



DRAFT
DATA SHARING AGREEMENT

Between

**[The Department of Justice]
and**

[The Department of Foreign Affairs]

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

**[Facilitating the processing of passport applications for
persons in receipt of naturalisation certificates]**



Table of Contents

1. Interpretation	3
2. Purpose of the Data Sharing	5
3. Data to be shared	7
4. Function of the Parties	8
5. Legal Basis	9
6. Impetus for Data Sharing	10
7. Categories of Data Shared	11
8. Duration and Frequency	12
9. How data will be processed	13
10. Restrictions	14
11. Security Measures	15
12. Retention	17
13. Methods Used to Destroy/Delete Data	18
14. Withdrawal from Agreement	19
15. Other Matters	20
16. Schedule A - Data Protection Impact Assessment	22
17. Schedule B	23
18. Schedule C	25
19. Authorised Signatory (completed at stage 7)	26
Data Protection Officers Statement	27



1. Interpretation

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

REFERENCE: DOJDFA_001_220203

NAME: DSA for Citizenship Data

BETWEEN

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

LEAD AGENCY NAME	ADDRESS
Department of Justice	51 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
Department of Foreign Affairs	Veagh House, 80 St. Stephen's Green, Dublin 2

The Parties hereby agree that the Department of Justice 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.



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 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
[I & IV above]	<p>The Department of Justice issue Naturalisation Certificates to persons meeting the relevant criteria necessary to obtain such certificates. Based on this certificate, persons will make an application to the Passport Service in the Department of Foreign Affairs for an Irish Passport.</p> <p>In order to issue a Passport, the Minister must be satisfied as to the identity of the applicant and that they are an Irish Citizen. Further the Minister may process such personal data, in respect of an applicant for a passport as are required for the issue of a passport to the applicant and the maintenance of the integrity of the system for issuing passports. The Passport Service uses the information provided to verify the validity of the Naturalisation Certificate received from the applicant.</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 recipient party is notified of inaccurate data by the data subject, this party is obliged to notify the disclosing party.

3.2 Subject Rights

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

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

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

3.3 Sharing with Third Parties

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

3.4 Detail of the information to be disclosed

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

Note:

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

	DESCRIPTION
Shared Personal Data	<ul style="list-style-type: none"> • Naturalisation Certificate Number • Applicant Name • Applicant Date of Birth • Date Certificate Issued • Naturalisation Application Category • Status of Certificate (Issued / Cancelled) • Date Certificate Cancelled (if applicable) • Address Date Address was provided to Citizenship / ISD
Non-personal Data	None

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 Justice]	The function of Citizenship in the Department of Justice is to process applications for naturalisation on behalf of the Minister, along with other functions specified under the Irish Nationality and Citizenship Act 1956 as amended.]
ii. Department of Foreign Affairs]	The function of the Passport Service in the Department of Foreign Affairs is to issue Irish passports in line with the Passports Act 2008 as amended.]

Table 4.1



5. Legal Basis

5.1 Legal Grounds

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

5.1.1 Appropriate Legislative Provisions for Sharing

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

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

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
	S.13(2)(a)(ii)(IV) to establish the entitlement of a person to the provision of a service being delivered by the first or second mentioned public body, on the basis of information previously provided by that person to the first mentioned public body(or another public body that previously disclosed the information to the first mentioned public body).

Table 5.1.1

5.1.2 Appropriate Legislative Provisions for Further Processing

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

- ~~ii. processing is necessary for compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (e)) [delete if not appropriate]~~
- iii. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e)) [delete if not appropriate]

LEGISLATION	DESCRIPTION
[5.1.2 (iii)]	<p>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)).</p> <p>The legislative provisions appropriate to the official authority referred to above are as follows:</p> <p>Sections 7(1)(a) & 8 of the Passports Act 2008 as amended</p>

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"/>	
Classes of Data Subjects	<input checked="" type="checkbox"/>	Only those data subjects issued with a Naturalisation Certificate.

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 31/03/2022 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 checked="" type="checkbox"/>	The transfer of data will take place following every Citizenship Ceremony which takes place twice or three times annually.
Other frequency	<input checked="" type="checkbox"/>	Data transfer on a monthly basis during the COVID pandemic. Occasionally where the Passport Service needs to expedite a passport application may request verification data from DoJ.

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]	Confirming Citizenship of passport applicant and to confirm the validity of a naturalisation certificate in line with the Passports Act 2008, Section 7(1)(a) and Section 8(1).

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]	Data is not further processed beyond original purposes for which 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 Justice	DoJ provides this information to DFA specifically for the purpose of cross-checking information on grants of naturalisation certificates to prevent the fraudulent procurement of Irish passports. The personal data should not be processed for any further purpose. Persons awarded Naturalisation Certificates are advised that their data is shared with DFA.

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 Outlined

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

STEPS	DESCRIPTION
[Insert step here]	The Department of Justice and the Department of Foreign Affairs' systems restrict access to the information only to required personnel and the extracted information is further protected in transit and at rest by encryption controls.

Table 11.2

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	Indefinite due to the possibility of revocation of citizenship.
2. Information resulting from the processing of the data	Standard Passport Retention periods apply to the data. The data will be held for 15 years after the date of passport issuance (the validity of the passport plus five years). After this time it will be marked for destruction and will be destroyed in line with internal guidelines and in accordance with guidance received from the National Archives.

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 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	

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
<p>Has been conducted [select appropriately]</p>	<p>[To include a summary of the matters referred to in Article 35(7) GDPR]</p> <p>The summary shall contain at least:</p> <ol style="list-style-type: none"> 1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; 2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes; 3. an assessment of the risks to the rights and freedoms of data subjects; 4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
<p>Has not been conducted [select appropriately]</p>	<p>[Outline why a DPIA has not been conducted.]</p> <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>

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 entitlement of a person to citizenship is governed by the Irish Nationality and Citizenship Act 1956, as amended (“the 1956 Act”).

The Minister for Foreign Affairs is responsible for the issue of passports to Irish citizens and does so pursuant to the provisions of the Passports Act 2008, as amended (“the 2008 Act”). Section 7 (1) (a) of the 2008 Act provides that:

“Before issuing a passport to a person, the Minister shall be satisfied –

(a) That the person is an Irish citizen, ...”

Section 8 (1) of the 2008 Act further provides that:

(b) “Subject to the Data Protection Regulation and the Act of 2018, the Minister may process such personal data, including biometric data, in respect of an applicant for a passport as are required for the issue of a passport to the applicant and the maintenance of the integrity of the system for issuing passports.”

Passport Service figures show that a high percentage of new Irish citizens who are issued with Naturalisation Certificates by the Department of Justice will apply for a passport.

The Passport Service experiences high demand for first time passports. These first time applications are complex to process and a rigorous process is required to verify the identity and citizenship status of applicants.

The Passport Service is not in a position to verify the authenticity of the naturalisation certificate submitted by the passport applicant with their passport application without access to data held by the Department of Justice. Furthermore, it had come to the attention of the Passport Service that a number of individuals were making applications for Irish passports using Naturalisation Certificates belonging to other people.

The sharing of this personal data by the Department of Justice allows the Passport Service to cross-reference Naturalisation Certificates submitted by passport applicants against Department of Justice naturalisation records. It allows for quick verification of the applicant’s Irish citizenship, streamlining the process and ensuring that the application will be processed within standard turnaround times.

Access to this data from the Department of Justice helps to prevent the issue of Irish passports to people who are not Irish citizens, helping to protect the integrity of the Irish passport, which recently placed 5th on the [2022 Henley Passport Index Global Ranking](#).



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.

DoJ data are held on secure servers and transfer is in a password protected attachment given personal data subject information is involved

Data received is held securely on Passport systems in accordance with the DFA's obligations under Article 32 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 Justice

Department of Foreign Affairs |



19. Authorised Signatory (completed at stage 7)

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

[Append further Authorised Signatory sections for each additional Party, use same format as above 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:	Tara Storey	Date:	24/01/2022
Print Name:	Tara Storey		
Position:	Data Protection Officer		
Email:	dataprotectioncompliance@justice.ie		
For and on behalf of:	Department of Justice		

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:	Kieran Houlihan	Date:	24 January 2022
Print Name:	Kieran Houlihan		
Position:	Data Protection Officer		
Email:	Data.protection@dfa.ie		
For and on behalf of:	Department of Foreign Affairs		

Table 19.3

[]