



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

Verifying membership in a Bord Bia Scheme which is a prerequisite to establish eligibility for a DAFM programme or 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 | 11 |
| 4. Function of the Parties..... | 13 |
| 5. Legal Basis..... | 14 |
| 6. Impetus for Data Sharing..... | 16 |
| 7. Categories of Data Shared | 17 |
| 8. Duration and Frequency | 18 |
| 9. How data will be processed..... | 19 |
| 10. Restrictions..... | 20 |
| 11. Security Measures | 21 |
| 12. Retention | 29 |
| 13. Methods Used to Destroy/Delete Data..... | 30 |
| 14. Withdrawal from Agreement..... | 31 |
| 15. Other Matters..... | 32 |
| 16. Schedule A - Data Protection Impact Assessment..... | 34 |
| 17. Schedule B | 35 |
| 18. Schedule C | 36 |
| 19. Authorised Signatory | 37 |
| Data Protection Officers Statement | 38 |



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 |
|--|---|
| The Department of Agriculture, Food and the Marine | Agriculture House, Kildare Street, D02 WK12 |

AND

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

| PARTY NAME | ADDRESS |
|------------|--|
| Bord Bia | 140 Pembroke Road, Dublin 4, Ireland D04 NV34 |

The Parties hereby agree that the Department for Agriculture, Food and the Marine 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 effect¹.

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

Table 1.4

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

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

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



2. Purpose of the Data Sharing

2.1 Framework

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

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

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

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

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

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



2.2 Performance of a Function

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

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

Table 2.2

2.3 Details about the Purpose

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

| PURPOSE | DESCRIPTION |
|---------|--|
| | <p>DAFM is responsible for the provision of income supports and funding to farmers for participation in DAFM operated programmes and schemes funded under the EU Common Agricultural Policy or directly funded by the exchequer.</p> <p>The eligibility criteria for these programmes or schemes includes membership in a Bord Bia Quality Assurance Scheme.</p> <p>The Bord Bia Quality Assurance Schemes (QA Schemes) are based on sustainability principles and operated by Bord Bia. Through measurement and analysis, the QA Schemes demonstrate the sustainability of Irish farming at individual farm level and provide constructive feedback to farmers to</p> |



| | |
|---|---|
| | <p>help them with decision making aimed at improving their sustainability performance.</p> <p>The eligibility criteria for participation in DAFM funding schemes requires proof of application and membership in a Bord Bia quality assurance scheme.</p> <p>The purpose of this proposed data sharing agreement between DAFM and Bord Bia is to:</p> <ul style="list-style-type: none">• allow Bord Bia to verify whether an applicant for a DAFM funding scheme is a member of a Bord Bia quality assurance scheme; and -• allow DAFM to then verify compliance with the terms and conditions of its funding scheme. |
| <p>(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</p> | <p>To make the process of confirming eligibility less burdensome for farmers and to avoid any potential fraud, DAFM, in consultation with Bord Bia determined direct validation, ensures the highest level of control over spending of public funds while simultaneously minimising the administrative burden on applicants. </p> |
| <p>(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</p> | <p>Herd/flock/producer number will be the sole personal identifier shared from DAFM to Bord Bia. Following validation of participation in a QA Scheme, Bord Bia will produce a report to share back with DAFM that verifies the status of each applicant's membership in a Bord Bia QA Scheme. This removes the requirement for farmers to provide individual evidence of membership in a Bord Bia scheme. It also ensures accuracy of information. </p> |



| | |
|--|--|
| <p>(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</p> | <p>Bord Bia may also use the generated report to prioritise audits to ensure DAFM programme/scheme applicants obtain or maintain membership in order to avail of the DAFM programme/scheme and receive the associated funding. This will also ensure the timely payment of support to all farmers by DAFM. </p> |
|--|--|

Table 2.3



3. Data to be shared

3.1 Quality

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

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

3.2 Subject Rights

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

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

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

3.3 Sharing with Third Parties

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

3.4 Detail of the information to be disclosed

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

Note:

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

| | DESCRIPTION |
|----------------------|--|
| Shared Personal Data | <ul style="list-style-type: none">Herd/flock/producer number which is linked to a farmer.Status of membership of the herd/flock/producer owner in the relevant Bord Bia QA Scheme. <p>A natural person can be associated with data which uniquely identifies livestock (i.e., herd, flock or producer numbers). These numbers may identify an owner or person associated with the unique identifier of the animal. In this case, both DAFM and Bord</p> |



| | |
|--------------------------|--|
| | Bia have access to data which can directly link a herd/flock owner/producer to a herd/flock/producer number. |
| Non-personal Data | (No other data shared) |

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 |
|---------------------------|---|
| <p>i. Bord Bia</p> | <p>DAFM will disclose the herd/flock/producer numbers which are linked to the owner (farmer). This will indicate who has applied for the DAFM programme/scheme. Bord Bia will disclose the QAe Scheme membership status to DAFM which is associated with the herd/flock/producer number provided.</p> <p>Both parties will be disclosing data. However, the purpose of the data being sent from DAFM to Bord Bia is to facilitate the administration of DAFM Schemes. Bord Bia may prioritise audits for entry to, or maintenance of membership to, its QA Schemes but this is solely to ensure that eligibility for DAFM Schemes is not being hindered by Bord Bia.</p> <p>Bord Bia administers its own Schemes in accordance with the An Bord Bia Act 1994, as amended, in order to fulfil its statutory purpose in line with Section 7 of the Bord Bia (Amendment) Act 2004.</p> |
| <p>ii. DAFM</p> | <p>DAFM will receive the QA Scheme membership status from Bord Bia associated with the herd/flock/producer number. This will be used to verify the eligibility of the applicant to DAFM Schemes where a criterion is Bord Bia QA Scheme membership. DAFM beef schemes are currently operated under the following legal bases:</p> <p>EU Regulations 2021/2115 & 2021/2116, and the Ministers and Secretaries Act 1924. (Additional schemes may be added in the future at the discretion of the Minister and in consultation with the Department of Public Expenditure and Reform.)</p> |

Table 4.1



5. Legal Basis

5.1 Legal Grounds

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

5.1.1 Appropriate Legislative Provisions for Sharing

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

- i. [processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e)) *[delete if not appropriate]*]

Specify the legal obligation for sharing in the table below.

| LEGISLATION | DESCRIPTION |
|--|--|
| <p>Section 13 (2)(a)(III),(IV),(V)</p> | <p>13(2)(a)(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 the mentioned public bodies needs to collect the personal data directly from that person.</p> <p>13(2)(a)(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.</p> <p>13(2)(a)(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.</p> <p>The sharing of data is to confirm eligibility to DAFM Schemes where the membership of a Bord Bia QA Schemes is a prerequisite for eligibility (13(2)(a)(IV))(13(2)(a)(V)). It would be possible to confirm eligibility directly with herd/flock owners and producers. However, this would be more cumbersome for both DAFM and the individuals applying for the DAFM Scheme (13(2)(a)(III)). It would also mean</p> |



| | |
|--|--|
| | DAFM would have to seek more data from these individuals directly to prove membership. As such, the process outlined in this agreement is in line with the principle of data minimisation. |
|--|--|

Table 5.1.1

5.1.2 Appropriate Legislative Provisions for Further Processing

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

- ii. |processing is necessary for compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (c)) *[delete if not appropriate]*
- iii. 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)) *[delete if not appropriate]* |

| LEGISLATION | DESCRIPTION |
|--|--|
| Insert relevant legal ground from 5.1.2 (i) or (ii) here | Data is processed in accordance with EU Regulations 2021/2115, 2021/2116 and also the Ministers and Secretaries Act, 1924. |

Table 5.1.2



6. Impetus for Data Sharing

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

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

Table 6.0



7. Categories of Data Shared

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

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

Select from the below table and comment as appropriate.

| CATEGORY | | COMMENT |
|--------------------------|-------------------------------------|--|
| Individual Data Subject | <input checked="" type="checkbox"/> | Livestock identifiers e.g. herd/flock/producer numbers that are linked to an individual owner. |
| Classes of Data Subjects | <input checked="" type="checkbox"/> | Farmers: Herd owners, flock owners, producers or other owners of livestock. |

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 14-09-2023 and continue until the parties agree to terminate the agreement.

[Delete as appropriate]

8.2 Frequency

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

| TYPE | | DESCRIPTION |
|--------------------------|-------------------------------------|--|
| Once off | <input type="checkbox"/> | |
| Frequent/regular updates | <input checked="" type="checkbox"/> | For each DAFM programme/scheme which requires Bord Bia QA Scheme membership as a condition of participation, data will be shared periodically in bulk, for example, once for each DAFM programme/scheme applicant per payment/per month. |
| Other frequency | <input type="checkbox"/> | |

Table 8.2



9. How data will be processed

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

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

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

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

9.2 Description of Processing

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

| DESCRIPTION OF PROCESSING | |
|---------------------------|---|
| Both parties | <p>DAFM intends to use the Bord Bia QA Scheme Membership status to confirm eligibility for its programmes/schemes.</p> <p>In instances where membership to a Bord Bia Scheme is required in order to avail of funding from DAFM, DAFM will send Bord Bia a list of herd/flock/producer numbers of the applicants for funding. Bord Bia will check the Bord Bia Scheme membership status associated with the number and return a report to DAFM which will state whether the number is a) associated with an existing membership, b) not associated with a membership or c) pending membership (has applied but not yet a member). This will be used by DAFM to confirm eligibility to its schemes.</p> <p>For pending memberships, Bord Bia may use the numbers received from DAFM to prioritise applications to its own QA Schemes. This is to assist the herd/flock owner or producer with meeting the criterion set out in the DAFM funding to ensure they are able to avail of the funding.</p> |

Table 9.2

9.3 Further Processing

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

| SPECIFY FURTHER PROCESSING | |
|----------------------------|-----|
| | N/A |

Table 9.3.1



10. Restrictions

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

| RESTRICTIONS ON DISCLOSURE AFTER PROCESSING | |
|---|---|
| All parties | <p>Bord Bia will already have herd, flock and producer numbers for its own purposes. However, the numbers that DAFM shares with Bord Bia reflect the individuals who have applied for a specific DAFM funding programme/scheme. Bord Bia will not use this information for any purpose other than to verify membership and for its own auditing purposes to facilitate the ability of a farmer/producer to participate in a DAFM funding programme/scheme.</p> <p>The report provided by Bord Bia will not be used for any purpose other than to verify status in a Bord Bia QA Scheme in order to determine eligibility in the DAFM funding programmes/schemes which has been applied for.</p> |

Table 10.0



11. Security Measures

11.1 Security and Training

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

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

This may include, but is not limited to:

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

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

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

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

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

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



11.2 Security Measures

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

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

11.2.1 Lead Agency/ Party Disclosing Data

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

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

| 11.2.1.1 TRANSMISSION | | COMPLIES | DOES NOT COMPLY |
|---|--|--|--------------------------|
| When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use. Please provide details. | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | | Data is sent from Bord Bia to DAFM using a secure process. | |

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 | <p>In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.</p> <p>Please provide details for all non-complying or 'not applicable' statements.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | | <p>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 Bord Bia 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 legislation and trained regularly.</p> <p>In DAFM, access controls are in place where any SCEP users accessing data must have the appropriate permission to do so. These</p> | | |



| | | | |
|----------|--|---|---|
| | | | permissions are periodically revalidated. |
| 11.2.2.2 | <p>Appropriate controls are in place if the disclosed data is accessed remotely.</p> <p>Please provide details.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | | <p>Bord Bia has a secure remote access system in place to access Bord Bia's network which requires multi factor authentication.</p> <p>Any information accessed remotely is done via secure channels to DAFM's systems, utilising multi factor authentication </p> | |
| 11.2.2.3 | <p>A least privileged principle (or similar) is in place to ensure that users are authenticated proportionate with the level of risk associated to the access of the data.</p> <p>Please provide details.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | | <p>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.</p> <p>In DAFM, only certain members of staff in the 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 </p> | |
| 11.2.2.4 | <p>Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).</p> <p>Please provide details of the protections in place and how they are managed.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | | <p>Both the DAFM and Bord Bia implement multiple cybersecurity protocols and measures. As a matter of policy, neither party discloses 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</p> | |



| | | | | |
|----------|---|--|--------------------------|--------------------------|
| | | resourcing of same for both security and operational reasons. | | |
| 11.2.2.5 | <p>Data is encrypted at rest on mobile devices such as laptops and removable media.</p> <p>Please provide details for all non-complying or 'not applicable' statements.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | | <p>Bord Bia owned laptops and internal hard drives are encrypted by the IT Helpdesk Team.</p> <p>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.</p> | | |
| 11.2.2.6 | <p>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.</p> <p>Please provide details.</p> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | | <p>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.</p> <p>ICT Security and GDPR training campaigns are run each quarter and cover a range of IT Security topics and GDPR</p> <p>All Department of Agriculture, Food and the Marine staff receive regular training through</p> | | |



| | | |
|------------------------|--|--|
| | | <p>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 an on-line system.]</p> |
| <p>11.2.2.7</p> | <p>Do you have policy in place that protects data from accidental erasure or other loss?</p> <p>Please provide details.</p> | <p>[Disaster recovery and backup Data is maintained to ensure the availability and ability to restore the Data</p> <p>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:</p> <p>There are several reasons for having an effective Backup and Recovery procedure for Computer-based information.</p> <ul style="list-style-type: none"> ○ 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. <p>DAFM's Backup and Recovery regime must provide for recovery of the most recent possible data in all situations.]</p> |
| <p>11.2.2.8</p> | <p>Is data stored in a secure location only for as long as necessary and then securely erased?</p> <p>Please provide details.</p> | <p>[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.</p> |



| | | |
|--|--|---|
| | | <p>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. </p> |
|--|--|---|

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.



Include details of archiving policies or standards in place.

Include details of any further security auditing policies in place.

Include details of any Information Security Management standards currently in place e.g. ISO27001 Bord Bia

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 11.2.4

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 | Bord Bia will retain the list of herd/flock/other numbers received from DAFM for 10 years for auditing purposes. |
| 2. Information resulting from the processing of the data | DAFM will retain the data containing the herd/flock/other numbers and the associated Bord Bia QA Scheme Membership Status for 10 years. |

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 Bord Bia QA 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. The secure destruction / deletion of files will be in line with the policy of the Direct Payments Division in DAFM who manage the schemes. |

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 OGCI0. Each of the proposed parties will be required to publish, on the same date as the consultation, a notice on their website that they are proposing to enter into the DSA. They should state the documents that are accessible to the public and link to their relevant DSA and DPO statements published on the public consultations website. This notice should invite submissions and include the date of publication of the notice.



15.5.2 Publishing Executed DSA

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

15.6 Base Registries

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



16. Schedule A - Data Protection Impact Assessment

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

OR

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

| DPIA | Select | SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT |
|------------------------|-------------------------------------|--|
| Has been conducted | <input type="checkbox"/> | |
| Has not been conducted | <input checked="" type="checkbox"/> | <p>Outline why a DPIA has not been conducted. Include reference to the checklist answers in Section 1.</p> <p>There is no high risk data processing envisioned. The data shared is very low risk and farmers will be aware that this data will be shared as they will have confirmed their Quality Assurance Scheme Membership status with DAFM when applying for the Scheme. Furthermore both the herd/flock numbers and the membership status are shared with other stakeholders by the farmer frequently so there are no real confidentiality concerns related to the data.</p> <p>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.</p> |

Table 16.0

Note: If the Data Sharing Agreement is amended to reflect a change in the scope, form or content of the data processing, then there is an obligation on the data controllers to consider whether the changes give rise to a high risk to the rights and freedoms of natural persons, such that a DPIA should be carried out.

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



17. Schedule B

17.1 Necessary for the Performance of a Function

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

DAFM is responsible for the provision of income and market supports to underpin the rural economy and the environment through the administration of a variety of schemes. The sharing of data with Bord Bia is to confirm eligibility to DAFM Schemes where the membership of a Bord Bia Quality Assurance Schemes is a prerequisite for eligibility (13(2)(a)(IV))(13(2)(a)(V)) in these schemes and programmes.

Upon confirmation from Bord Bia that the participant(s) are compliant, such as that they are a member of a Bord Bia Quality Assurance Scheme like SBLAS, DAFM will then consider the applicant compliant with this eligibility requirement. The necessary confirmation of eligibility allows DAFM to carry out its functions in making timely payments while ensuring public funds are appropriately safeguarded.

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.

1.1 Minimal personal data is shared. Data is being shared for a specific purpose. There are security measures in place to protect personal data shared. Sharing is being conducted in a transparent manner and data subjects will be aware of their rights. The data will be managed and processed by DAFM and Bord Bia in accordance with each organisation's obligations under the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation and in the light of operational experience to ensure (among other things) that:

- a) appropriate security arrangements are in place and regularly reviewed,
- b) retention and disposal policy are regularly reviewed,
- c) data shared is adequate and not excessive for the declared purposes, and,
- d) data will be suitably destroyed when no longer needed for the purposes for which it was provided for under this agreement.

1.2 The Department of Agriculture, Food and the Marine will provide Bord Bia with the herd/flock/producer number data of applicants to a scheme, through transfer via a secure server with access restricted to a limited number of people. The file will be password protected before transfer. Bord Bia will then respond with report sent to DAFM to confirm if the participants are active members i.e. Yes / No.



1.3 Bord Bia will then revert with the verification check marked on the file. Processing of this file will be access restricted to a limited number of people who are directly involved in administering the QA Scheme. It will be password protected before transmission to DAFM.

1.4 On receipt of the data in DAFM it will be stored in a restricted access area.]

18. Schedule C

18.1 List of Parties to this Agreement

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

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

- The Department of Agriculture, Food and the Marine
- Bord Bia



19. Authorised Signatory

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

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

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

19.1 Lead Agency

| LEAD AGENCY | |
|-----------------------|--|
| Signature: | Date: |
| Print Name: | |
| Position held: | [[Insert position of Authorised Signatory] |
| Email: | |
| For and on behalf of: | [[Department of Agriculture, Food and the Marine |

Table 19.1

19.2 Other Party/Parties

| OTHER PARTY | |
|-----------------------|-----------------------------|
| Signature: | Date: |
| Print Name: | Susan McDonnell |
| Position held; | Director Corporate Services |
| Email: | Susan.mcdonnell@bordbia.ie |
| For and on behalf of: | Bord Bia |

Table 19.2



Data Protection Officers Statement

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

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

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

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

Lead Agency DPO Statement

| LEAD AGENCY DATA PROTECTION OFFICERS STATEMENT | | | |
|--|--|---|----------|
| I have reviewed the proposed agreement | | [<input checked="" type="checkbox"/>] | |
| I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law | | [<input checked="" type="checkbox"/>] | |
| I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation | | [<input checked="" type="checkbox"/>] | |
| Signature: | Caitriona McEvoy | Date: | 26.07.23 |
| Print Name: | Caitriona McEvoy | | |
| Position: | Data Protection Officer | | |
| Email: | caitriona.mcevoy@agriculture.gov.ie | | |
| For and on behalf of: | Department of Agriculture, Food and the Marine | | |

Table 20.1



Other Party/Parties DPO Statement

| OTHER PARTY DATA PROTECTION OFFICER STATEMENT | | | |
|--|--|-------|-------------------------------------|
| I have reviewed the proposed agreement | | | <input checked="" type="checkbox"/> |
| I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law | | | <input checked="" type="checkbox"/> |
| I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation | | | <input checked="" type="checkbox"/> |
| Signature: | Filippo Marchetti | Date: | July 26 th , 2023 |
| Print Name: | Filippo Marchetti | | |
| Position: | Data Protection Officer | | |
| Email: | Filippo.marchetti@trilateralresearch.com | | |
| For and on behalf of: | Bord Bia | | |

Table 20.2