DRAFT

DATA SHARING AGREEMENT

Between

The Department of Agriculture, Food and the Marine (DAFM)

and

Bord Bia

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

To enable the verification of Animal Identification Movement Data (AIMs) in order to meet the criteria of the relevant Bord Bia Scheme

Table of Contents

Interpretation Table 3
1. Evaluation for a Data Protection Impact Assessment (DPIA) 5
2. Purpose of the Data Sharing 7
3. Data to be shared 9
4. Function of the Parties 11
5. Legal Basis 12
6. Impetus for Data Sharing 14
7. Categories of Data Shared 15
8. Duration and Frequency 16
10. Restrictions 18
11. Security Measures 19
12. Retention 25
13. Methods Used to Destroy/Delete Data 26
14. Withdrawal from Agreement 27
15. Other Matters 28
16. Schedule A - Data Protection Impact Assessment 30
17. Schedule B 32
18. Schedule C 34
19. Authorised Signatory 35
Data Protection Officers Statement 36

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
Bord Bia	**Bord Bia,** **140 Pembroke Road, Dublin 4, D04 NV34.**

AND

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

PARTY NAME	ADDRESS
The Department of Agriculture, Food and the Marine	**Agriculture House, Kildare Street, Dublin, D02 WK12**

The Parties hereby agree that **Bord Bia** 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	DESCRIPTION
In line with table 2.2. Data Provided to facilitate the evaluation and implementation of the programme aimed to achieve a reduction of the carbon footprint for those herds signed up to the scheme	This Data Sharing Agreement covers sharing of Personal Data necessary in the delivery of Bord Bia's core services where Animal Identification & Movement (AIMs) data is processed. This processing produces calculations in support of the reduction of carbon emissions and to demonstrate and analyse the integrity of the livestock sample using AIMs data. This calculation is provided to the relevant farmer within the farmer feedback report. This reporting supports the analysis and reporting which benchmarks the farming activities of Bord Bia clients. This Personal Data is used in Bord Bia's calculation of sustainability and carbon emission reduction, contributing to a service to the state of vital importance.

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	Data which uniquely identifies livestock (tag or herd numbers) can identify a natural person associated with this identifier. Livestock tags and herd numbers may identify an owner or person associated with the unique identifier of the animal. Herd Number Tag Number

Non-personal Data	Livestock data including, elements such as age, movements and other non-personal data sets. Report Year <u>Animal details</u> Sex Date of Birth Breed Dam Breed Sire Breed Date Movement into herd Date movement out of herd Movement Type Dam Tag Number Where relevant date last calved

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. Department of Agriculture , Food and the Marine	DAFM will share AIMs data with Bord Bia. There is a legislative requirement for DAFM to maintain data on livestock which, species dependant, includes details on the registration, identification / tagging and movement of livestock. This include herd number, tag numbers, other relevant information. The information available may, where appropriate, be provided to support other schemes which facilitates the promotion of the livestock industry.
ii. Bord Bia	This data sharing supports activities outlined in the Bord Bia Sustainable Assurance Scheme Membership Agreement between Bord Bia and herd owners so herd owners are fully aware of the activity. Bord Bia receives the data from DAFM to enable Bord Bia to deliver its core services where AIMs data is processed. This processing produces carbon footprint calculations in support of the reduction of carbon emissions and to demonstrate and analyse the integrity of the livestock sample using AIMs data. Carbon footprint calculations are provided to herd owners as part of the membership to the Sustainable Assurance Schemes.

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:

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 (1); Section 13 (2)(a)(V) ; (VII) and (VIII) refer	(V) to facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being 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:

i. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e))

LEGISLATION	DESCRIPTION
Legal Ground from 5.1.2 (i) or (ii) here]	Not Applicable – there is no further processing

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	☒	Tag and herd numbers which can identify individuals]
Classes of Data Subjects	☒	Herd owners, farmers

Table 7.0

8. Duration and Frequency

8.1 Duration

Define the start and end dates of the information transfer:

i. This Data Sharing Agreement will commence on 29/09/2022 and will continue until the parties agree to terminate the 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	☒	Transfer is required on an ongoing basis

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
Bord Bia	Data provided from the Department's AIMs database following the receipt of consent from the herd owners concerned. Bord Bia- Bord Bia Carbon Footprint Tool. AIMs data used in the calculation of Carbon Footprint calculations released to the herd owner.

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
Bord Bia	No further processing will take place.

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
Department of Agriculture Food and the Marine **Bord Bia**	The data provided by the Department is to be used solely for the purpose for which it is provided and as set out in this document. It should not be used for further analysis and should only be provided to those parties for which the purpose has been set out in this document.

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.	☒	☐
		Data is sent from DAFM to Bord Bia using a secure process. The data is encrypted and data can only be decrypted by the intended recipient.	

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.
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

11.2.1.3 SECURITY SPECIALIST FOR LEAD AGENCY	YES/NO
Please confirm your security specialist has reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.2

11.2.2 Party/Parties Receiving Data

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

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

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

11.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1	**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 controls are in place to restrict access to Personal Data to only users who require access for a specified and legitimate purpose. Only members of the Quality Assurance Team and only nominated authorised persons have access to the shared Personal Data. Access controls and permissions are reviewed regularly and updated as required. Bord Bia operates a password management policy and has identity and access management procedures as well. Employees are informed of their responsibilities under Data Protection Law and trained regularly.		
11.2.2.2	**Appropriate controls are in place if the disclosed data is accessed remotely.** Please provide details.	☒	☐	☐
		Bord Bia has a secure remote access system in place to access Bord Bia's network which requires multi factor authentication.		

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.	☒	☐	☐
		Access to information is granted on a need only basis. Staff are granted specific access to allow them to carry out their job functions. A manager or delegate must approve access to data on the network. This process is outlined in the Identity and Access Management Policy and Guidelines and covers approval for access. A request must be logged with the Helpdesk IT Team and the requestor.		
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.	☒	☐	☐
		Both the DAFM and Bord Bia implement multiple cybersecurity protocols and measures. As a matter of policy, neither party disclose details of systems and processes which could in any way compromise their information security posture. In particular, it is not considered appropriate to disclose information on the cyber activities and the resourcing of same for both security and operational reasons.		
11.2.2.5	**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.	☒	☐	☐
			Bord Bia owned laptops and internal hard drives are encrypted by the IT Helpdesk Team. All provided mobile devices that host Bord Bia data are protected by encryption and layered authentication where appropriate. Implementation of	

			Mobile Device Management (MDM) is applied to all mobile devices.	
11.2.2.6	**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.	☒	☐	☐
		Appropriate security measures and policies are in place and regularly reviewed. Bord Bia operates an acceptable use policy which users of the network and Bord Bia's IT assets must sign up to. As stated above, Employees are informed of their responsibilities under Data Protection Law and trained regularly. ICT Security and GDPR training campaigns are run each quarter and cover a range of IT Security topics and GDPR.		
11.2.2.7	**Do you have policy in place that protects data from accidental erasure or other loss?** Please provide details.	Disaster recovery and backup Data is maintained to ensure the availability and ability to restore the Data.		
11.2.2.8	**Is data stored in a secure location only for as long as necessary and then securely erased?** Please provide details.	Backed up data is located in a secure data hosting environment and is part of the managed services provided. Data is backed up currently for 7 or 10 years depending on data type. IT does not delete or erase any data unless instructed by Head of Corporate Services.		

Table 11.2.3

11.2.2.9 – SECURITY STATEMENT
Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures. You may also provide details of additional measures in place that are relevant to this arrangement.
The AIMs data from the export files provided by DAFM is imported into a Bord Bia server which is in a fully locked-down environment with restricted access to key personnel only. It is also subject to independent security audits via annual penetration testing**.** The export files are deleted immediately when the import is complete. Within the server, the data is accessible only for the authorised purpose on the form signed by the producer. The web application accessing the data is strictly coded within the stated purpose of the data, and the Bord Bia management team and software development team are all aware of the restrictions of the use of the data. The server is securely backed up in accordance with Bord Bia's IT backup policy.

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	10 years for EU auditing purposes.
2. Information resulting from the processing of the data	10 years for EU auditing purposes.

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	Any manual files created at any stage of this processing activity are securely disposed of or destroyed where the copies of Personal Data are no longer necessary to be retained.
2. Information resulting from processing of the data	Secure deletion from the Quality Assurance database once the retention period has been met. Any manual files created at any stage of this processing activity are securely disposed of or destroyed where the copies of Personal Data are no longer necessary to be retained.

Table 13.0

14. Withdrawal from Agreement

14.1 Procedure

Each Party commits to giving a minimum of six months 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.

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]	☐	(To include a summary of the matters referred to in Article 35(7) GDPR) The summary shall contain at least: 1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; 2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes; 3. an assessment of the risks to the rights and freedoms of data subjects; 4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
Has not been conducted [select appropriately]	☒	Outline why a DPIA has not been conducted. Include reference to the checklist answers in Section 1. It was not necessary to conduct a Data Protection Impact Assessment (DPIA) in respect of the data sharing of AIMs data independently as the data being processed did not pose a high risk to the rights and freedoms of individuals, only minimal personal data is being processed and there is no special category data or criminal data being processed. With respect to Section 1 and the linked DPC guidance, it is clear that the data sharing activity does not meet the threshold for conducting a DPIA, with no novel technology involved, no automated decision making being undertaken, no profiling of individuals being conducted. Furthermore, the data subjects will have an expectation that this activity will be undertaken and calculations are shared back with the data subjects. In addition, and as set out in Section 11, appropriate security measures are in place to protect the data during and post transfer. It should be noted however, that a DPIA was conducted on the Carbon Footprint process which utilises AIMs data in the calculation of emissions and sustainability calculations.

		This DPIA assessed the data flows, uses and processor used to deliver the Carbon Footprint tool. A finding within this DPIA was to ensure that written agreements are in place to govern the data sharing between DAFM and Bord Bia.

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.

(1) The Personal Data processed is necessary for the assessments and validation carried out by Bord Bia in support of its statutory remit. The Personal Data received within the AIMs data transfer has been assessed to be proportionate to meeting the objectives of Bord Bia's activities.

(2) The objectives of the processing carried out by Bord Bia is undertaken to support Bord Bia's Public Task by producing calculations in the support of reductions of carbon emissions and to demonstrate and analyse the integrity of the livestock sample.

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.

Personal Data contained within the AIMs transfer is limited to herd numbers and tag numbers which provide unique identifiers of livestock, which in turn can identify natural persons associated with these numbers.

Personal Data shall be kept secure through the implementation of appropriate security measures and safeguards.

Appropriate security measures and policies are in place and regularly reviewed.

Personal Data is deleted or securely disposed or destroyed in accordance with the retention schedule as implemented by Bord Bia.

Access controls are in place to restrict access to Personal Data to only users who require access for a specified and legitimate purpose.

Only members of the Quality Assurance Team and only nominated authorised persons have access to the shared Personal Data.

Employees are informed of their responsibilities under Data Protection Law and trained regularly.

IT and Security measures are in place to protect Personal Data stored in electronic form such as encryption of Personal Data, restriction and monitoring of network access and usage. Access controls and permissions are reviewed regularly and updated as required. Disaster recovery and backup Data is maintained to ensure the availability and ability to restore the Data.

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, in particular for any information addressed specifically to a child. [2]The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. [3]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.

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.

- Bord Bia
- DAFM

19. Authorised Signatory

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

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

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

19.1 Lead Agency

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

Table 19 .0

19.2 Other Party/Parties

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

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:	Dr. Filippo Marchetti (On behalf of Trilateral Research)	**Date:**	31/08/2022
Print Name:	Trilateral Research Ltd		
Position:	Data Protection Officer		
Email:	Filippo.marchetti@trilateralresearch.com		
For and on behalf of:	Bord Bia		

Table 19.2

Other Party/Parties DPO Statement

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:**	31/08/2022
Print Name:	Caitriona McEvoy		
Position:	Data Protection Officer		
Email:	dataprotectionofficer@agriculture.gov.ie		
For and on behalf of:	The Department for Agriculture, Food and the Marine		

Table 19.3