



# **DRAFT**

# **DATA SHARING AGREEMENT**

## **Between**

**The Department of Foreign Affairs  
and  
The Health Service Executive**

## **Pursuant to**

**The Data Sharing and Governance Act 2019**

## **For the purpose of**

**Providing the signed undertaking, received by the Department of Foreign Affairs (DFA) in the course of an Emergency Travel Certificate (ETC) Application, to the Health Service Executive to assist it in the provision of healthcare services that may be required by children born through international surrogacy once they arrive in Ireland.**



## Table of Contents

---

<b>Interpretation Table .....</b>	<b>3</b>
<b>Data Sharing Agreement.....</b>	<b>4</b>
<b>1. Evaluation for a Data Protection Impact Assessment (DPIA).....</b>	<b>5</b>
<b>2. Purpose of the Data Sharing .....</b>	<b>7</b>
<b>3. Data to be shared .....</b>	<b>10</b>
<b>4. Function of the Parties.....</b>	<b>12</b>
<b>5. Legal Basis.....</b>	<b>13</b>
<b>6. Impetus for Data Sharing.....</b>	<b>15</b>
<b>7. Categories of Data Shared .....</b>	<b>16</b>
<b>8. Duration and Frequency .....</b>	<b>17</b>
<b>9. How data will be processed.....</b>	<b>18</b>
<b>10. Restrictions.....</b>	<b>19</b>
<b>11. Security Measures .....</b>	<b>20</b>
<b>12. Retention .....</b>	<b>25</b>
<b>13. Methods Used to Destroy/Delete Data.....</b>	<b>26</b>
<b>14. Withdrawal from Agreement.....</b>	<b>27</b>
<b>15. Other Matters.....</b>	<b>28</b>
<b>16. Schedule A - Data Protection Impact Assessment.....</b>	<b>30</b>
<b>17. Schedule B .....</b>	<b>31</b>
<b>18. Schedule C .....</b>	<b>32</b>
<b>19. Authorised Signatory .....</b>	<b>33</b>
<b>Data Protection Officers Statement .....</b>	<b>34</b>



## Interpretation Table

DEFINITION	MEANING
<b>Data controller</b>	Has the meaning given to it by the General Data Protection Regulation (2016/679).
<b>Party disclosing data</b>	Shall mean the Party transferring personal data to the receiving Party or Parties.
<b>Party receiving data</b>	Shall mean the Party receiving personal data from the Party disclosing data.
<b>Data Protection Impact Assessment(DPIA)</b>	Means an assessment carried out for the purposes of <a href="#">Article 35</a> of the General Data Protection Regulation.
<b>GDPR</b>	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.
<b>Lead Agency</b>	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.
<b>Personal Data</b>	Has the meaning given to it by the General Data Protection Regulation (2016/679).
<b>Personal data breach</b>	Has the meaning given to it by the General Data Protection Regulation (2016/679).
<b>Processing</b>	Has the meaning given to it by the General Data Protection Regulation (2016/679).
<b>Public Service Body (PSB)</b>	Means a Public Body as defined by section 10 of the Data Sharing and Governance Act 2019.
<b>Shared personal data</b>	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
<b>The Department of Foreign Affairs</b>	Iveagh House, 80 St. Stephen's Green, Dublin 2

## AND

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

PARTY NAME	ADDRESS
<b>Health Service Executive</b>	Dr. Steevens Hospital, Steevens Lane, Dublin 8

The Parties hereby agree that The Department of Foreign Affairs 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?	<input type="text" value="YES"/>

Table 1.1

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

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.2	A new purpose for which personal data is processed?	<input type="text" value="Choose Y/N"/>
1.1.3	The introduction of new types of technology?	<input type="text" value="Choose Y/N"/>

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?	<input type="text" value="Choose Y/N"/>

Table 1.3

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



## 1.2 Further Considerations

There are limited circumstances where a mandatory DPIA should be carried out, even where processing was underway prior to the GDPR coming into effect<sup>1</sup>.

	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 <a href="#">Article 35(1)</a>:</p> <p><u><a href="#">Lists of Types of Data Processing Operations which require a DPIA.</a></u></p> <p>(if this hyperlink does not work, use the following url: <a href="https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf">https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf</a>)</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.

<sup>1</sup> <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 checked="" 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 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
Table 2.2 – I, IV and V	<p>The DFA can issue Emergency Travel Certificates (ETCs) to persons meeting the relevant criteria necessary to obtain such certificates under the Passports Act 2008, as amended.</p> <p>This Data Sharing Agreement relates to children born outside the state through surrogacy who will travel to Ireland on an ETC. In order to issue an ETC, the DFA must be satisfied as to the identity of the applicant and the identity of their genetic father. As part of the ETC application process, the genetic father signs an undertaking to attend their local Health Service Executive health clinic with their child. He also acknowledges that the DFA will share this undertaking with relevant Government Departments, Offices and Agencies which, in the event of failure to comply with</p>



	<p>the undertakings, may take appropriate action to ensure that the child’s best interests are protected.</p> <p>The responsibility for health service provision within a specific geographical area lies with the Community Health Organisation. Therefore the National Primary Care Office will electronically forward the notification to the relevant Community Health Organisation for issue to the relevant primary care disciplines advising that a child is in a specific Primary Care Team (PCT) location to allow appropriate service arrangements.</p> <p>The commissioning adults will be advised by the passport officials that the child should be registered with appropriate services at their local health centre and they should seek access to services. The <u>Department of Justice 2012 guidelines</u> state that the commissioning adults will provide a written undertaking that they will notify their local health centre of the child's presence within two working days on their arrival in the state. In this regard the Primary Care Team will be the first point of contact for the commissioning adult and child and will advise the commissioning adult of the full range of services recommended for the child. Issue of notification from the Community Health Organisation to the relevant PCT members will be progressed without delay in order to avoid confusion when the commissioning adult presents within the timeframe. This will be achieved by confirmation back to the National Primary Care Office that the local Primary Care Team has been thus advised. Local PCT members will need to ensure that the baby is registered for services as is the case for all babies.</p>
--	--

Table 2.3



## 3. Data to be shared

### 3.1 Quality

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

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

### 3.2 Subject Rights

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

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

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

### 3.3 Sharing with Third Parties

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

### 3.4 Detail of the information to be disclosed

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

Note:

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

	DESCRIPTION
Shared Personal Data	<p>Set out the details of the personal data set (the minimum needed for the purposes stated in this Data Sharing Agreement)]</p> <ul style="list-style-type: none"><li>• Applicant Name</li><li>• Applicant Date of Birth</li><li>• Applicant Place of Birth</li><li>• Genetic father's Name</li><li>• Genetic father's Address</li><li>• Date of Travel</li><li>• Undertaking of genetic father</li><li>• Address of Health Clinic</li></ul>



Non-personal Data	N/A
-------------------	-----

*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 Foreign Affairs	The function of the Passport Service in the DFA is to issue Irish passports and Emergency Travel Certificates (ETCs) in line with the Passports Act 2008 as amended. In the case of a child born by international surrogacy the DFA receives an undertaking from the genetic father to assist in applying for ETC. This is in accordance with the principles contained in guidance issued by The Department of Justice in relation to international surrogacy and, in the case of the data shared with the Health Service Executive, to ensure that the child is presented at a Health Service Executive health care centre within agreed timeframes.
ii. HSE	The function of The HSE is to convey information to relevant services in line with data regulations and policy to ensure services are delivered promptly. The HSE will ensure that each child receives all relevant services in a timely manner in line with HSE policy. The HSE will liaise as appropriate with the DFA to ensure all relevant information is effectively communicated to appropriate services and to ensure families can avail of necessary healthcare services.

Table 4.1



## 5. Legal Basis

### 5.1 Legal Grounds

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

#### 5.1.1 Appropriate Legislative Provisions for Sharing

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

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

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
Section 13(2)(a)(ii)(I)	Section 13(2)(a)(ii)(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
Section 13(2)(a)(ii)(IV)	Section 13(2)(a)(ii)(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) and;
Section 13(2)(a)(ii)(V)	Section 13(2)(a)(ii)(V) To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned of the Data Sharing and Governance Act 2019 refers

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:

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
[Insert relevant legal ground from 5.1.2 (i) or (ii) here]	N/A

Table 5.1.2



## 6. Impetus for Data Sharing

---

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

THE IMPETUS FOR THE DISCLOSURE OF DATA WILL COME FROM:	TICK AS APPROPRIATE
i. Data subject	<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"/>	Child born to an Irish citizen genetic father through international surrogacy arrangement Irish citizen genetic father of a child born through international surrogacy arrangement.
Classes of Data Subjects	<input checked="" type="checkbox"/>	Children born to an Irish citizen genetic father through international surrogacy arrangement Irish citizen genetic fathers of children born through international surrogacy arrangement

Table 7.0



## 8. Duration and Frequency

### 8.1 Duration

Define the start and end dates of the information transfer:

[The Data Sharing Agreement will commence on 16 December 2022 and continue until the parties agree to terminate agreement.]

### 8.2 Frequency

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

TYPE		DESCRIPTION
Once off	<input type="checkbox"/>	
Frequent/regular updates	<input type="checkbox"/>	
Other frequency	<input checked="" type="checkbox"/>	The transfer of this data, being the relevant undertaking received by the DFA, will take place once only at the time a child born outside Ireland through international surrogacy travels to Ireland on an ETC after said ETC has been issued by DFA.

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	
HSE	The office of Primary Care Operations in the HSE receives a notification from the DFA in a password protected document. The National Primary Care Operations Office will then issue a letter of notification to the relevant local area/ service through the Office of the Chief Officer in a password protected document. This office will notify relevant local services of the details of the family who are due to present themselves. When the family presents themselves to local services, in line with the written undertaking of the commissioning parent, the local area will respond to the original email back to the Office of Primary Care Operations. Primary Care Operations will share the confirmation from the Chief Officer with the DFA. This concludes the process.

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	
HSE	Data is not further processed beyond original purposes for which it is received.

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 Foreign Affairs	<p>The DFA provides this information to the Health Service Executive, being a signed undertaking from the genetic father of a child born through international surrogacy, to assist it in the provision of healthcare services that may be required by these children following their arrival in Ireland.</p> <p>The personal data should not be processed for any other purpose considered incompatible with this purpose. The persons providing this undertaking are aware that the data contained therein will be shared with the Health Service Executive.</p>

Table 10.0



## 11. Security Measures

---

### 11.1 Security and Training

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

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

This may include, but is not limited to:

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

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

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

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

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

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



## 11.2 Security Measures

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

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

### 11.2.1 Lead Agency/ Party Disclosing Data

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

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

11.2.1.1	TRANSMISSION	COMPLIES	DOES NOT COMPLY
	When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Please provide details.	In relation to data transferred, data is password protected and encrypted whilst being transferred by email and is stored by the recipient, the HSE, in line with its relevant ICT policies.	

Table 11.2.1

11.2.1.2 – SECURITY STATEMENT	
Give an outline of the security measures to be deployed for transmission of personal data, in a manner that does not compromise those security measures.	
You may also provide details of additional measures in place for the sharing of data that are relevant to this arrangement.	
The DFA systems restrict access to the information only to required personnel. Information is transmitted via email through inboxes that are secured and protected by relevant DFA ICT security systems and measures.  The ICT Data Transfer Policy will be applied to the transmission of personal data.	
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>The is outlined in the HSE Access Control Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/access-control-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/access-control-policy.pdf</a>)</p>	
11.2.2.2	<p>Appropriate controls are in place if the disclosed data is accessed remotely.</p> <p>Please provide details.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<p>This is outlined in the HSE Remote Access Control Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/remote-access-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/remote-access-policy.pdf</a>)</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"/>	<input type="checkbox"/>
			<p>This is outlined in the HSE Access Control Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/access-control-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/access-control-policy.pdf</a></p>	



11.2.2.4	<b>Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).</b> Please provide details of the protections in place and how they are managed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	This is outlined in the HSE IT Acceptable Use Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/i-t-acceptable-use-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/i-t-acceptable-use-policy.pdf</a>
11.2.2.5	<b>Data is encrypted at rest on mobile devices such as laptops and removable media.</b> Please provide details for all non-complying or 'not applicable' statements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	This is outlined in the HSE Encryption Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/encryption-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/encryption-policy.pdf</a>
11.2.2.6	<b>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.</b> Please provide details.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>Policy and Controls:</b> This is outlined in the HSE IT Acceptable Use Policy available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/i-t-acceptable-use-policy.pdf">https://www.hse.ie/eng/services/publications/pp/ict/i-t-acceptable-use-policy.pdf</a>  <b>Training:</b> The HSE launched a Cyber Security Awareness training module on HSELand, this training is mandatory for all staff
11.2.2.7	<b>Do you have policy in place that protects data from accidental erasure or other loss?</b> Please provide details.	There are a number of HSE IT Security Policies available from: <a href="https://www.hse.ie/eng/services/publications/pp/ict/">https://www.hse.ie/eng/services/publications/pp/ict/</a>			



<b>11.2.2.8</b>	<b>Is data stored in a secure location only for as long as necessary and then securely erased?</b> Please provide details.	This is outlined in the HSE Record Retention Policy available from: <a href="https://www.hse.ie/eng/gdpr/data-protection-covid-19/record-retention-policy-2013.pdf">https://www.hse.ie/eng/gdpr/data-protection-covid-19/record-retention-policy-2013.pdf</a>
-----------------	---	---

Table 11.2.3

<b>11.2.2.9 – SECURITY STATEMENT</b>	
<b>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.</b>	
You may also provide details of additional measures in place that are relevant to this arrangement.	
The HSE systems restrict access to the information only to required personnel. Information is transmitted via email through inboxes that are secured and protected by relevant HSE ICT security systems and measures as outlined in section 11.2.2 above. implementation and compliance with this policy is the responsibility for each individual HSE Directorate	
<b>11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA</b>	<b>YES/NO</b>
<b>Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.</b>	<b>YES</b>

Table 11.2.4

### 11.3 Data Breaches and Reporting

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



## 12. Retention

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

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

INFORMATION TYPE	RETENTION REQUIREMENTS
1. Information to be disclosed	The DFA is the disclosing body and is subject to the National Archives Act 1986 (as amended) and data is retained in accordance with the provisions of Sections 7 & 8 of the aforementioned Act and in line with the Passport Service Retention Policy. Data is securely held and reviewed after 30 years of issuance of the emergency travel certificate, in line with the Department's obligations under the National Archives Act.]
2. Information resulting from the processing of the data	The HSE is the receiving body. In line with HSE data retention policies Personal data shall not be kept for longer than is necessary for the purposes for which they are retained. The HSE policy states that records of Children and Young people should be retained until their 25 <sup>th</sup> birthday]

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	[The data of the disclosing body will be destroyed in line with internal DFA guidelines and in accordance with guidance received from the National Archives.]
2. Information resulting from processing of the data	[The HSE is the recipient body. The data will be destroyed in line with relevant Health Service Executive Policy.]

Table 13.0



## 14. Withdrawal from Agreement

---

### 14.1 Procedure

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

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

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

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

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

### 14.2 Severance

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



## 15. Other Matters

---

### 15.1 Variation

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

### 15.2 Review of Operation of the Data Sharing Agreement

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

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

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

### 15.3 Jurisdiction

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

### 15.4 Indemnity

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

### 15.5 Publication

#### 15.5.1 Public Consultation and publishing a Notice

Public Consultation is managed on behalf of the parties by the Data Governance Unit in 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		SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT
Has been conducted [select appropriately]	<input type="checkbox"/>	
Has not been conducted [select appropriately]	<input checked="" type="checkbox"/>	<p>A DPIA was not deemed to be necessary as the processing of this data does not adversely impact on the rights and freedoms of the data subject.</p> <p>The DFA, as Lead Agency and in accordance with its own policies and procedures as a Data Controller, has conducted an evaluation in order to determine whether a DPIA is necessary. As part of this evaluation it considered that this processing was in place prior to 25 May 2018, that data is not being processed for a new purpose and no changes to how this data is processed have been made.</p> <p>The processing involves the data of a very small subset of applicants for an Emergency Travel Certificate and that information on the processing, including the sharing of information with the HSE, is available on the DFA website. The DFA and the HSE have applied the principle of data minimisation to the data being transmitted. Given the security measures in place, the means of transmission and subsequent storage any potential risk to the data or individuals is further minimised.</p> <p>It is on this basis that both the DFA and the HSE have concluded that there is not a need to complete a DPIA in relation to this processing.</p>

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.

The function of the Passport Service in the DFA is to issue Irish passports and Emergency Travel Certificates (ETCs) in line with the Passports Act 2008 as amended. In the case of a child born by international surrogacy the DFA receives an undertaking from the genetic father to assist in applying for ETC. This is in accordance with the principles contained in guidance issued by The Department of Justice in relation to international surrogacy and, in the case of the data shared with the Health Service Executive, to ensure that the child is presented at a Health Service Executive health care centre within agreed timeframes.

The function of The HSE is to convey information to relevant services in line with data regulations and policy to ensure services are delivered promptly.

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. The surrogacy notification contains basic demographic details as outlined in section 3. The process of verifying the child / children presented for services cannot be completed without this basic demographic detail and therefore this is necessary to perform the function. This is the minimum dataset required to meet the intended aim and therefore is proportional in this context.

### 17.2 Safeguards

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

The DFA and the Health Service Executive's systems restrict access to the information only to required personnel and the shared information is further protected in transit and at rest by encryption controls. The data is only used for the purposes of performance of a function as outlined in section 4 & 17.1 above. The data received by the HSE is the minimum data set required for the performance of the function and the data is retained and subsequently destroyed in line with HSE policy. The HSE maintain the confidentiality of the data at all times.

All data retained and processed are subject to the DFA's data protection privacy policies.



## 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.

- |  |
|--|
| <ul style="list-style-type: none"><li>• Department of Foreign Affairs</li><li>• Health Service Executive</li></ul> |
|--|



## 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:	[Insert name of organisation ]		

Table 19.0

### 19.2 Other Party/Parties

OTHER PARTY			
Signature:		Date:	
Print Name:			
Position held;	[Insert position of Authorised Signatory]		
Email:			
For and on behalf of:	[Insert name of organisation ]		

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			<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:	Kieran Houlihan	Date:	01/09/2022
Print Name:	KIERAN HOULIHAN		
Position:	Data Protection Officer		
Email:	Data.protection@dfa.ie		
For and on behalf of:	Department of Foreign Affairs		

Table 19.2



## 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:		Date:	01/09/2022
Print Name:	Johnny Farren		
Position:	Interim Acting Data Protection Officer		
Email:	dpo@hse.ie		
For and on behalf of:	Health Service Executive		

Table 19.3

