DATA SHARING AGREEMENT

Between

Strategic Banking Corporation of Ireland ('SBCI')

and

Minister for Agriculture, Food and the Marine ('MAFM')
And
Minister for Enterprise, Trade and Employment ('METE')

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

Enabling the SBCI to share personal data in relation to individuals, who have availed of the SBCI schemes, including the Future Growth Loans Scheme (the "FGLS") and the Brexit Impact Loan Scheme (the "BILS").

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

Data Sharing Agreement

BETWEEN

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

LEAD AGENCY NAME	ADDRESS
Strategic Banking Corporation of Ireland	Treasury Dock, North Wall Quay, Dublin 1 D01A9T8

AND

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

PARTY NAME	ADDRESS
Minister for Agriculture, Food and the Marine And	Agriculture House, Kildare St, Dublin
Minister for Enterprise, Trade and Employment	23 Kildare Street, Dublin 2

The Parties hereby agree that Strategic Banking Corporation of Ireland 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?	NO
1.1.3	The introduction of new types of technology?	NO

Table 1.2

If '**Yes'** to either of the last two questions, proceed to 1.1.4.
If '**No'** to both of the last two questions, proceed to 1.2.

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

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	DESCRIPTION
(V)	**Section 13(2)(a)(ii)(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* The SBCI was established for the purpose of making low-cost credit available to Irish Small to Medium Size Enterprises (SME's) and small mid-cap enterprises, it does this through several functions as set out in Section 8 of the Strategic Banking Corporation of Ireland Act 2014. The Schemes provided by the Government of Ireland and listed in this Data Sharing Agreement, are subject to administration and supervision by the Government of Ireland and the purpose of the sharing of information is to provide oversight to the relevant Departments, party to this Agreement. The SBCI, as provided for in the co-operation agreements between the SBCI, MAFM and METE, may disclose a certain limited amount

	of personal data to the Ministers, as required by the Ministers, in conjunction with the SBCIs establishment, development, launch and operation of the schemes. In order to ensure that public monies are being spent for the purpose for which they were intended DAFM and/or DETE may undertake audits of schemes. In the course of these audits, the Department's will randomly select a percentage of scheme participants to review to ensure compliance with the eligibility criteria and intent of the scheme. All the relevant scheme documentation for the selected scheme participants may be requested in order to conduct the review and in some instances personal data is transferred as the scheme is open to both incorporated and unincorporated enterprises (sole traders or individuals). The Strategic Banking Corporation of Ireland Act 2014 establishes the SBCI, including in respect of the share capital of the SBCI and its ownership. The Loan Guarantee Scheme Agreements (Strategic Banking Corporation of Ireland) Act 2021, referred to in this agreement as the "2021 Act", provides for review of the functioning of these arrangements in section 3.

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	The SBCI facilitates lending to Small to Medium Size Enterprises and small mid-cap enterprises, these are companies, sole traders or individuals and can therefore include personal data including but not limited to i. Name ii. Address iii. Eircode iv. E-mail address v. Telephone number vi. Customer Eligibility Reference Number vii. CRO Number viii. VAT Number ix. Department of Agriculture, Food and the Marine Identifier x. Bank Account Numbers Certain SMEs, due to the nature of the company may share personal information for example, as they are sole traders, or the company is run from their home.

	Information at this level is only shared where necessary for the purpose of auditing and will only be personal in a very small number of cases.
Non-personal Data	Details including but not limited to information in relation to the company or business, including their size, sector, finances, and loan details and State-Aid details. For the purposes of clarification, as the SMEs are in the majority of cases a company, the detail set out above as non-personal data is relating to companies rather than individuals.

Table 3.4

4. Function of the Parties

4.1 Function of the Parties

In table 4.1 below:

i. Specify the function of the party disclosing data to which the purpose (as defined in table 2.3) of the data sharing relates

ii. Specify the function of the party receiving data to which the purpose (as defined in table 2.3) of the data sharing relates.

PARTY	FUNCTION
i. SBCI	BILS: The role of SBCI is to utilise funds provided by the MAFM and METE to establish, develop, launch and operate the BILS, and to guarantee part of the credit risk of certain finance providers in making financing available to SMEs and small mid-cap enterprises established or with a branch in the State (the "**Borrowers**") pursuant to term loan facilities provided directly by the finance provider to the Borrowers. This arises by virtue of a scheme established pursuant to the Loan Guarantee Scheme Agreements (Strategic Banking Corporation of Ireland) Act 2021 (the "**2021 Act**") to provide support to the Borrowers affected by the invocation by the British government of Article 50 of the Treaty on the European Union on 29 March 2017 and the Covid-19 pandemic. The purpose of sharing of information, to include personal data with the Ministers, is in conjunction with the SBCI's establishment, development, launch and operation of the BILS, for the purpose of providing State-Aid information to the MAFM and for assessing and auditing SBCI's compliance with the BILS by the MAFM and the METE. FGLS: The role of SBCI is to utilise funds provided by the MAFM and METE to establish, develop, launch and operate the FGLS, and to guarantee part of the credit risk of financial sub-intermediaries in making financing available to SMEs and small mid-cap enterprises. This arises by virtue of the FGLS which is set up pursuant to the European Investment Fund Act 2018 (the "**2018 Act**") to support those enterprises including those engaged

	in primary agriculture in Ireland by facilitating the provision of discounted long-term loans and flexible credit facilities to those enterprises through financial sub-intermediaries. The purpose of sharing of information, to include personal data, with the Ministers, is in conjunction with the SBCI's establishment, development, launch and operation of the FGLS for the purpose of providing State-Aid information to the MAFM and for assessing and auditing SBCI's compliance with the FGLS by the MAFM and the METE
ii. MAFM	BILS: The role of the Minister under the BILS is to provide the funds to enable SBCI to fulfil its obligations pursuant to its functions set out in the Strategic Banking Corporation of Ireland Act 2014 (the "**2014 Act**") as guarantor and cover costs and expenses incurred by the SBCI in connection with the establishment, development, launch and operation of the scheme and to assess and audit SBCI's compliance with the terms of the BILS. The Minister also has an oversight role to monitor State-Aid through the scheme and to assess and audit SBCI's compliance in operating the BILS within the terms set out for the BILS. FGLS: The role of the Minister under the FGLS is to provide the funds to enable SBCI to fulfil its obligations pursuant to its functions set out in the Strategic Banking Corporation of Ireland Act 2014 (the "**2014 Act**") as guarantor and cover costs and expenses incurred by the SBCI in connection with the establishment, development, launch and operation of the scheme and to assess and audit SBCI's compliance with the terms of the FGLS. The Minister also has an oversight role to monitor State-Aid through the scheme and to assess and audit SBCI's compliance in operating the FGLS within the terms set out for the FGLS.
iii. METE	BILS: The role of the Minister under the BILS is to provide the funds to enable SBCI to fulfil its obligations pursuant to its functions set out in the Strategic Banking Corporation of Ireland Act 2014 (the "**2014 Act**") as guarantor and cover costs and expenses incurred by the SBCI in connection with the establishment, development, launch and operation of the scheme

	and to assess and audit SBCI's compliance with the terms of the BILS. The Minister also has an oversight role to assess and audit SBCI's compliance in operating the BILS within the terms set out for the BILS. FGLS: The role of the Minister under the FGLS is to provide the funds to enable SBCI to fulfil its obligations pursuant to its functions set out in the Strategic Banking Corporation of Ireland Act 2014 (the "**2014 Act**") as guarantor and cover costs and expenses incurred by the SBCI in connection with the establishment, development, launch and operation of the scheme and to assess and audit SBCI's compliance with the terms of the FGLS. The Minister also has an oversight role to assess and audit SBCI's compliance in operating the FGLS within the terms set out for the FGLS.

[*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
[Section 13(2)(a)(ii)(V)	**Section 13(2)(a)(ii)(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

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:

No further processing is undertaken.

LEGISLATION	DESCRIPTION
[N/A	N/A

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	☒	SME's and small mid-cap enterprises availing of SBCI products

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 15th December 2022 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	☐	
Other frequency	☒	A variety of reporting from weekly, monthly and quarterly to ad hoc.

Table 8.2

9. How data will be processed

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

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

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

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

9.2 Description of Processing

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

	DESCRIPTION OF PROCESSING
MAFM	Processing of personal data by MAFM shall be processed solely for the purpose of monitoring State-Aid arising from the BILS and FGLS and assessing and auditing of the SBCIs compliance with the terms of the BILS and FGLS Co-operation agreement between the SBCI, MAFM and METE and at all times in accordance with their obligations as Controllers under Data Protection Law and all other applicable laws. High level data in respect of the activity for each of the schemes is shared with MAFM. This high level data sets out the activity in the scheme at an overall level and is used to provide oversight of the scheme. This information is sent via secure file transfer. The information is stored securely in DAFM. The data is reviewed by staff in the relevant unit to consider the activity of the schemes. For specific audit exercises the documentation in respect of the application under the scheme is shared with the Department as necessary. This information is reviewed by the relevant unit. The information is stored securely in DAFM. State-aid reporting on the schemes to DAFM is required and the necessary information is provided to DAFM via secure file transfer. The information is stored securely in DAFM.
METE	Processing of personal data by METE shall be processed solely for the purpose of assessing and auditing of the SBCIs compliance with the terms of the BILS and FGLS Co-operation agreement between the SBCI, METE and MAFM and at all times in accordance with their obligations as Controllers under Data Protection Law and all other applicable laws. High level data in respect of the activity for each of the schemes is shared with METE. This high level data sets out the activity in the scheme at an overall level and is used to provide oversight of the scheme. This information is sent via secure file transfer. The information is stored securely in DETE. The data is reviewed by staff in the relevant unit to consider the activity of the schemes. For specific audit exercises the documentation in respect of the application under the scheme is shared with the Department as necessary. This information is reviewed by the relevant unit. The information is stored securely in DETE.

Table 9.2

9.3 Further Processing

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

	SPECIFY FURTHER PROCESSING
METE	METE processes the data only to the extent, and in such manner as is necessary and set out above. Data is not further processed beyond the original purpose.
MAFM	MAFM processes the data only to the extent, and in such manner as is necessary and set out above. Data is not further processed beyond the original purpose.

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
METE	METE shall process the personal data only to the extent, and in such a manner, as is necessary in connection with the Personal Data Purpose referred to in Table 9.2 above, and shall not process the SBCI personal data for any other purpose. METE shall not transfer the personal data to a country outside of the European Economic Area.
MAFM	MAFM shall process the personal data only to the extent, and in such a manner, as is necessary in connection with the Personal Data Purpose referred to in Table 9.2 above, and shall not process the SBCI personal data for any other purpose. MAFM shall not transfer the personal data to a country outside of the European Economic Area.

Table 10.0

11. Security Measures

11.1 Security and Training

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

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

This may include, but is not limited to:

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

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

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

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

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

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

11.2 Security Measures

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

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

11.2.1 Lead Agency/ Party Disclosing Data

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

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

11.2.1.1	TRANSMISSION	COMPLIES	DOES NOT COMPLY
	When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use. Please provide details.	☒	☐
		Personal data provided for under this arrangement is sent from the SBCI to DETE and DAFM using secure file transfer. The NTMA secure file transfer system (Accellion) provides a secure web based facility hosted by the NTMA to enable the exchange of large files and folder with other bodies.	

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 SBCI transmit data using the NTMA Secure File Transfer. Files sent via Accellion are stored on the system and available for download by DETE and DAFM for 5 days before deletion. The SBCI will not utilise the NTMA's email system to transmit personal data files under this agreement. DETE and DAFM users require an account on the NTMA Secure File Transfer system to download data. Security practices are in place for the creation and management of external user accounts on the NTMA Secure File Transfer system.

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 Department of Agriculture, Food and the Marine

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.	☒	☐ *[Please provide details for all non-complying or 'not applicable' statements.]*	☐
11.2.2.1.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒ Any information accessed remotely is done via Citrix which is a secure log-in portal for the Department of Agriculture, Food and the Marine Systems.	☐	☐
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.	☒ Only members of staff in the Access to Finance section of the Economics and Planning Division of the Department of Agriculture, Food and the Marine are granted access to the area where the data will be stored. This access is granted via a designated information officer and only with the approval of senior management of the section/division	☐	☐
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.	Only authorised personnel are granted access to where the data is stored. The data is password protected where necessary. Department of Agriculture, Food and the Marine systems do not permit removable media to be used with its systems/equipment either remotely or on-site		
11.2.2.5	**Data is encrypted at rest on mobile devices such as laptops and removable media.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐	☐
			Please provide details for all non-complying or 'not applicable' statements.	
11.2.2.6	**There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location.** Please provide details.	☒	☐	☐
		All Department of Agriculture, Food and the Marine staff receive regular training through HR Learning and Development Unit on Data Protection controls and regulations including specific examples of best practice for saving data. Completion of training in Data Protection is compulsory for all staff and is traced by the Doras on-line system		
11.2.2.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	DAFM has a Backup and Recovery Policy in place, this policy covers several environments including Windows, Email, databases etc.. Below is an overview of the policy: There are several reasons for having an effective Backup and Recovery procedure for Computer-based information. ○ To ensure the availability of a recent copy of any data file which may become corrupt or otherwise unusable		

		○ To allow for recovery of data files which may have been wrongly updated due to an application or procedural error ○ To maintain a copy of Operating System software which can be reloaded in the event of equipment malfunction ○ To hold a complete copy of all data items for use in the event of a disaster. DAFM's Backup and Recovery regime must provide for recovery of the most recent possible data in all situations.
11.2.2.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Yes. The Department of Agriculture has a data retention policy in operation that complies with governing regulations in relation to the secure storage and disposal of data. The data collected will be held by the Department only as long as there is a business need to do so, in line with the purpose(s) for which it is collected. After this time, it will be marked for destruction and will be destroyed in line with internal guidelines or guidelines for destruction received from the National Archives Office or associated permissions received from them. Summary reports of the findings of the specific audit exercises will be retained by the Department of Agriculture, Food and the Marine for 8 years post the expiry of the BILS and FGLS-though this may be extended, if deemed appropriate, at a later time. These summary reports do not contain personal data. State-Aid related data is to be retained for 10 years from the date on which the ad hoc aid was granted or the last aid was granted under an aid scheme as outlined in current Agriculture Block Exemption Regulations.

11.2.2.9 – SECURITY STATEMENT
Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures. You may also provide details of additional measures in place that are relevant to this arrangement.
Department of Agriculture, Food and the Marine has an Information Security Policy in place to protect the information held by the Department, reducing the likelihood of potential threats. The policy conforms to the requirements of international standards for information security management ISO/IEC 27001:2013. The objectives of this policy include: 1. Ensure that information is accessible only to those authorised to have access; 2. Safeguard the accuracy and completeness of information and processing methods; 3. Manage security issues related to services and processes to ensure that information security risks are identified, and appropriate controls are implemented and documented; 4. Investigate and act upon all breaches of security, actual or suspected; 5. Provide a secure working environment for staff; 6. Produce, maintain and test on a regular basis Information security continuity plans; 7. Promote and ensure mandatory cyber, data protection and information security awareness training for DAFM staff and outside support; 8. Ensure that Information Security is continually improved and that regular reviews are performed to ensure that the operation of the ISMS is appropriate and aligned with requirements; 9. Ensure that no unauthorised Software is installed by staff with administrator access; 10. Investigate and act upon Data Protection breaches, actual or suspected.

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA	YES/NO
Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.3

11.2.2.1 Department of Enterprise, Trade and Employment

11.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1	**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.	☒	☐ *[Please provide details for all non-complying or 'not applicable' statements.]*	☐
11.2.2.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒ Any information accessed remotely by the Department of Enterprise Trade and Employment is done via secure access devices issued to employees by the Department of Enterprise, Trade and Employment.	☐	☐
11.2.2.3	**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.	☒ Only members of staff in the Access to Finance Unit in the Department of Enterprise, Trade and Employment are granted access to the area where the data will be stored. This access is granted on a Need-to-Know basis and respects Data Minimisation Rules.	☐	☐
11.2.2.4	**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.	☒ Only authorised personnel in the Access to Finance Unit are granted access to where the data is stored. This access is granted on a Need-to-Know basis and respects Data Minimisation Rules.	☐	☐

11.2.2.5	**Data is encrypted at rest on mobile devices such as laptops and removable media.** Please provide details for all non-complying or 'not applicable' statements.	☒	☐ *Please provide details for all non-complying or 'not applicable' statements.*	☐
11.2.2.6	**There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location.** Please provide details.	☒	☐ All Department of Enterprise, Trade and Employment staff receive regular training through HR Learning and Development Unit on Data Protection controls and regulations including specific examples of best practice for data protection compliance. Completion of training in Data Protection is compulsory for all new staff and re-fresher courses are offered regularly for existing staff.	☐
11.2.2.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	DETE has a Backup and Recovery Policy in place, this policy covers several environments including Windows, Email, databases etc.. Below is an overview of the policy: Data in fileshares and in business systems is backed up nightly, with milestone backup saved to off-line tape on a monthly basis.		
11.2.2.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Yes. The Department of Enterprise, Trade and Employment stores personal data securely and will not retain or use personal information for any longer than is necessary. Personal data sets will be securely destructed by us upon completion of the assessment exercises of the BILS and FGLS. However, summary reports of the findings of the specific audit exercises will be retained by the Department of Enterprise, Trade and Employment for 6 years post the expiry of the BILS and FGLS. These summary reports do not contain personal data.		

Table 11.2.4

11.2.2.9 – SECURITY STATEMENT
Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures. You may also provide details of additional measures in place that are relevant to this arrangement.
Security management in key areas such as securing, monitoring and oversight and response resilience are in place for the Department of Enterprise, Trade and Employment, including the following: (a) Security • System controls in place in line with industry best practices, including secure transfer of Personal Data to SBCI from Department of Enterprise, Trade and Employment using appropriate secure channels to transfer encrypted files. • Information Security and Cyber Security teams in place. • Security management programme in place. • Physical security management. • Policies and procedures; and • End User Security Awareness training. (b) Monitoring and Oversight • Processes in place for regular patching of systems including proactive patching or mitigation of known vulnerabilities. • Independent third-party security assessments, vulnerability scanning and penetration testing in place. • Threat analytics capabilities. • Third-party security assessments. • Risk management governance and oversight; and, • Regulatory auditing and compliance. (c) Resilience • Business Continuity Plans including cyber incident plans. • Crisis Management Procedures. • Procedures reviewed and tested at least annually.

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA	YES/NO
Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.4

11.3 Data Breaches and Reporting

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

12. Retention

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

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

INFORMATION TYPE	RETENTION REQUIREMENTS
1. Information to be disclosed	The SBCI facilitates lending-to Small to Medium Size Enterprises and small mid-cap enterprises, these are companies, sole traders or individuals and can therefore include personal data including but not limited to Name, Address, Eircode, E-mail address, Telephone number, Customer Eligibility Reference Number, CRO Number, VAT Number, Department of Agriculture, Food and the Marine Identifier, Bank Account Numbers including but not limited to information in relation to the company or business, including their size, sector finances, loan details and State-Aid details. Information disclosed to MAFM in relation to scheme applications should be retained for a minimum of 8 years from the date of expiry of the scheme with State Aid related information being retained in line with the prevailing Agriculture Block Exemption Regulation. Such records shall be kept for 10 years from the date on which the ad hoc aid was granted or the last aid was granted under an aid scheme. Personal information disclosed to METE will not be retained for any longer than is necessary and will be destroyed upon completion of the assessment exercises of the BILS and FGLS. summary reports of the findings of the specific audit exercises will be retained by the Department of Enterprise, Trade and Employment for 6 years post the expiry of the BILS and FGLS. These summary reports do not contain personal data.
2. Information resulting from the processing of the data	Compliance/non-compliance of SBCI in terms of operating the schemes within the terms of the schemes and State-Aid reporting and monitoring requirements.

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	At the end of the retention period the nominated officers in DETE and DAFM will review the information for disposal or further retention by their Department. The data will be disposed of in accordance with section 7 of the National Archives Act 1986 as amended.
2. Information resulting from processing of the data	At the end of the retention period the nominated officers in DETE and DAFM will review the information for disposal or further retention by their Department. The data will be disposed of in accordance with section 7 of the National Archives Act 1986 as amended.

Table 13.0

14. Withdrawal from Agreement

14.1 Procedure

Each Party commits to giving a minimum of 21 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.

14.3 [Termination]

The Parties acknowledge and agree that they have entered into this Data Sharing Agreement due to the sharing of Personal Data arising from the [Co-Operation Agreements]. Subject to clause 14.1 above, this Data Sharing Agreement shall survive for as long as at least one of the [Co-Operation Agreements] is in force. On the expiry or termination of all the [Co-Operation Agreements] either Party may terminate this Data Sharing Agreement on written notice.

14.3.1 [Withdrawal from agreement]

If either Party exercises its right to withdraw from this Data Sharing Agreement in accordance with clause 14.1 while there is a still at least one of the [Co-Operation Agreements] in force then: (i) for the avoidance of doubt, such [Co-Operation Agreement(s)] shall survive termination or

expiry of this Data Sharing Agreement; and (ii) upon such termination or expiry of the Data Sharing Agreement in accordance with clause 14.1, each Party shall use reasonable endeavours to enter into an equivalent agreement providing for the sharing and processing of Personal Data relating to the [Co-Operation Agreement(s)] then in force.

14.3.2 [Required continuance of processing]

Where this Data Sharing Agreement is terminated in accordance with clause 14.3 or it is terminated in accordance with clause 14.1 then pending such termination, the Parties agree and acknowledge that they may need to continue processing Personal Data pursuant to this Data Sharing Agreement to the extent necessary to conclude the processing required thereunder, provided that such processing complies with the requirements of this Data Sharing Agreement and the GDPR.

14.3.3 Terms

For the purposes of this clause the term "**Co-Operation Agreements**" means, in relation to **BILS**: (1) co-operation agreement dated 07/09/2021 between the Minister for Agriculture, Food and the Minister for Marine, Enterprise, Trade and Employment and the SBCI and in relation to **FGLS**: (1) co-operation agreement dated 21 December 2018 between the Minister for Agriculture, Food and the Marine, Minister for Enterprise, Trade and Employment and the SBCI and (2) amended co-operation agreement dated 24/07/2020 between the Minister for Agriculture, Food and the Marine Minister for Enterprise, Trade and Employment and the SBCI

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.

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 [select appropriately]	☐	
Has not been conducted [select appropriately]	☒	The transfer of data from the SBCI to METE and MAFM was determined unlikely to result in a high risk to the privacy rights and freedoms of natural persons given the type and volume of the personal data involved.

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.

BILS: The Loan Guarantee Schemes Agreements (Strategic Banking Corporation of Ireland) Act 2021 (the "**2021 Act**") entitles Ministers of the Government to enter into agreements with SBCI to facilitate access to finance pursuant to certain loan guarantee schemes by qualifying enterprises. The BILS has been established pursuant to the 2021 Act. The SBCI is required to report to the Ministers during the continuance of the scheme, so as to provide State-Aid information to the MAFM, and to allow the MAFM and METE to assess and audit SBCI's compliance with the terms of the BILS. The processing of personal data by the Ministers is necessary to facilitate this and is solely for the purpose of monitoring State-Aid and assessing and auditing of the SBCI's compliance with the terms of the BILS co-operation agreement between the SBCI, METE and MAFM.

FGLS: The European Investment Fund Act 2018 (the "**2018 Act**") entitles Ministers of the Government to enter into agreements with the European Investment Fund for the purpose of facilitating access to finance for qualifying enterprises. The FGLS has been established pursuant to the 2018 Act. The SBCI is required to report to the Minister during the continuance of the schemes, so as provide State-Aid information to the MAFM, and to allow the MAFM and METE to assess and audit SBCI's compliance with the terms of the FGLS. The processing of personal data by the Ministers is necessary to facilitate this and is solely for the purpose of monitoring State-Aid and assessing and auditing of the SBCI's compliance with the terms of the FGLS co-operation agreement between the SBCI, METE and MAFM.

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.

The data held by the SBCI is held in compliance with Article 32 of the GDPR, including but not limited to the measures set out in section 11.1 of this agreement.

The information held by the SBCI and shared under this agreement is gathered from persons who have applied under one of the schemes. The schemes are part of Government policy and their ongoing effectiveness and management need to be monitored, therefore the sharing is required.

The SBCI and the Departments have security measures in place which ensure that the information is shared in a secure manner and the security and safeguards are proportionate. The effects of disclosure of any of the data shared pursuant to this agreement, including personal data, on the affected Data Subjects would be minimal given the limited categories of personal data involved in the processing activity.

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.

- Strategic Banking Corporation of Ireland
- Minister for Agriculture, Food and the Marine
- Minister for Enterprise, Trade and Employment

19. Authorised Signatory

An authorised signatory/signatories is/are 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/signatories has/have 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:	Seán Farrell	**Date:**	14/12/2022
Print Name:	Seán Farrell		
Position held:	Head of Products, Research and Marketing, SBCI		
Email:	sean.farrell@sbci.gov.ie		
For and on behalf of:	Strategic Banking Corporation of Ireland		
LEAD AGENCY			
Signature:	June Butler	**Date:**	15/12/2022
Print Name:	June Butler		
Position held:	Chief Executive Officer, SBCI		
Email:	june.butler@sbci.gov.ie		
For and on behalf of:	Strategic Banking Corporation of Ireland		

Table 19 .0

19.2 Other Party/Parties

OTHER PARTY			
Signature:	Fiona Kilcullen	**Date:**	13/12/2022
Print Name:	Fiona Kilcullen		
Position held;	Principal, Access to Finance Unit		
Email:	Fiona.kilcullen@enterprise.gov.ie		
For and on behalf of:	Minister for Enterprise, Trade and Employment		

Table 19.1

OTHER PARTY			
Signature:	Sean Bell	**Date:**	13/12/2022
Print Name:	Sean Bell		
Position held;	Chief Economist, Head of Economics and Planning Division		
Email:	Sean.bell@agriculture.gov.ie		
For and on behalf of:	Minister of Agriculture, Food and the Marine		

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:	Philip Bowler	**Date:**	13/12/2022
Print Name:	Philip Bowler		
Position:	Data Protection Officer		
Email:	Philip.Bowler@ntma.ie		
For and on behalf of:	Strategic Banking Corporation of Ireland		

Table 19.2

Other Party/Parties DPO Statement – Department of Enterprise, Trade and Employment

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:**	13/12/2022
Print Name:	Celyna Coughlan		
Position:	Data Protection Officer		
Email:	dataprotection@enterprise.gov.ie		
For and on behalf of:	Minister for Enterprise, Trade and Employment		

Table 19.3

Other Party/Parties DPO Statement – Department of Agriculture, Food and the Marine

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:**	13/12/2022
Print Name:	Caitriona McEvoy		
Position:	Data Protection Officer		
Email:	dataprotectionofficer@agriculture.gov.ie		
For and on behalf of:	Minister for Agriculture, Food and the Marine		

Table 19.3