



DRAFT

DATA SHARING AGREEMENT

Between

**[The Department of Foreign Affairs
and
Department of Social Protection]**

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

**[Identifying next of kin in emergency situations where Irish
Citizens have been seriously injured or died suddenly
abroad]**



Table of Contents

Interpretation Table	3
Data Sharing Agreement.....	4
1. Evaluation for a Data Protection Impact Assessment (DPIA).....	5
2. Purpose of the Data Sharing	7
3. Data to be shared	9
4. Function of the Parties.....	11
5. Legal Basis.....	12
6. Impetus for Data Sharing.....	13
7. Categories of Data Shared	14
8. Duration and Frequency	15
9. How data will be processed.....	16
10. Restrictions.....	17
11. Security Measures	18
12. Retention	23
13. Methods Used to Destroy/Delete Data.....	24
14. Withdrawal from Agreement.....	25
15. Other Matters.....	26
16. Schedule A - Data Protection Impact Assessment.....	28
17. Schedule B	30
18. Schedule C	32
19. Authorised Signatory	33
Data Protection Officers Statement	34



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
Department of Foreign Affairs	Iveagh House, 80 St. Stephens Green, Dublin 2

AND

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

PARTY NAME	ADDRESS
Department of Social Protection	Áras Mhic Dhiarmada, Store St, Dublin 1

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 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><u>Lists of Types of Data Processing Operations which require a DPIA.</u></p> <p>(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)</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 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 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 – V	<p>The Department of Foreign Affairs (DFA) provides consular services for Irish citizens and this activity can necessitate the processing of personal data.</p> <p>Occasionally, in the event of the death or serious injury of an Irish citizen abroad, DFA may be required to identify and provide contact details of next of kin to An Garda Síochána. This is not always possible using only the DFA's dataset.</p> <p>Therefore, in some limited circumstances, DFA requests the General Register Office (GRO) to search and provide some personal data it holds on close relatives of the deceased. This information is then combined with the data held by DFA in order to identify next of kin. An Garda Síochána can then get in contact with the next of kin and inform them of what has happened.</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>When a sudden death or serious injury of an Irish Citizen occurs abroad and there is a difficulty identifying a next of kin, the Department of Foreign Affairs supply the following information to the General Register Office (GRO) (or as much information as is known to Department of Foreign Affairs) to assist with identifying the next of kin:-</p> <ol style="list-style-type: none">1) Name (of Irish Citizen)2) DOB (of Irish Citizen)3) Mothers (of Irish Citizen) birth surname (Or Mother's full details, name, DOB, place of Birth should the Irish



	<p>Citizen have included them on their Passport application)</p> <p>4) PPSN (of Irish Citizen)</p> <p>Although birth, marriage and death certificates are publicly available, given the urgency of the situation, the General Register Office (GRO) can provide when asked a subset of the publicly available information outlined below to assist in locating/contacting next of kin in a timely manner:-</p> <ol style="list-style-type: none">1. Citizen's spouse alive <u>Register of marriages</u>: name of spouse, address at the time of marriage2. Citizen has children, no spouse <u>Register of births</u>: Name of co-parent, address at the time of birth3. Citizen has no spouse, no children <u>Register of births</u>: name of parents, address at the time of birth4. Citizen has no spouse, no children, and parents deceased <u>Register of births</u>: name(s) of siblings, address at the time of birth5. Citizen has children, co-parent deceased <u>Register of births</u>: name(s) of child(ren), address at the time of birth.
Non-personal Data	

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 Social Protection	<p>The Civil Registration Service (GRO) operates under the aegis of the Department of Social Protection.</p> <p>It provides ongoing evidence of life events by means of supplying certificates and verification of events registered and by validating certain life event records to a legal standard.</p> <p>It also ensures that current and historic records are preserved for future enquiry, enabling research and preserving the value of records for future generations.</p> <p>The Civil Registration Act (CRA) 2004 provides for the current system of civil registration and the modern electronic production of life certificates and related information surrounding civil registration.</p>
ii. Department of Foreign Affairs	<p>The Department of Foreign Affairs (DFA) provides assistance to Irish Citizens overseas. The Department's lawful basis for processing personal data to carry out this function is provided by Section 1(xi) of the Ministers and Secretaries Act 1924-2013 and Section 38 (1)(a) of the Data Protection Act 2018.</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))

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
S.13(2)(a)(ii)(V)	To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned.

Table 5.1.1

5.1.2 Appropriate Legislative Provisions for Further Processing

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

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

LEGISLATION	DESCRIPTION
5.1.2 (ii)	Where the legal basis lies in the performance of a legal obligation} 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)) Section 1(xi) of the Ministers and Secretaries Act 1924-2013 and Section 38 (1)(a) of the Data Protection Act 2018.

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 type="checkbox"/>	
Classes of Data Subjects	<input checked="" type="checkbox"/>	Relatives of a deceased or seriously injured person.

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 16/12/2022 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 data will take place only as and when required to establish next of kin details for an Irish Citizen who has suddenly died or seriously injured abroad.

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	
Department of Foreign Affairs	In order to identify the appropriate next of kin, information received from the GRO is used by the authorised officers in the Department of Foreign Affairs to cross-reference with the data already held, including Passport Service data. Once the identity of the appropriate next of kin is established by the Department of Foreign Affairs, this information is then provided to An Garda Síochána.

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	
Department of Foreign Affairs	<p>Data is processed for the specified, explicit and legitimate purpose as set out in Section 9(2) of this agreement. Once the identity of the appropriate next of kin is established by the Department of Foreign Affairs, the information received is then provided to An Garda Síochána for the purposes of notifying the next of kin involved.</p> <p>Data is retained and stored securely in accordance with the Department's obligations under the National Archives Act 1986 (as amended).</p>

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 Social Protection	The information given will be used to identify a next of kin. Once the next of kin has been identified and notified to An Garda Síochána, the data provided should only be used again by the authorised officers in the Department of Foreign Affairs in the event that further investigation is required to identify another relative.

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.	This transmission will follow existing procedures in GRO. Data is contained in an encrypted excel document and the email is encrypted when sent from DSP.	

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 data is recorded in an excel spreadsheet which is password protected and the password is shared with DFA. The email is encrypted when sent to the recipient address using Cisco Secure Envelope (CSE) Technology. The recipient requires a valid DFA email address registered with the CSE service to unencrypt the excel document and the recipient requires the password to open the document.	
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"/>
11.2.2.2	<p>Appropriate controls are in place if the disclosed data is accessed remotely.</p> <p>Please provide details.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
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"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



	Please provide details of the protections in place and how they are managed.	Appropriate use of ICT Resources Policy Removable Storage Media Policy		
11.2.2.5	Data is encrypted at rest on mobile devices such as laptops and removable media. Please provide details for all non-complying or 'not applicable' statements.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> There is no remote/mobile access to the data
11.2.2.6	There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location. Please provide details.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Compulsory Security Awareness Training and Data Protection training for all users. Appropriate use of ICT resources agreement with users.
11.2.2.7	Do you have policy in place that protects data from accidental erasure or other loss? Please provide details.	Yes, the ICT Backup and Recovery Policy will protect data from accidental erasure or loss.		
11.2.2.8	Is data stored in a secure location only for as long as necessary and then securely erased? Please provide details.	Data is stored in a secure location only for as long as necessary and then will be securely erased in accordance with Passport Service Record Management and Retention Policy		

Table 11.2.3

**11.2.2.9 – SECURITY STATEMENT**

Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures.

You may also provide details of additional measures in place that are relevant to this arrangement.

The following policies will be applied to the storage and access of personal data:

User Access Control Policy

Appropriate use of ICT Resources

Removable Storage Media Policy

Personal Data Breach management

ICT Backup and Recovery Policy

ICT Security Policy

Change control Policy

ICT Application Security Policy

ICT Data Transfer Policy

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA**YES/NO**

Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.

YES

Table 11.2.4

11.3 Data Breaches and Reporting

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



12. Retention

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

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

INFORMATION TYPE	RETENTION REQUIREMENTS
1. Information to be disclosed	<p>The information disclosed is information already held in the civil registers of births, deaths and marriages. This information is publicly available.</p> <p>Any requests for information will be retained by GRO, and securely held in our offices in Roscommon. GRO will maintain an index of all requests and the subsequent internal processing requirements for completion of requests for a period of 7 years.</p>
2. Information resulting from the processing of the data	<p>The Department of Foreign Affairs is subject to the National Archives Act 1986 (as amended) and data must be retained in accordance with the provisions of Sections 7 & 8 of the aforementioned Act. Data will be disposed of subject to and in accordance with the relevant certificates of disposal received under S.7 of the National Archives Act 1986 (as amended). Any data processed to which a certificate of disposal issued under S.7 of the National Archives Act 1986 (as amended) does not apply will be securely held and reviewed for possible transfer to the National Archives under S.8 of the aforementioned Act..</p>

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 request will be destroyed in line with Internal DSP Guidelines.
2. Information resulting from processing of the data	The data will be destroyed in line with internal DFA guidelines and will be disposed of in accordance with section 7 of the National Archives Act, 1986.

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>The DFA, as Lead Agency and in accordance with its own policies and procedures as a Data Controller, has considered if a DPIA is necessary in this case.</p> <p>It took into account 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. The information being provided is publicly available. It involves the processing of the personal data of a very small subset of persons (up to 20 per annum) who may become seriously injured or deceased abroad, and their relatives. Information on the potential processing, including the sharing of this information with the GRO as part of DSP, is available on the DFA website.</p> <p>The DFA and the DSP 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>



		It is on this basis that both the DFA and the DSP have concluded that there is not a need to complete a DPIA in relation to this processing.
--	--	--

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 disclosure of information under this agreement is necessary to identify the Next of Kin (NoK) of an Irish Citizen that has suddenly died or is seriously injured abroad.

Part of the role of the DFA is to provide consular assistance to Irish Citizens who are overseas. At times, Missions overseas or the DFA's Citizen Services Division may receive notice from persons or authorities overseas that an Irish Citizen may have become seriously injured or has died suddenly abroad. In some such cases, the NoK of the affected individual may not be known by the authorities or person(s) reporting this matter to the DFA. In such cases, the DFA will review the information it has to hand on its systems and may contact the General Register Office (Department of Social Protection), to cross check information in order to ascertain the correct NoK.

Given the sensitivity of the matter, it is imperative that the correct NoK be identified to avoid any unnecessary sharing of data with An Garda Síochána. An Garda Síochána, having completed its own checks on the data received from the Department of Foreign Affairs, are responsible for notifying the NoK. Given that the information held on DFA systems alone will not always be enough to identify who the individual's NoK is, data received from the General Register Office (Department of Social Protection) may be necessary to provide a link between information held on the deceased or seriously injured individual and the information held on NoK.



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.

In accordance with Article 32 of the GDPR, the parties will 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.

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

Shared personal data shall be limited to the personal data described in this agreement and will be shared only in the manner as set out in this agreement and only for the purposes specified in the agreement.

Appropriate safeguards are in place in respect of data disclosed to DFA and safeguards are also in place for any necessary further disclosure by DFA's to An Garda Síochána. An Garda Síochána will perform its own checks, in advance of notifying next of kin.

Both parties have the appropriate data protection policies in place and have taken the measures to ensure data subjects can exercise their rights under Articles 12 to 22 of the GDPR. |



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.

Department of Foreign Affairs
Department of Social Protection / General Register Office



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:	5/09/22
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

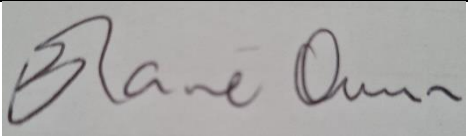
OTHER PARTY DATA PROTECTION OFFICER STATEMENT			
I have reviewed the proposed agreement			<input checked="" type="checkbox"/>
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			<input checked="" 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:	5/09/22
Print Name:	Elaine Quinn		
Position:	Data Protection Officer		
Email:	elaine.quinn@welfare.ie		
For and on behalf of:	Department of Social Protection		

Table 19.3