Tailte Éireann – Valuation for the purposes of cross validation against our commercial records. This will alert us to any inconsistencies between the datasets that will need to investigated and fixed
	DPENDR	The data will be accessed by DPENDR to uniquely identify and correct erroneous information held on corporate beneficiaries by DPENDR.
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	**RSA**	The data will be accessed by the RSA as part of the creation of an RSA online business registration account. By having access to the UBIN data it will reduce or remove the need for the RSA to collect the same information from the same businesses when they are availing of various RSA Services.
	DETE	With the UBIN it may be possible to reduce the survey burden that we place on companies by using data collected by other public sector bodies instead of surveying the companies. By having access to the UBIN data it will reduce or remove the need for the DETE to collect the same information from the same businesses when they are availing of various DETE Services.
	DAFM	DAFM will use the UBIN data to reduce or avoid the administrative burden of collecting identifying information about our business customers to whom we are delivering a service or a scheme.
	TE	To reduce the administrative burden associated with correcting erroneous data and to reduce delays in service delivery associated with inaccurate data.

directly from that person.	**DPENDR**	The data will be used to minimise the administrative burden related to the collection of information on business that are delivering outcomes that are funded (wholly or in part) through the application of EU Funds.
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).	**RSA**	The UBIN data will assist the RSA in establishing the entitlement of a business to the provision of an RSA Service. For example, in determining whether a Transport Operator is involved in the provision of freight or passenger transportation can be obtained via the NACE code element of the UBIN and so assist in providing of RSA related services to Bus Operators.
	DETE	DETE will use the UBIN data or information previously provided to establish the entitlement of a person to the provision of DETE schemes and services.
	DAFM	DAFM will use the UBIN data or information previously provided to establish the entitlement of a person to the provision of DAFM schemes and services.
	DPENDR	DPENDR will use the data to enhance the validation of corporate beneficiaries and to limit fraudulent activity across the draw-down of EU funds.
	TE	To more efficiently establish the correct valuation of commercial property for business occupiers and ensure equity for businesses in the service of valuation.
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.	**RSA**	The RSA will use the data for the purposes of facilitating the administration, supervision and control of RSA services to businesses by using it as part of the process to create an RSA online business registration account.
	DETE	DETE propose to use the UBIN to facilitate the administration, supervision and control of DETE services / schemes to businesses and in the broader development of policy deliverables.
	DAFM	DAFM propose to use the UBIN to facilitate the administration, supervision and control of DAFM services / schemes to businesses and in the broader development of policy deliverables.
	TE	The data will be accessed by Tailte Éireann – Valuation for the purposes of facilitating the administration, supervision and control of services to business.
	DPENDR	DPENDR will use the UBIN to facilitate the administration, supervision and control of programmes and systems to ensure compliance with national and EU regulatory requirements.
VI - To facilitate the improvement or	**RSA**	The RSA will use the UBIN data to facilitate the targeting of an existing service, programme or policy and enhance decision making around proposed decisions or policies in relation to road

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.		safety. For example, the UBIN data would assist RSA in being able to provide customised and relevant road safety messaging of interest to specific business groupings.
	DETE	The UBIN will facilitate the improvement of DETE policies being delivered by linking DETE business datasets with datasets in other departments, enabling fresh analysis for policy making.
	DAFM	DAFM intend to utilise the UBIN to facilitate and enhance the delivery of schemes and services whilst providing data to enhance policy making decisions.
	TE	The UBIN dataset will support the Tailte Éireann strategy for more digitally driven services and integration between valuation, surveying and registrations to improve the provision of public services.
	DPENDR	DPENDR will use the data to improve the delivery of the EU funds programmes by ensuring that only those corporate beneficiaries entitled to claim are awarded funds.
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.	**RSA**	The RSA will use the UBIN data to aid in road safety related policy evaluation and oversight. It will also mean our datasets relating to businesses can be enriched and offer further potential for approved research cases led internally in RSA or via agencies such as the CSO.
	DETE	DETE will use the UBIN dataset to facilitate the evaluation, oversight or review of services, programmes and policy.
	DAFM	DAFM purport to use UBIN data for the evaluation and review of schemes/services and programmes. This will facilitate the development of future programmes/services and policy implementation.
	TE	The UBIN webservice will provide data to enable the evaluation, oversight or review of a service, programme or policy delivered or implemented for enterprises.
	DPENDR	The verification of data help by DPENDR through the UBIN webservice will assist in the review of funds provided to businesses to minimise or eliminate potential fraud, corruption and or conflicts of interest related to the drawdown of monies by business across multiple funds.
VIII - To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned.	**RSA**	The RSA will use the UBIN data to assist in analysis of items such as the service delivery channels (online or in person) being availed of by our business customers.
	DETE	Through the implementation of the UBIN, DETE will gain validation of its data which will enable better evaluation of its supports to businesses.
	DAFM	DAFM intend to apply the UBIN to support the analysis of its business functions and programmes which is reliant on UpToDate valid data.
	TE	The UBIN dataset will support the analysis and identification of appropriate uses for digitally driven automations for future valuations and to improve the speed of service delivery.
	DPENDR	The UBIN webservice will provide validation of information already being collected as part of the payment application for EU funds, providing a single identifier, avoiding duplication and the re-use of existing investment across the Public Service supporting the build once, use often principle for digital services.

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	• Unique Business Identifier Number • Business Name • Business Address • Eircode • VAT number • PREM number • CRO number
Non-personal Data	• NACE code • NACE description.

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	Legislation
i. **The Office of the Revenue Commissioners**	Revenue's mission is to serve the community by fairly and efficiently collecting taxes and duties and implementing Customs controls. Revenue maintains records on businesses operating in the Irish state that submit information to Revenue as part of their fiscal obligations.	1. Section 879 (2) of the Taxes Consolidation Act. 1997 as amended. 2. Section 880 of the Taxes Consolidation Act. 1997 as amended. 3. Section 882 of the Taxes Consolidation Act, 1997 as amended. 4. Section 988 of the Taxes Consolidation Act. 1997 as amended. 5. Section 65(1) of the VAT Consolidation Act. 2010 as amended. Giving effect to 6. Article 19 of the Council Regulation (EU) No. 904/2010.
ii. **Road Safety Authority**	Our mission is to make Irish roads safer for everyone. The functions for which the RSA is responsible are set out in the Road Safety Authority Act, 2006 and the Commercial Vehicle Roadworthiness Act 2012, and related conferral of functions orders. They include driver testing and training, driver licensing, vehicle testing and standards and enforcement functions, road safety promotion, driver education, and road safety research.	1. S.4 of the Road Safety Authority Act, 2006 as amended, and related Conferral of Functions Order 2006 S.4 RSA Act 2006 RSA Act 2006 (Conferral of Functions) Order; 2. S.37 of the Commercial Vehicle Roadworthiness Act 2012 and related

	The RSA is required to maintain records of businesses spanning across a wide range of its functions including specifically in relation to the following: • Commercial Vehicle Roadworthiness Testing (CVRT). • Driver Certificate of Professional Competence (CPC) services (including managing approval and quality assurance of CPC training organisations). • Tachograph card service (including issuing of company cards). • Standardisation and quality assurance of driver instruction. • Delivery of driving tests (including for bus and truck categories). In line with the Government strategy on digitalisation of public services the RSA are consolidating its online services onto one platform and this includes the services availed of by business customers.	regulations S. 37 of CVR Act 2021; 3. Regulation 6 of the European Union (Road Transport) (Working Conditions and Road Safety) Regulations 2017 (SI 229 of 2017). 4. European Communities (Vehicle Drivers Certificate of Professional Competence((No.2) Regulations 2008 (SI 359/2008). 5. S.18 of the Road Traffic Act 1968 and related regulations S.18 RT Act 1968 .
iii. Department of Enterprise, Trade, and Employment	The Department of Enterprise, Trade and Employment (DETE) leads in advising and implementing the Government's policies of stimulating the productive capacity of the economy and creating an environment which enables employment creation and sustainability. The Department is also charged with promoting fair competition in the marketplace, protecting consumers and safeguarding workers. The DETE Survey Unit collects data on numbers employed in enterprise agency clients (i.e. clients of Enterprise Ireland, IDA Ireland, Údarás na Gaeltachta) through its Annual Employment Survey. The Annual Employment Survey covers approximately 6,000 firms. DETE Survey Unit also collects data on sales, exports, value added, R&D expenditure and other company data on approximately 3,500 enterprise agency clients that have 10 or more employed or are identified as being High Potential Start Ups by Enterprise Ireland.	1. Further processing of the data is covered by Section 38.1.a of the Data Protection Act 2018. 2. Ministers and Secretaries Act, 1924. (as amended).

	The functions of the Department of Enterprise, Trade and Employment fall under the Ministers and Secretaries Act, 1924 to 2020 (as amended).	
iv. Department of Agriculture, Food and the Marine	The mission of the Department of Agriculture, Food and the Marine is to serve the government and people of Ireland by leading, developing and regulating the agri-food sector, protecting public health and optimising social, economic and environmental benefits. The Department is tasked with the delivery of the Common Agricultural Policy (CAP) in the Irish context and is the national accredited paying agency for EU CAP related funds. The Common Agricultural Policy (CAP) protects family farm incomes, supports the rural economy, ensures the production of high-quality safe food for consumers and protects rural landscapes and the environment. A paying agency is the dedicated department or body of an EU country responsible for the management and control of expenditure from the two funds of the common agricultural policy (CAP) – the European agricultural guarantee fund (EAGF) and the European agricultural fund for rural development (EAFRD). For each support scheme financed by CAP, paying agencies undertake a rigorous system of checks before payments are made including cross-checks with other databases, where considered appropriate. The department's function as per statutory basis under the Ministers and Secretaries Act 1924 is as follows: The administration and business generally of public services in connection with agriculture and lands,	1. Agriculture, Food and the Marine (Delegation of Ministerial Functions) Order 2021 (S.I. No. 40 of 2021). 2. Ministers and Secretaries Act 1924 (Commencement) Order 1924 (S.R.O. No. 804 of 1924). Signed on 30 May 1924. 3. The Irish Land Commission (Re-Distribution of Public Services) Order 1927 (S.R.O. No. 55 of 1927). 4. Ministers and Secretaries (Amendment) Act 1928 (Commencement) Order 1928 (S.R.O. No. 49 of 1928). 5. Forestry (Re-Distribution of Public Services) Order 1933 (S.R.O. No. 158 of 1933). 6. Fisheries (Re-Distribution of Public Services) Order 1934 (S.R.O. No. 40 of 1934). 7. Fisheries (Transfer of Departmental Administration and Ministerial Functions) Order 1957 (S.I. No. 67 of 1957). 8. Fisheries (Transfer of Departmental Administration and Ministerial Functions) Order

	including the fixing of rents and tenure of lands, acquisition by occupying tenants of full ownership by means of public funds, enlargement and other economic improvement of holdings of land, purchase of land for distribution by way of re-sale, relief of rural congestion and like uneconomic conditions, promotion of agriculture by means of educational grants, and of lectures on special subjects, agricultural statistics, forestry, veterinary services, survey and mapping of land, and all powers, duties and functions connected with the same, and shall include in particular the business, powers, duties and functions of the branches and officers of the public services specified in the Fifth Part of the Schedule to this Act, and of which Department the head shall be, and shall be styled, an t-Aire Tailte agus Talmhaíochta or (the Minister for Lands and Agriculture.	1965 (S.I. No. 83 of 1965). 9. Agriculture (Alteration of Name of Department and Title of Minister) Order 1965 (S.I. No. 146 of 1965). 10. Lands (Transfer of Departmental Administration and Ministerial Functions) Order 1977 (S.I. No. 28 of 1977). 11. Fisheries (Transfer of Departmental Administration and Ministerial Functions) Order 1977 (S.I. No. 30 of 1977). 12. Fisheries (Transfer of Departmental Administration and Ministerial Functions) Order 1977 (S.I. No. 31 of 1977). 13. Agriculture (Alteration of Name of Department and Title of Minister) Order 1987 (S.I. No. 97 of 1987). 14. Food Standards (Transfer of Departmental Administration and Ministerial Functions) Order 1987 (S.I. No. 129 of 1987). 15. Energy (Transfer of Departmental Administration and Ministerial Functions) Order 1993 (S.I. No. 10 of 1993). 16. Agriculture and Food (Alteration of name of Department and Title of Minister) Order 1993 (S.I. No. 11 of 1993).

		17. Forestry (Transfer of Departmental Administration and Ministerial Functions) Order 1997 (S.I. No. 300 of 1997). 18. Agriculture, Food and Forestry (Alteration of Name of Department and Title of Minister) Order 1997 (S.I. No. 302 of 1997). 19. Agriculture and Food (Alteration of Name of Department and Title of Minister) Order 1999 (S.I. No. 307 of 1999). 20. Rural Development (Transfer of Departmental Administration and Ministerial Functions) Order 2002 (S.I. No. 296 of 2002). 21. Horse and Greyhound Racing (Transfer of Departmental Administration and Ministerial Functions) Order 2002 (S.I. No. 297 of 2002). 22. Agriculture, Food and Rural Development (Alteration of Name of Department and Title of Minister) Order 2002 (S.I. No. 306 of 2002). 23. Sea Fisheries, Foreshore and Dumping at Sea (Transfer of Departmental Administration and Ministerial Functions) Order 2007 (S.I. No. 707 of 2007).

		24. Agriculture and Food (Alteration of Name of Department and Title of Minister) Order 2007 (S.I. No. 705 of 2007). 25. Horse and Greyhound Racing (Transfer of Departmental Administration and Ministerial Functions) Order 2010 (S.I. No. 179 of 2010). 26. Marine Tourism (Transfer of Departmental Administration and Ministerial Functions) Order 2011 (S.I. No. 163 of 2011). 27. Agriculture, Fisheries and Food (Alteration of Name of Department and Title of Minister) Order 2011 (S.I. No. 455 of 2011). and any further amendments.
v. Tailte Éireann	The core business of Tailte Éireann – Valuation is to provide our stakeholders with accurate, up-to-date valuations of commercial and industrial properties. These valuations are integral to the business rating system in Ireland, and form the basis for a very significant element of local government revenue each year. We also provide a valuation service to Government Departments and Offices, State agencies and other public bodies. We carry out open market capital and rental valuations including valuations for rent reviews for these customers. Open market valuations are provided for properties being transferred between Government Departments, State bodies and other public	1. The functions of the Valuation Office are principally set out in the Valuation Act 2001, as amended. A number of Statutory Instruments are also in place. 2. A "working consolidation" of the Valuation Act 2001 and subsequent amendments (up to 12th August 2020) is available here. It is provided by the Commissioner of Valuation as an aid to customers and other stakeholders of the Valuation Office and does not purport to constitute a definitive consolidated text of

	authorities and agencies across the country.	the legislation. Use of this document is subject to the disclaimer therein. 3. Reference Section 19 (4) 4. Reference 71. (1) Notwithstanding any enactment or rule of law— 5. (a) relevant person shall, upon a request from the Commissioner, provide the Commissioner with such information in the possession or control of the relevant person as the Commissioner may reasonably require for the purpose of enabling the Commissioner to perform his or her functions under this Act, and 6. (b) the Commissioner shall provide a rating authority with such information in the possession or control of the Commissioner, pursuant to this Act, as that rating authority may reasonably require for the purpose of enabling it to perform its functions by or under any enactment. (2) In this section— “relevant person” means any of the following: a rating authority. the Commissioners of Public Works in Ireland. the Registrar of Companies. the Property Registration Authority. the Property Services Regulatory Authority. the Office of

		the Revenue Commissioners. (g) any other person for the time being prescribed.
vi. DPENDR	The Office of the Chief Government Chief Information (OGCIO) is a division with the Department of Public Expenditure, NDP Delivery and Reform that leads on the digital transformation agenda across Government while providing and developing pan-public service ICT infrastructure, service delivery models and cross government applications. In addition, it provides IT services to the Department which include provisioning IT systems to support the management to EU Funds including the Common Provision Regulations, the Recovery and Resilience Facility and the Brexit Adjustment Reserve. The OGCIO has configured a number of project types that manage the complex workflows that support certain EU funds including CPR, RRF and BAR on the Department's Enterprise Project and Portfolio Management Solution (EPPM). The ERDF and RRF project types capture corporate beneficiary information as part of the workflow and information related to the beneficial owners. These corporate beneficiaries are registered businesses. The use of UBIN will provide the Department with a means to capture one instance of a particular corporate beneficiary and validate that information it holds on these entities is correct and where errors are found update its information. In addition, the European Commission requires detail on all corporate beneficiaries to minimise or eliminate potential fraud, corruption and or conflicts of interest related to the drawdown of monies by business across multiple funds.	1. Art. 22 of REGULATION (EU) 2021/241 – Recovery and Resilience Facility (RRF) 2. REGULATION (EU) 2021/1060 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – Common Provisions Regulations (CPR) 3. REGULATION (EU) 2021/1755 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – Brexit Adjustment Reserve (BAR) 4. Ministers and Secretaries (Amendment) Act, 2011.

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 compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (c))

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))

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
Data Sharing and Governance Act 2019 - S13 2) a) i) I, II, III, IV, V, VI, VII, VIII	(i) to verify the identity of a person, where the first or second mentioned public body is providing or proposes to provide a service to that person. (ii) to identify and correct erroneous information held by the first or second mentioned public body. (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 the first or second mentioned public body were the second mentioned public body to collect the personal data directly from that person. (iv) to establish the entitlement of a person to the provision of a service being delivered by the first or second mentioned public body, on the basis of information previously provided by that person to the first mentioned public body (or another public body that previously disclosed the information to the first mentioned public body). (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 the first or second mentioned public body. (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 the first or second mentioned public body. (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 the first or second mentioned public body. (viii) to facilitate an analysis of the structure, functions, resources and service delivery methods of the first or second mentioned public body.

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:

LEGISLATION	DESCRIPTION
RSA	• S.4 of the Road Safety Authority Act, 2006 as amended, and related Conferral of Functions Order 2006; • S.37 of the Commercial Vehicle Roadworthiness Act 2012 and related regulations; • Regulation 6 of the European Union (Road Transport) (Working Conditions and Road Safety) Regulations 2017 (SI 229 of 2017); • European Communities (Vehicle Drivers Certificate of Professional Competence((No.2) Regulations 2008; • S.18 of the Road Traffic Act 1968 and related regulations. • S.30 of the Statistics Act 1993.
DPENDR	• Section 38 (1)(a) of the Data Protection Act 2018 • EU Regulation 1303/2013; • Articles 13, 14, 16, 19, 37 as well as Section 7 of EU Regulation 1828/2006; • Chapter 2.2.3 of the Commission's Communication on the Anti-Fraud Strategy of 22 June 2011; • Regulation 1046/2018 in the light of Articles 325 and 317 of the Treaty on the functioning of the European Union (TFEU).
DAFM	• Data is processed in accordance with EU Regulations 2021/2115, 2021/2116. • Section 38(1)(a) and (b) of the Data Protection Act 2018 • Ministers and Secretaries Act, 1924. (as amended)
Tailte Éireann	• Section 38 (1)(a) of the Data Protection Act 2018 • Valuation Acts 2001 to 2020 Sections 71. (1), (2)
DETE	• Further processing of the data is covered by Section 38.1.a of the Data Protection Act 2018. • Ministers and Secretaries Act, 1924. (as amended).

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	☐
ii. Public Body	☒

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	☐	
Classes of Data Subjects	☒	Data subjects consisting of business undertakings that are either individuals or businesses that have provided tax information to Revenue (and registration information to the CRO) and could benefit from the specified purposes outlined above i.e., reduced administrative burden, ease of service delivery, administration of a service, programme, or policy, targeting of a service, programme or policy and improvement to service programmes or policies provided by public service bodies.

Table 7.0

8. Duration and Frequency

8.1 Duration

Define the start and end dates of the information transfer:

i. The Data Sharing Agreement will commence on **30 September 2024** and continue until the parties agree to terminate agreement.

8.2 Frequency

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

TYPE		DESCRIPTION
Once off	☐	
Frequent/regular updates	☒	The UBIN webservice provides real-time access to a continuously updated database of business information maintained by The Office of the Revenue Commissioners.
Other frequency	☐	

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.

All 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.

Road Safety Authority	RSA will process the UBIN data for the purposes highlighted in section 2.2 and described in 2.3 of this DSA. Once a business has an online business account with the RSA this will reduce/eliminate the need for the RSA to collect the same information from the same businesses when they are availing of different RSA Services as all RSA services will ultimately be made available via the single business portal. The RSA will use the NACE code data element (which is part of the UBIN dataset) to help determine the business activity of a particular business and so thereby ensure the relevant and related RSA services for that business activity are made accessible to them online. Where the relevant consent is obtained via the online business account, the RSA can use the UBIN data to facilitate the targeting of a programme or policy by for example providing customised and relevant road safety messaging of interest to specific business groupings. The data will be stored in a secured database and the data will only be accessible to those authorised by the data owner to access this data in the delivery of the relevant RSA service. Information gathered from customers is shared with other Business Areas within the RSA for the purposes of facilitating the administration and delivery of RSA services to the relevant business. Only aggregated results will be shared with a third party so that individuals will not be identified. Where aggregated results are presented this will be done in line with the CSO Guidance on statistical disclosure control (SDC) measures to ensure there is no unintentional disclosure of any personal information. The RSA may use the data to carry out research to enable the evaluation or review of an RSA service, programme, or policy. The RSA is obliged by law to provide data on request to the Central Statistics Office under Section 30 of the Statistics Act 1993 and to An Garda Síochána and other bodies in accordance with current data protection legislation.
Department of Enterprise, Trade and Employment	DETE will process the UBIN for the purposes highlighted in section 2.2 and described in 2.3 of this DSA. The data will be stored in a database(s) in a secure location within the EU/EEA in compliance with the GPDR and Data Protection Act 2018 and will only be accessible to those authorised to access the information. Data will not be shared outside of the authorised group of users.

Department of Agriculture, Food and the Marine	DAFM will process the UBIN data for the purposes highlighted in section 2.2 and described in 2.3 of this DSA. Access to UBIN will allow us to record the UBI for our business customers and improve the quality of business identifiers in our database as it will be used for the following purposes: • The UBIN will reduce/eliminate the need for DAFM to collect the same information from the same businesses and it will help to ensure valid and complete records for businesses. • The UBIN will give us an accurate Business Name & address that we can cross-reference and validate with any previous collected details. • The UBIN will allow DAFM to cross validate the accuracy of our Eircode and improve the quality of our Eircode records. • The UBIN will allow us to validate or complete CRO and VAT records for customers in our database. • DAFM will use the NACE code data to help determine the declared business activity of customers. The NACE code will be used to improve and validate our customer categorisation and description. The data will be stored in a database and in a secure location and will only be accessible to those working in DAFM. Only aggregated results will be shared with any third party so that individuals will not be identified. Information gathered from customers is shared with other Business Areas within the Department for the purposes of facilitating and processing payments or collecting charges in a timely and efficient manner. DAFM is also obliged by law to provide data on request to the Central Statistics Office under Section 30 of the Statistics Act 1993, to the Department of Employment Affairs and Social Protection (DEASP) under Section 262 of the Social Welfare Consolidation Act 2005 (as amended), to the Revenue Commissioners under the Taxes Consolidation Act 1997 and S.I. 273 of 2011 Returns of Payments (Government Departments and Other Bodies) Regulations 2011, to An Garda Síochána and other bodies and will only do so where a legal basis is established, in accordance with current data protection legislation.
Tailte Éireann	Tailte Éireann – Valuation will process the UBIN for the purposes highlighted in section 2.2 and described in 2.3 of this DSA. The UBIN will give us an up-to-date Business Name that we can cross-reference with our Occupier details. The UBIN will be an excellent resource to cross validate the accuracy of our Eircode matching project. It will allow us to spot errors in our Eircode matching project and improve the quality of our Eircode accuracy. The UBIN will allow us to link properties from the UBIN to our Commercial database using the Eircode. This in turn will allow us automatically fill in any blank CRO columns in our database. The UBIN will allows us to improve the accuracy and quality of our Address columns by cross-referencing against the UBIN address columns using the Eircode column as the link. All the cross-validation processing will be automated using in house technologies.

Department of Public Expenditure NDP Delivery and Reform	DPENDR will process the UBIN for the purposes highlighted in section 2.2 and described in 2.3 of this DSA. The data will be stored in a database(s) in a secure location within the EU/EEA in compliance with the GPDR and Data Protection Act 2018 and will only be accessible to those authorised to access the information. Data will not be shared outside of the authorised group of users.

Table 9.2

9.3 Further Processing

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

	SPECIFY FURTHER PROCESSING
All parties	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
All parties	Any sharing of the UBIN data with any third party other than the parties named in this agreement is restricted without the express permission of the Office of the Revenue Commissioners. Unless a clear legal basis has been established to allow the release of this data in accordance with the GDPR and data protection legislation in force at the time.

Table 10.0

11. Security Measures

11.1 Security and Training

All 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.

All 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. Please provide details.	☒	☐
		Web connection is via HTTPS, which is encrypted by default. This is standard for Revenue's external facing webservices.	

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.
The UBIN webservice is secured via ROS digital certificates. These certificates are produced and managed by Revenue and only certificates explicitly created for the UBIN service will have the ability to access any and all endpoints and data. Certificates will be sent to PSB's requiring UBIN access on an individual basis,

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.

11.2.2.1 DAFM

11.2.2.1	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
			Access to data is restricted by roles and authorisations at an application data level. Further access is limited by user/password restrictions.	
11.2.2.1.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		DAFM has a secure suite of systems behind Private VPN's and Citrix Desktop software to ensure the proper controls are in place for data remotely accessed by users.		
11.2.2.1.3	**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.** Please provide details.	☒	☐	☐
		Privileged access is practised here in DAFM with least amount of access given to the user based on the roles and authorisations given.		
11.2.2.1.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed.	☒	☐	☐
		All customer and client data is held on centralised databases instances running on hardware located in DAFM's on premises Data Centre. All removable data ports (USB etc) have written privileges disabled.		

11.2.2.1.5	**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.	☐	☐	☒
			The data will not be stored on mobile devices such as laptops and removable media.	
11.2.2.1.6	**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.	☒	☐	☐
			DAFM provides sound training for all staff in data awareness and complies with the various ISO procedures in this area.	
11.2.2.1.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.		DAFM has invested significantly in restore and recovery capabilities for all its enterprise level data which also includes Disaster Recovery and Business Continuity procedures. All office documents stored on DAFM's shared drives are also subject to rigorous backup policies.	
11.2.2.1.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.		Yes, all DAFM data is securely stored in its on-premise Data Centre and is archived according to internal data retention policies.	

Table 11.2.3

11.2.2.1.9 – 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.
The data from the files provided to DAFM will be (/is) imported into a server which is in a locked-down environment with restricted access to relevant personnel only. DAFM's information security management system is ISO27001 certified, including the Data Centre housing the server environment. Within the server, the data is accessible only for the authorised purpose. The server is securely backed up in accordance with DAFM's IT backup policy.

11.2.2.1.10 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

11.2.2.2 Department of Enterprise, Trade and Employment

11.2.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.2.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
11.2.2.2.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		Systems are in place to provide secure remote access to DETE staff to the corporate network. DETE uses two remote access methods – both of which are industry leading technologies, details of which we can provide to the lead agency but will not name here for purposes of our own security. One is primarily used by non-staff to provide secure remote access using non-DETE-owned devices with all activity taking place within remote desktop type services. This system is configured to prevent file sharing between the remote client and DETE server session. Access to this system must approved and authorised by DETE ICT initially and MFA is required at each logon. Staff instead use an industry leading VPN, from domain-joined and managed laptops that are hard-disk encrypted with TPM chip protection. This remote access channel is IPsec encrypted and all traffic is routed through the corporate network and controls with no ability to bypass or disable the VPN and is only available on DETE owned and on-prem domain joined devices. Bring your own device scenarios are not supported.		
11.2.2.2.3	**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.** Please provide details.	☒	☐	☐
		Access rights are based on a staff member's role, their need to access systems and the level of access required. All accounts are subject to least privilege principles.		

11.2.2.2.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed.	☒	☐	☐
		The ability to write to removable media is not generally provided, and where available it is strictly controlled and audited. Those staff granted the ability to use removable media may read from any media but may only write to media that has been encrypted by us using an industry leading encryption platform.		
11.2.2.2.5	**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.	☒	☐	☐
11.2.2.2.6	**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.	☒	☐	☐
		DETE provides training and has several policies covering records management and Information Security.		
11.2.2.2.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	DETE has an enterprise backup solution in place covering file shares and databases. Additionally, core systems and datasets are within scope of the Department's Business Continuity and Disaster Recovery Plans. Since local storage on PCs / Laptops is not backed up and is therefore volatile users are instructed by policy not to store critical information or sensitive information in places such as the local desktop etc.		
11.2.2.2.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Yes, all DETE data is securely stored and is deleted according to internal data retention policies.		

Table 11.2.3

11.2.2.2.9 – 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.
Access to data and resources are managed on the Principle of Least Privilege with access auditing in place. Remote access to departmental IT resources is governed by technological controls and policies. All laptops are encrypted, and access to portable media is restricted and audited. The Department has deployed a range of Information Security tools, including systems for logging and monitoring. A comprehensive suite of Information Security policies and standards are in place, these outline the controls in place and the acceptable usage of the IT resources. These policies include Acceptable Usage, User Access, Remote Access, Incident Management and Threat and Vulnerability Management. Policies are subject to review on a regular basis. Regular Information Security awareness and advice is provided to staff. The Department has several resilience measures in place including, taking routine backups, and testing these, Business Continuity and Disaster Recovery Plans along with Incident Response Plans. The Department also has access to independent security advice and a third party undertakes security assessments and penetration testing as required.

11.2.2.2.10 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

11.2.2.3 Road Safety Authority

11.2.2.3	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.3.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
			RSA operates a password management policy and has identity and access management procedures in place. Employees are informed and regularly reminded by the RSA DPO of their responsibilities under Data Protection Law. Note: [May 2023] -The RSA Online Business Portal which will interface with the UBIN API is part of the overall RSA Digitalisation Strategy, which is not yet in place. Access controls for the RSA Online Business Portal and supporting back-end systems will be set out and will adhere to the RSA – Access Control Policy which covers approval for all RSA system access. Access controls and permissions will be reviewed regularly and updated as required.	
11.2.2.3.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		RSA has a secure remote access system in place to access RSA's network which requires multi factor authentication]		
11.2.2.3.3	**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.** Please provide details.	☒	☐	☐
		The RSA has an Access Control Policy in place which sets out the approval process in relation to all RSA system access requests. This process includes a request being logged with the RSA ICT Helpdesk Team and requires inclusion of evidence to support the authoriser's confirmation that the access is required to allow the employee carry out their job function.		

		Note: [May 2023] -The RSA Online Business Portal which will interface with the UBIN API is part of the overall RSA Digitalisation Strategy and is not yet in place. Access controls for the RSA Online Business Portal and supporting back-end systems will be set out and will adhere to the RSA – Access Control Policy. Under the RSA Online Business Portal project will be the specific inclusion of the following access control measures: • Definition of User Roles and Groups to enable the limiting of access to Personal Data to only those users who require access for a specified and legitimate purpose in the delivery of RSA services. • A process which ensures that access controls and permissions are reviewed regularly and updated as required.		
11.2.2.3.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed.	☒	☐	☐
		RSA have implemented a cybersecurity policy. It is not considered appropriate to disclose information on the cyber activities and the resourcing of same for both security and operational reasons.		
11.2.2.3.5	**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.	☒	☐	☐
			All RSA laptops, and any internal hard drives, are encrypted by the RSA ICT Helpdesk Team prior to issue. All provided mobile devices that host RSA data are protected by encryption and layered authentication where appropriate. Implementation of Mobile Device Management (MDM) is applied to all mobile devices.	
11.2.2.3.6	**There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate**	☒	☐	☐
		Appropriate security measures and policies are in place and regularly reviewed. RSA operates an Acceptable Usage Policy which users of the network and RSA IT assets must agree to. Employees are informed by the RSA DPO of their responsibilities under Data Protection Law and trained regularly.		

	manner or to an inappropriate, less secure location. Please provide details.	ICT Security and GDPR training campaigns are run regularly and cover a range of IT Security topics.
11.2.2.3.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	Disaster recovery and backup routines are maintained and the scope of this will be expanded to ensure the availability and ability to restore the Data under this agreement as part of the design and implementation of the RSA Online Business Portal and supporting back-end systems.
11.2.2.3.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Data will be stored in a secure location as part of the overall RSA Business Customer Profile entity. Data records within this entity will be securely erased in line with the RSA business Data Retention procedure which is set for the minimum amount of time having regard to any organisational legal requirements or specific RSA business requirements.

Table 11.2.3

11.2.2.3.9 – 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.
The RSA has an ICT Security Policy in place and the scope of this policy covers all Information Systems spanning infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store information owned by the RSA. The objective of the security policy is to set out the security controls implemented to safeguard RSA Information Systems that process RSA information and ensure the security, confidentiality, integrity and availability of the information held therein. The policy covers areas including: • User Access, • System Security Architecture • Vulnerability Management • Application Security • Data Security • Incident Management The Policy is owned by the Director of Technology Platforms & Solutions and approved by the RSA Senior Leadership Team and is subject to formal review.

11.2.2.3.10 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 11.2.2.3

11.2.2.4 Tailte Éireann

11.2.2.4	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.4.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
			User access to network and application data is controlled on the Principle of Least Privilege (PoLP) supported by Active Directory Group Policy and password management software. We employ an IAM solution for all data within our cloud infrastructure and this reviewed regularly.	
11.2.2.4.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		We use VPN software to control how our users access data remotely.		
11.2.2.4.3	**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.** Please provide details.	☒	☐	☐
		Principle of least privilege is applied to the operating environment that will be accessing the data.		
11.2.2.4.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed.	☒	☐	☐
		At a local level we have a removable media lock down policy. At a database and Amazon Web Services (AWS) level we have a cloud guard application by check point which incorporated Data Leaks Protection (DLP).		
11.2.2.4.5	**Data is encrypted at rest on mobile devices such as laptops and removable media.**	☒	☐	☐
			All data is encrypted via Advanced Encryption Standard (AES). Microsoft Intune Mobile Device	

	Please provide details for all non-complying or 'not applicable' statements.		Management (MDM) manages all mobile devices. BitLocker protects all laptops and mobile.	
11.2.2.4.6	**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.	☒	☐	☐
		Department security policy, remote access policy, mobile device policy and acceptable usage policy, in particular, provides direction on file and data storage policies. All policies are reviewed annually and are the primary content of our security education and awareness program that runs continually for all staff during the calendar year.		
11.2.2.4.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	Our Enterprise Data Warehouse (EDW) is part of the AWS infrastructure that incorporates disaster recovery. We have an onsite recovery that allows us to recover lost data up to 30 days.		
11.2.2.4.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	It is stored in our secure environment in our AWS and on internal machines. Data minimisation is applied, and data retention policies are in line with best practices.		

Table 11.2.3

11.2.2.4.9 – 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 data supplied and managed under this agreement is stored in Tailte Éireann – Valuation cloud infrastructure. All data is encrypted in transit and at rest to AES-256 standards. Additionally, our third-party support partners who manage our data warehouse and cloud infrastructure are ISO/IEC 27001 certified and provide full logging of all data access requests. Our cloud and on-premise network infrastructure systems are vulnerability assessed and penetration tested annually. All access to data/resources are managed on the Principle of Least Privilege and full auditing of data access is recorded per our security policies. Access tour on premise data is managed at a device level through our Intune MDM solution and supported by local security policies incorporating restricted access via USB keys/sticks and other Data Leak Prevention systems. All staff are obliged to read, acknowledge and comply with our ICT Security Policy Suite which includes Acceptable Usage, Remote Access and Mobile Device Access. All security policies are reviewed annually by our ICT Security Manager, owned by our Chief Information Officer and approved by our Senior Management Board as part of our Corporate Governance and Risk Management process. We have a continuous Security Education and Awareness Programme for all staff which supports our security posture.

11.2.2.4.10 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 11.2.2.4

11.2.2.5 DPENDR

11.2.2.5	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.5.1	**In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
11.2.2.5.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		DPENDR ensures the confidentiality and integrity of data at all stages in the data lifecycle which includes the provision of end-to-end effective data encryption for data at rest, in transit and in use. The application has been externally audited under ISO 27001:2013 as evidence of this control and ensures appropriate controls are in place when data s access remotely.		
11.2.2.5.3	**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.** Please provide details.	☒	☐	☐
		All access is based on the principle of least privilege. Access is provided to users based on their role and the assignment of appropriate security groups. Only authorised client admins can assign a user to the appropriate role and security groups.		
11.2.2.5.4	**Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).** Please provide details of the protections in place and how they are managed .	☒	☐	☐
		DPENDR's Build to Share Desktop service policy does not allow use of non-authorised removable media.		

11.2.2.5.5	**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.	☒	☐	☐
11.2.2.1.6	**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.	☒	☐	☐ DPENDR requires all those working within the Department to read and acknowledge the content of its ICT Acceptable Usage Policy, Internet Content Access Policy, the Official Secrets and Integrity Act, attend Cybersecurity training and review and comply with policies and documents in relation confidentiality and awareness.
11.2.2.5.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	DPENDR's Managed Desktop Service production infrastructure is designed to be highly available with multiple levels of redundancy. The databases that will hold the UBIN data for part of a SaaS based application that is ISO 27001 certified and provisioned from a Cloud Service Provider (CSP) platform that is itself ISO 27001 certified. Deletion of data can only be carried out by authorised personnel. All data is backed up.		
11.2.2.5.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	The databases that will hold the UBIN data are part of a SaaS based application that is ISO 27001 certified and provisioned from a Cloud Service Provider (CSP) platform that is itself ISO 27001 certified. Data will be securely erased from all devices (databases, backups etc.) following instruction by DPENDR authorised officers.		

Table 11.2.3

11.2.2.5.9 – 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.
ISO Certification The OGCIO's Management Desktop service is ISO 27001 certified, the application that will hold and manage access to the UBIN data is ISO 27001 certified as it the Cloud Service Provider. All users authenticated and provisioned on the application are subject to confidentiality agreements and their access approved by appropriate authorities. **Access Control** A record of security privileges of individuals having access to data is maintained and industry standard practices to identify and authenticate users who attempt to access information systems are maintained. In addition, technical support personnel are only permitted to have access to data when needed. Passwords are stored in a way that makes them unintelligible while they are in force. **Disaster Recovery, Resilience and Backup** Both on-site and off-site backups are included in the backup policy. Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances.

11.2.2.5.10 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

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	Revenue's policy for data retention is "current plus ten years" i.e., records are retained while current plus an additional ten years from when they become non-current.
1.1 DAFM	DAFM's policy for data retention is "current plus ten years" i.e., records are retained while current plus an additional period of 10 years unless there is a clear business requirement for retention. This timeline will be subject to ongoing review on annual basis.
1.2 DETE	Where we have updated our records using the UBIN dataset we will retain that data for "current plus ten years".
1.3 RSA	It is the RSA's policy to manage all records through creation, maintenance, protection, retention and disposal in accordance with the relevant regulatory guidance, applicable legal obligations and having regard for RSA's operational needs. Records are not permitted to be retained 'just in case' of some potential usefulness in the future. Once the personal data has served its purpose it is required to be destroyed as planned. The RSA Data Protection Officer (DPO) is the officer responsible for the administration of the RSA Record Retention Procedure and to ensure it is followed by RSA Business Areas. UBIN data will be stored in a secure location as part of the overall RSA Business Customer Profile entity. Data records within this entity will be securely erased in line with the RSA business Data Retention policy which will be set for the minimum amount of time having regard to any organisational legal requirements or specific RSA business requirements.
1.4 Tailte Éireann	Data will be retained for "current plus ten years".
1.5 DPENDR	The Data will be retained for current plus five years. The EU requires the retention of data for the period of the current funds (2021 – 2027) and a further 5 years following the final claim. It is expected that the final payment claim will be made before the end of 2029. Article 82 Availability of documents 1. Without prejudice to the rules governing State aid, the managing authority shall ensure that all supporting documents related to an operation supported by the Funds are kept at the appropriate level for a 5-year period from 31

	December of the year in which the last payment by the managing authority to the beneficiary is made. 2. The time period referred to in paragraph 1 shall be interrupted either in the case of legal proceedings or by a request of the Commission.
2. Information resulting from the processing of the data	Revenue's policy for data retention is "current plus ten years" i.e., records are retained while current plus an additional ten years from when they become non-current.
2.1 DAFM	DAFM's policy for data retention is "current plus ten years" i.e., records are retained while current plus an additional period of 10 years.
2.2 DETE	We will retain this data also for "current plus ten years".
2.3 RSA	It is the RSA's policy to manage all records through creation, maintenance, protection, retention, and disposal in accordance with the relevant regulatory guidance, applicable legal obligations and having regard for RSA's operational needs. Records are not permitted to be retained 'just in case' of some potential usefulness in the future. Once the personal data has served its purpose it is required to be destroyed as planned. The RSA Data Protection Officer (DPO) is the officer responsible for the administration of the RSA Record Retention Procedure and to ensure it is followed by RSA Business Areas. UBIN data will be stored in a secure location as part of the overall RSA Business Customer Profile entity. Data records within this entity will be securely erased in line with the RSA business Data Retention policy which will be set for the minimum amount of time having regard to any organisational legal requirements or specific RSA business requirements.
2.4 Tailte Éireann	Data will be retained for "current plus ten years".
2.5 DPENDR	The Data collected is for a specific purpose, outlined in this agreement and in line with DPENDR policies and EU Regulations the data will be deleted once it is no longer required and its deletion validated. UBIN data will be stored in a secure location with EU / EEA regions in ISO 27001 certified, hosting platform, application and accessed by devices in an ISO 27001 certified Managed Desktop service.

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	Revenue records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
1.1 DAFM	Records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
1.2 DETE	Records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
1.3 RSA	In line with the RSA Record Management procedures, at least on a bi-annual basis, the RSA Business Data Owner will identify any Business Customer Profile entity records that require deletion having regard for omitting any records where there may be an exceptional reason not to delete/ dispose (e.g., there is threatened/actual legal proceedings and/or there is open complaint). The RSA Business Data Owner prepares a listing/ audit log of Business Customer Profile entity records for deletion and submits them through the relevant agreed operational ICT process for execution. The relevant RSA ICT System Support team will delete the identified records and confirm to RSA Business Data Owner that this has been done.
1.4 Tailte Éireann	TÉ records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
1.5 DPENDR	Records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended). At the end of the retention period, personal data stored in any format will be formally validated and permanently deleted.
2. Information resulting from processing of the data	Revenue records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
2.1 DAFM	Records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
2.2 DETE	Records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
2.3 RSA	In line with the RSA Record Management procedures, at least on a bi-annual basis, the RSA Business Data Owner will identify any Business Customer Profile entity records that require deletion having regard for omitting any records where

	there may be an exceptional reason not to delete/ dispose (e.g., there is threatened/actual legal proceedings and/or there is open complaint). The RSA Business Data Owner prepares a listing/ audit log of Business Customer Profile entity records for deletion and submits them through the relevant agreed operational ICT process for execution. The relevant RSA ICT System Support team will delete the identified records and confirm to RSA Business Data Owner that this has been done.
2.4 Tailte Éireann	TÉ records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).
2.5 DPENDR	The records will be destroyed at the end of the retention period in accordance with Section 7 of the National Archives Act (as amended).

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 OGCIO. 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.

15.7 Additional Information

To exercise your rights under data protection legislation, Data Protection Units of the PSB's noted in this document can be contacted at:

Revenue
Address: Data Protection Unit, Ground Floor, Cross Block, Dublin Castle, Dublin 2. D02 F342
Email: dataprotection@Revenue.ie

DAFM
Address: Data Protection Unit, Department of Agriculture, Food and the Marine, Pavilion A Grattan Business Park, Dublin Road, Portlaoise, Co Laois R32 K857.
Email: dataprotectionofficer@agriculture.gov.ie

DETE
Address: Data Protection Unit, Department of Enterprise, Trade and Employment, 23 Kildare Street, Dublin 2, D02 TD30.
Email: dataprotection@enterprise.gov.ie

RSA
Address: Data Protection Unit, Road Safety Authority, Moy Valley Business Park, Primrose Hill, Ballina, Co. Mayo F26 V6E4.
Email: DataProtection@rsa.ie

TE
Address: Data Protection Unit, Tailte Éireann, Chancery Street, Dublin 7 D07 T652.
Email: dataprotection@tailte.ie

DPENDR
Address: Data Protection Unit, Department of Public Expenditure, NDP Delivery and Reform, Government Buildings, Upper Merrion Street, Dublin 2, D02 R583.
Email: dataprotection@per.gov.ie

Note: To allow identification of records further information may be sought before this right can be fully considered and processed.

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		SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT
Has been conducted	☒	In line with the Data Sharing and Governance Act 2019, Revenue will make available to other Public Sector Bodies (PSBs) a dataset of Irish businesses containing a newly created Unique Business Identifier Number (UBIN) and certain other identifying information. All taxpayers on Revenue systems with: 1) a live CRO number, or 2) a live VAT number. will be included in the dataset. This will therefore include all companies, and any sole traders or other entities registered for VAT - noting that there is already a publicly available system to verify a VAT number at the following link: *https://ec.europa.eu/taxation_customs/vies/#/vat-validation* The following fields will be included in the dataset: a) Unique Business Identifier Number, b) Business name c) Business address d) Eircode (where available), e) NACE code, f) NACE description, g) VAT registration number, h) CRO registration number, and i) PREM number (where applicable). Taxpayers that hold a PREM registration only and no CRO/VAT registration are excluded from the UBIN. This is to limit the inclusion of small traders whose business may be based out of their residence. However, where a taxpayer holds a PREM registration in addition to a CRO/VAT registration then the PREM number will be included as part of the dataset and may be searched or returned as part of a query. The dataset will be held securely on a Revenue server, and a machine-to-machine application made available to support queries as follows: (i) Approved PSBs may submit a UBIN, VAT, PREM, CRO or Eircode and will receive in return the information in the dataset that relates to that criterion; or

		(ii) Approved PSBs may submit information for two or more of the nine fields above and receive a message indicating whether an entity exists on the UBI dataset. Access by PSBs will be subject to legislation and governance.
Has not been conducted	☐	

Table 9.0

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.

RSA

The RSA mission is to make Irish roads safer for everyone. The functions for which the RSA is responsible for include driver testing and training, driver licensing, vehicle testing, road safety promotion and road safety research.

As many businesses engage with the RSA and avail of many or all of these services the RSA is required to maintain records of these businesses.

In areas such as Commercial Vehicle Roadworthiness Testing (CVRT), professional driver training, tachograph card services and the delivery of driving tests in bus and truck categories in particular, businesses can often be the primary customer as regards these RSA services.

In line with the Government strategy on digitalisation of public services the RSA are consolidating its online services onto one platform and this includes the services availed of by business customers.

The RSA require the UBIN data for the eight purposes set out in Table 2.2 to:

1. Verify the identity of a business so as to facilitate the creation of an RSA online business registration account and enable that company avail of an RSA online service.
2. Correct erroneous information which the RSA may hold in relation to a business entity engaging with the RSA.
3. Create a single RSA online business registration account thereby reducing/removing the need for the RSA to collect the same information from the same businesses when they are availing of various RSA Services.
4. Assist in establishing the entitlement of a business to the provision of an RSA Service. For example, in determining whether a Transport Operator is involved in the provision of freight or passenger transportation can be obtained via the NACE code element of the UBIN and so assist in providing of RSA related services to Bus Operators.
5. Facilitate the administration, supervision and control of RSA services to businesses by using it as part of the process to create an RSA online business registration account.
6. Facilitate the targeting of an existing service, programme or policy and enhance decision making around proposed decisions or policies in relation to road safety. For example, the UBIN data combined with relevant consent would assist RSA in being able to provide customised and relevant road safety messaging of interest to specific business groupings.
7. Aid in road safety related policy evaluation and oversight as it will also mean our datasets relating to businesses can be enriched and offer further potential for approved research cases led internally in RSA or via agencies such as the CSO.
8. Facilitate analysis of the RSA business functions/resources and RSA service delivery methods. For example, RSA online service delivery to businesses.

The personal data disclosed to RSA as part this data sharing agreement has been assessed and is considered necessary and proportionate in the context of carrying the RSA statutory functions and to allow the RSA to align to the broader government public service data strategy.

DETE

The Department of Enterprise, Trade and Employment leads in advising and implementing the Government's policies of stimulating the productive capacity of the economy and creating an environment which enables employment creation and sustainability. The Department is also charged with promoting fair competition in the marketplace, protecting consumers and safeguarding workers. The analysis, linking and validation of data sets is central to the delivery of these functions.

DETE require the UBIN data for the eight purposes set out in Table 2.2 to:

1. DETE will use the data for the purposes of verification of the identity of a business and may use the data to verify the identity of a business or a person. This verification process is required for the purposes of producing national statistical publications to inform policy formulation and for research and analysis purposes. The data sets are not published in raw format and will remain unpublished in this format.
2. The data will be accessed by DETE for the purposes of verification of the identity of a business and may be used to identify and correct erroneous information held by DETE. This verification and correction of erroneous data will be used to enhance policy formulation and programme/project formulation by the DETE. The accuracy of these data sets will also enhance the targeting of enterprise support programmes and be used to inform future policy programme-specific funding aimed at maximising productive capacity, employment creation and sustainability which are part of the core functions of the DETE.
3. DETE will use the UBIN data to reduce or avoid the administrative burden of re-collecting identifying information about our business customers to whom we are delivering a service or a scheme. This will assist the DETE in meeting the cross-government objectives set out in the *Public Service Data Strategy*.
4. DETE will use the UBIN data or information previously provided to establish the entitlement of a person to the provision of DETE schemes and services where DAFM is part of the scheme or service being delivered with the DETE. The data will be used to ensure value for money for Exchequer funding and to reduce the risk of incidences of fraud. The data sets will also be used to inform the effectiveness of targeted schemes and services and inform future policy formulation.
5. DETE propose to use the UBIN to facilitate the administration, supervision and control of DETE services / schemes to businesses and in the broader development of policy deliverables. The data sets will be used for analysis in the DETE of the effective administration, supervision and control of targeted and sector-specific services and schemes to business and inform future policy formulation aimed at achieving the DETE's mandate.
6. DETE intend to utilise the UBIN to facilitate and enhance the delivery of schemes and services whilst providing data to enhance policy making decisions. The availability of up-to date and accurate data sets is essential in assisting the DETE to more effectively analyse the efficacy of targeted funding and enhancing the design and delivery of schemes and services to meet its mission while also providing value for money for the Exchequer.
7. DETE purport to use UBIN data for the evaluation and review of schemes/services and programmes. This will facilitate the development of future programmes/services and policy implementation. The data sets will be used to evaluate and review both existing and future schemes, programmes and services to provide greater insight into the effectiveness of such initiatives and provide qualitative analysis to inform the future formulation of such initiatives. For example, the Ukraine Credit Guarantee Scheme, the Growth and Sustainability Loan Scheme, the Tailored Company Expansion Package.
8. DETE intend to apply the UBIN to support the analysis of its business functions and programmes which is reliant on up-to-date and valid data. Real-time, accurate data sets are essential in assisting the DETE to enhance its quantitative and qualitative analysis of the effectiveness of the delivery of its business functions and ensuring that targeted funding initiatives are meeting enterprise needs to generate sustainable employment creation and sustainability.

The personal data received within UBIN data transfer has been assessed to be necessary to assist the DETE in meeting its statutory functions and aligns to the broader government objectives contained within the Public Service Data Strategy.

DAFM

The personal data received within the UBIN data transfer has been assessed to be necessary to assist DAFM in meeting its statutory functions and aligns to the broader government objectives contained within the Public Service Data Strategy.

DAFM require the UBIN data for the eight purposes set out in Table 2.3 to:

1. DAFM will use the data for the purposes of verification of the identity of a business and may be used to verify the identity of a business or a person.
2. The data will be accessed by DAFM for the purposes of verification of the identity of a business and may be used to identify and correct erroneous information held by DAFM.
3. DAFM will use the UBIN data to reduce or avoid the administrative burden of collecting identifying information about our business customers to whom we are delivering a service or a scheme.
4. DAFM will use the UBIN data or information previously provided to establish the entitlement of a person to the provision of DAFM schemes and services.
5. DAFM propose to use the UBIN to facilitate the administration, supervision and control of DAFM services / schemes to businesses and in the broader development of policy deliverables.
6. DAFM intend to utilise the UBIN to facilitate and enhance the delivery of schemes and services whilst providing data to enhance policy making decisions.
7. DAFM purport to use UBIN data for the evaluation and review of schemes/services and programmes. This will facilitate the development of future programmes/services and policy implementation.
8. DAFM intend to apply the UBIN to support the analysis of its business functions and programmes which is reliant on up-to-date and valid data.

Tailte Éireann

Tailte Éireann already support an open data API which provides linked attributions to commercial properties to the public. The sharing of the UBIN dataset represents a proportionately small increase to the existing sharing of data but will enable, and is necessary to, delivery of the Tailte Éireann strategic vision and future service delivery.

DPENDR

DPENDR already collect information on corporate beneficiaries albeit in a non-validated form. The UBIN dataset will provide this existing dataset in a validated form and therefore represents a proportionately limited increase in sharing of existing data. The UBIN data is however necessary to minimise fraud in the draw-down of EU funds and for DPENDR to fulfil their delegated EU audit role.

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.

RSA

Via the delivery of its own functions the RSA already processes a variety of personal data and the safeguards already in place for this data will be leveraged to also protect the UBIN data which will be shared under this agreement.

These safeguards include the following:

Access Control

- Secure remote access to RSA's network which requires multi factor authentication.
- RSA laptops and any internal hard drives are encrypted by the RSA ICT Helpdesk Team prior to issue.
- Implementation of Mobile Device Management (MDM) is applied to all mobile devices.
- Access to information is granted on a need only basis in line with RSA Access Control Policy and Acceptable Usage Policy.

Disaster recovery

- Disaster recovery and backup routines are maintained and regularly reviewed.

Cyber Control

- RSA have implemented a cybersecurity policy.

Data Retention

- RSA has a Data Retention procedure which is set for the minimum amount of time having regard to any organisational legal requirements or specific RSA business requirements.

Training and Awareness

- RSA staff employees are informed of their responsibilities under Data Protection Law and trained regularly.
- Regular internal phishing awareness campaigns are carried out to measure and raise profile of cyber security awareness.

Each of the above safeguard measures and policies are regularly reviewed.

DAFM

- The data provided to DAFM will be (/is) imported into a server which is in a locked-down environment with restricted access to relevant personnel only. DAFM's information security management system is ISO27001 certified, including the datacentre housing the server environment. Within the server, the data is accessible only for the authorised purpose. The server is securely backed up in accordance with DAFM's IT backup policy.
- Access to data is restricted by roles and authorisations at an application data level. Further access is limited by user/password restrictions.
- Privileged access is practised here in DAFM with least amount of access given to the user based on the roles and authorisations given.
- DAFM has a secure suite of systems behind Private VPN's and Citrix Desktop software to ensure the proper controls are in place for data remotely accessed by users.
- All customer and client data is held on centralised databases instances running on hardware located in DAFM's on prem Data Centre. All removable data ports (USB etc) have write privileges disabled.
- DAFM provides sound training for all staff in data awareness and complies with the various ISO procedures in this area.

- DAFM has invested significantly in restore and recovery capabilities for all its enterprise level data which also includes Disaster Recovery and Business Continuity procedures. All office documents stored on DAFM's shared drives are also subject to vigorous backup policies.
- All DAFM data is securely stored in its on prem Data Centre and is archived according to internal data retention policies.
- The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. 2 In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

DETE

- Regular data protection training is provided to staff. Tailored training also available to business units. Regular Information Security awareness and advice is also provided to staff. Data protection and Information Security awareness training is provided as part of induction.
- A comprehensive suite of Information Security policies and standards are in place, these outline the controls in place and the acceptable usage of departmental IT resources. These policies include Acceptable Usage, User Access, Remote Access, Incident Management and Threat and Vulnerability Management. Policies are subject to review on a regular basis. Additionally, a Data protection policy has been prepared by Data Protection Officer.
- Access to data and resources are managed on the Principle of Least Privilege with access auditing in place. Remote access to departmental IT resources is governed by technological controls and policies. All laptops are encrypted, and access to portable media is restricted and audited.
- The Department has deployed a range of Information Security tools, including systems for logging and monitoring.
- The Department has several resilience measures in place including, taking routine backups, and testing these, Business Continuity and Disaster Recovery Plans along with Incident Response Plans.
- The Department also has access to independent security advice and a third party undertakes security assessments and penetration testing as required.

Tailte Éireann

The list below summarises the safeguards applicable to the data shared under this agreement.

Data Access and Controls

User access to network and application data is controlled on the Principle of Least Privilege supported by Active Directory Group Policy and Password Management Software.
We employ an IAM solution for all data within our cloud infrastructure and this reviewed regularly. Users access is restricted by roles at an application data level. At a local level we have a removable media lock down policy. At a database and AWS level we have a cloud guard application by check point which incorporated Data Leaks Protection (DLP).

Staff Awareness

Department security policy, remote access policy, mobile device policy and acceptable usage policy, in particular, provides direction on file and data storage policies. All policies are

reviewed annually and are the primary content of our security education and awareness program that runs continually for all staff during the calendar year.

Security Policies
All security policies are reviewed annually by our ICT Security Manager, owned by our Chief Information Officer and approved by our Senior Management Board as part of our Corporate Governance and Risk Management process.
We have a continuous Security Education and Awareness Programme for all staff which supports our security posture.

Retention
Data will be retained for “current plus ten years”.

DPENDR
ISO Certification
The OGCIO’s Management Desktop service is ISO 27001 certified, the application that will hold and manage access to the UBIN data is ISO 27001 certified as it the Cloud Service provider. All users authenticated and provisioned on the application are subject to confidentiality agreements and their access approved by appropriate authorities.

Human Resources Security
DPENDR informs its personnel about relevant security procedures and their respective roles. It also informs its personnel of possible consequences of breaching the security rules and procedures. DPENDR provides security awareness material to all clients for security awareness training.

Access Control
A record of security privileges of individuals having access to data is maintained and industry standard practices to identify and authenticate users who attempt to access information systems are maintained. In addition, technical support personnel are only permitted to have access to data when needed. Passwords are stored in a way that makes them unintelligible while they are in force.

Information Security Incident Management
A record of all security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data is maintained.

Disaster Recovery, Resilience and Backup
Both on-site and off-site backups are included in the backup policy. Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up at a remote site. The remote site back process uses storage and database replication. The Data Backup Frequency is one (1) day, the Backup Retention Time is seven (7) days. The integrity of backups is validated by:

1. real time monitoring of the storage snapshot process for system errors,
2. validating CHECKSUM at the end of a backup process to assure the same number of bits exists on both source and destination storage systems, and
3. and annual restoration of production data from an alternate site to validate both data and restore flows integrity.

Retention
Data will be retained for current plus five years.

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.

The Office of the Revenue Commissioners.
Road Safety Authority.
Department of Agriculture, Food and the Marine.
Department of Enterprise, Trade and Employment.
Tailte Éireann – Valuation.
Department of Public Expenditure NDP Delivery and Reform – OGCIO.

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:	Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	[The Office of the Revenue Commissioners		

Table 19 .0

19.2 Other Party/Parties

OTHER PARTY			
Signature:		**Date:**	
Print Name:			
Position held;	[Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	[Road Safety Authority]		

Table 19.1

OTHER PARTY			
Signature:		**Date:**	
Print Name:			
Position held;	[Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	[Department of Agriculture, Food and the Marine		

Table 19.1

OTHER PARTY			
Signature:		**Date:**	
Print Name:			
Position held;	[Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	Department of Enterprise, Trade and Employment		

Table 19.1

OTHER PARTY			
Signature:		**Date:**	
Print Name:			
Position held;	[Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	Tailte Éireann		

Table 19.1

OTHER PARTY			
Signature:		**Date:**	
Print Name:			
Position held;	[Insert position of Authorised Signatory] PO or above		
Email:			
For and on behalf of:	Department of Public Expenditure NDP Delivery and Reform		

Table 19.1

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			☒
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			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	*Joan French*	**Date:**	7 May 2024
Print Name:	Joan French		
Position:	Data Protection Officer		
Email:	Dataprotection@revenue.ie		
For and on behalf of:	Office of the Revenue Commissioners		

Table 19.2

Other Party/Parties DPO Statement

DAFM

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
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			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	Caitriona McEvoy	**Date:**	11 July 2024
Print Name:	Caitriona McEvoy		
Position:	Data Protection Officer		
Email:	dataprotectionofficer@agriculture.gov.ie		
For and on behalf of:	Department of Agriculture, Food and the Marine		

DETE

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
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			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	*Celyna Coughlan*	**Date:**	8 February 2024
Print Name:	Celyna Coughlan		
Position:	Data Protection Officer		
Email:	Celyna.coughlan@enterprise.gov.ie		
For and on behalf of:	Department of Enterprise, Trade and Employment		

RSA

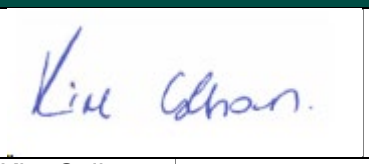
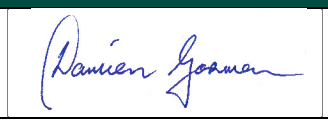
OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:		**Date:**	29 January 2024
Print Name:	Kim Colhoun		
Position:	Data Protection Officer		
Email:	DataProtection@rsa.ie		
For and on behalf of:	Road Safety Authority		

Table 19.3

Tailte Éireann

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
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			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:		**Date:**	29 January 2024
Print Name:	Damien Gorman, Data Protection Officer, Tailte Éireann		
Position:	Data Protection Officer		
Email:	Damien.Gorman@tailte.ie		
For and on behalf of:	Tailte Éireann		

DPENDR

OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			☒
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			☒
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			☒
Signature:	*David Feeney*	**Date:**	29 January 2024
Print Name:	David Feeney		
Position:	Acting Data Protection Officer		
Email:	dataprotection@per.gov.ie		
For and on behalf of:	[Department of Public Expenditure, NDP Delivery and Reform		