

**Controller to Controller Data Sharing Agreement in
Respect of Data Sharing**

Between

**Office of the Registrar General (GRO), Department of Social
Protection**

and

The Adoption Authority of Ireland (AAI)

for the

Sharing and Processing of Personal Data

pursuant to

Part 2 of the Birth Information and Tracing Act, 2022

for the purpose of

Enabling adopted persons to receive their birth certificates

Contents

1.	Parties to the Data Sharing Agreement	1
2.	Interpretation	1
3.	Duration	1
4.	Purpose of this Data Sharing Agreement	1
5.	Data Protection Impact Assessment	2
6.	Purpose of the data sharing	2
7.	Functions of the Parties to the Data Sharing Agreement	2
8.	Legal basis for data sharing	3
9.	Categories of Personal Data Shared Under this Agreement	3
10.	Further processing	3
11.	Obligations of the Parties in Respect of Fair and Lawful Processing	3
12.	Data Quality	4
13.	Data Retention and Deletion	4
14.	Sharing with Third Parties	5
15.	Security and Training	5
16.	Data Breaches and Reporting	7
17.	Variation	7
18.	Review of operation of the Data Sharing Agreement	7
19.	Termination	7
20.	Severance	8
21.	Jurisdiction	8
22.	Agreement	8

1. Parties to the Data Sharing Agreement

1.1. The Office of the Registrar General (GRO) with its principal office at Government Offices, Convent Road, Roscommon, F42 VX53

1.2. The Adoption Authority of Ireland (AAI) having its registered address at 3/4 Shelbourne House, Ballsbridge, Dublin 4, D04 H6F6 (together the “Parties”)

2. Interpretation

“**BITA**” means the Birth, Information and Tracing Act 2022

“**data controller**” has the meaning given to it by the General Data Protection Regulation (2016/679)

“**DPA**” refers to the Data Protection Acts 1988 through to 2018.

“**GDPR**” shall be taken as a reference to the General Data Protection Regulation (2016/679) including such legislation as may be enacted by the houses of the Oireachtas in relation thereto.

“**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)

“**special categories of personal data**” has the meaning given to it by the General Data Protection Regulation (2016/679)

“**shared personal data**” means that data shared pursuant to this agreement and listed in the schedule no.1 in this agreement.

3. Duration

The Data Sharing Agreement will remain in place while there are applications from adopted persons under Part 2 of the BITA.

4. Purpose of this Data Sharing Agreement

4.1. 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.

4.2. The purpose of this Data Sharing Agreement is to ensure that any sharing of personal data by the parties pursuant to Part 2 of the BITA is carried out in

accordance with Data Protection Law. The information to include personal data to be shared is more fully described in Part 2 of the BITA.

5. Data Protection Impact Assessment

- 5.1. A data protection impact assessment (“DPIA”) has been conducted by the GRO in respect of the shared personal data and the necessity of the sharing and such sharing goes no further than is necessary for the purposes 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 in schedule no. 1 to this agreement.
- 5.2. The parties agree that the summary of the GRO DPIA is included for information purposes only and that the inclusion of this summary should not be deemed to be an acceptance of the terms of the GRO DPIA by the AAI, as the AAI has its own independent obligations under GDPR in this respect.

6. Purpose of the data sharing

- 6.1. The Parties have determined that the sharing is necessary to meet the Parties' statutory obligations under Part 2 of the Birth Information and Tracing Act 2022.

7. Functions of the Parties to the Data Sharing Agreement

- 7.1. **Description of GRO functions:** Application forms submitted to GRO will be electronically scanned. The designated GRO officer(s) will search the register of births, adoptions register and confidential index in order to locate the applicant's birth registration record.
- 7.2. GRO will complete Form A and send by password protected e-mail to the AAI.
- 7.3. Following receipt of information on the contact preference from the AAI and, if required, the GRO will complete Form B and provide the applicant's contact details to the AAI in order for the AAI to instigate the information session required under the Act.
- 7.4. **Description of AAI functions:** The AAI will use the information received on Form A from the GRO to check their Contact Preference Register. AAI must ensure that they have the correct record for the applicant and to verify if the applicant's birth parent(s) have indicated whether they do or do not want to be contacted by the applicant.
- 7.5. The AAI will indicate on Form A the contact preference and, if an information session with the applicant is required, seek the contact details of the applicant from the GRO to enable the AAI to comply with its obligations under the Act to conduct an information session with the applicant.

7.6. Form B will be completed when the information session is completed and sent to the GRO. The GRO will issue the birth certificate to the applicant once the information session is complete.

8. Legal basis for data sharing

Part 2 of Birth and Information Tracing Act, 2022.

9. Categories of Personal Data Shared Under this Agreement

9.1. The personal data shared by the Parties is set out in Schedule no. 2 to this agreement.

9.2. The personal data shared is in relation to individual data subjects.

10. Further processing

10.1. AAI will not engage in processing of data received from GRO other than to comply with the processes set out in the Birth Information and Tracing Act 2022 or where otherwise required or permitted by applicable law.

10.2. GRO processing of data received from the AAI will be confined to the identification of the birth register record and the issue of a birth certificate or other information / documentation referenced in section 6 of the BITA.

11. Obligations of the Parties in Respect of Fair and Lawful Processing

11.1. Each party will ensure that the shared personal data is processed fairly and lawfully.

11.2. Each party will comply with the requirements of the DPA, GDPR and any legislation amending or extending same, in relation to the data shared.

11.3. Each party undertakes to comply with the principles on data protection set out in Article 5 of the GDPR in the disclosing of information in this Data Sharing Agreement.

11.4. For the purposes identified in this Data Sharing Agreement each party shall ensure that it processes personal data on the basis of one of the following legal grounds:

- processing is necessary for compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (c)).

- 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)).
- 11.5. Both parties shall, in respect of shared personal data, ensure that their privacy notices are clear and provide sufficient information to data subjects in order for them to understand the personal data the parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity with whom the data is shared or a description of the type of organisation that will receive the personal data.
- 11.6. Both parties undertake to inform data subjects of the purposes for which it will process their personal data and provide all of the information that it must provide in accordance with applicable laws, to ensure that the data subjects understand how their personal data will be processed by the data controller.
- 11.7. Each party will notify, as appropriate, data subjects of the following:
- the categories of data shared between the Parties
 - the purpose of the processing of the data
 - the legal basis for processing the data
 - the identity of the GRO as the disclosing party
 - how the data subjects may exercise their data rights
 - other relevant information as set out under Data Protection legislation and the Data Sharing in the Public Sector guidelines produced by the Data Protection Commission.

12. Data Quality

- 12.1. Both parties will provide the most up to date personal data they hold when sharing data.
- 12.2. The AAI acknowledges that, pursuant to Clause 12.1 above, the personal data the AAI receives from the GRO under this Agreement, will be the most up to date personal data that the GRO has available to it.
- 12.3. Shared personal data shall be limited to the personal data described in schedule no. 2 to this agreement and will be shared only in the manner as set out in schedule no. 3 therein.

13. Data Retention and Deletion

- 13.1. Schedule no. 2 specifies the GRO retention periods of (i) the shared personal data and (ii) the information resulting from the processing of that data, which may be updated periodically and notified to the data receiver as appropriate.

- 13.2. At the end of the retention periods set out in schedule no. 2, data will be destroyed in an appropriate, secure manner. (i) The GRO will scan all application forms to the secure network and shred paper applications. (ii) The Birth and Information Tracing
- 13.3. Act requires GRO to verify if an information session has taken place. This verification will be confirmed by the AAI at the GRO request when the application is made. This information will be retained by the GRO for a period of no longer than 7 years to ensure that an applicant can request further certificates without further exchange of personal information with the AAI.
- 13.4. In the event of termination of the Data Sharing Agreement the data will be retained for a period of no longer than 7 years from the date of the application.
- 13.5. For the avoidance of doubt, the parties agree that nothing in this clause 13 or schedule no. 2 shall prevent the AAI from retaining shared personal data for such period as is necessary for the AAI to comply with its obligations under applicable law including but not limited to the BITA and / or the National Archives Act 1986.

14. Sharing with Third Parties

The Parties shall not further share the shared personal data with a third party data controller (a) without the express written permission of the other party (not to be unreasonably withheld) or (b) where so required, facilitated or permitted by the BITA, the Adoption Act 2010, as amended or otherwise by law to include the National Archives Act 1986.

15. Security and Training

- 15.1. Both parties shall adhere to the procedures at Schedule no. 3 regarding the transfer and receipt of data.
- 15.2. The parties 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 can include, but is not limited to:
- Policies, guidelines and procedures governing information security.
 - Password protection for computer access.
 - Automatic locking of idle PCs.
 - Appropriate virus-checking 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.
 - Adequate security where remote access is allowed.
 - Encryption of data held on portable devices.
 - Logs of data accesses.
 - Data breach procedures.
 - Adequate 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.
- 15.3. The parties shall ensure that all persons who have access to and who process the shared personal data are obliged to keep the shared personal data confidential.
- 15.4. The parties shall ensure that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data.
- 15.5. Access to the shared personal data will be restricted to persons on the basis of least privilege, sufficient to allow such persons to carry out their role.
- 15.6. Each party will keep the data secure and ensure that it is transferred securely in accordance with the procedures of this agreement.

16. Data Breaches and Reporting

If a personal data breach occurs after the data transmits to the party receiving the shared personal data (i.e. the “data receiver”), the data receiver will act in accordance with GDPR requirements and current personal data breach guidance from the Data Protection Commission.

17. Variation

No variation of this agreement shall be effective unless it is agreed between the parties, set out in writing, and signed by the parties to this Data Sharing Agreement.

18. Review of operation of the Data Sharing Agreement

- 18.1. 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— (a) in the case of the first such review, the date on which the Data Sharing Agreement came into effect in (referred to as the “effective date”), and (b) in the case of each subsequent review, the date of the previous review.
- 18.2. A review under clause 18.1 shall consider the impact of the technical, policy and legislative changes that have occurred since the date of the previous review under that clause.
- 18.3. Where the parties to the Data Sharing Agreement consider that it is appropriate following completion of a review they shall prepare a draft 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.

19. Termination

- 19.1. Each party commits to giving a minimum of 90 days notice of its intention to terminate this Data Sharing Agreement.
- 19.2. Both parties reserve the right to terminate, without notice, access to personal data where either party has reason to believe the conditions of this Data Sharing Agreement are not being observed.
- 19.3. Where a service is terminated, the terminating party shall provide to the other party reasons for terminating the service as soon as practicable following termination.
- 19.4. Where the terminating party is subsequently satisfied that the conditions of the Data Sharing Agreement are being observed, access will be restored forthwith.

20. Severance


- 20.1. 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.
- 20.2. Either Party reserves the right to terminate (the “terminating party”), without notice, access to personal data where either party has reason to believe any of the conditions of the agreement are not being observed. The terminating party will accept no responsibility for any consequences arising from the exercise of this right. Where a service is so terminated, reasons for terminating the service will be provided as soon as is practicable following termination. Where the terminating party is subsequently satisfied that the conditions of this agreement are being observed, access will be restored forthwith.

21. Jurisdiction


- 21.1. 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 Ireland.
- 21.2. Both parties agree that the officer who signs this agreement, and their successor(s), shall take responsibility for the adherence to terms and conditions of this agreement.

22. Agreement

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.

Signature:  _____ Date: 20/12/ 2022
Name: [NAME] DAVID DILLON
Position: An tArd-Chláráitheoir/Principal Officer
For and on behalf of Department of Social Protection

In the presence of

Signature:  _____ Date: 20/12/ 2023
Name: [NAME]
Position: An tArd-Chláráitheoir-Cúnta/Assistant Principal Officer
Department of Social Protection

Signature:  _____ Date: 15th of December 2023
Name: Colm O'Leary
Position: Interim Chief Executive Officer
For and on behalf of the Adoption Authority of Ireland

In the presence of

Signature:



Date: 15th of December 2023

Name: Ross Higgins

Position: Director of Information Services and Records
The Adoption Authority of Ireland

SCHEDULE 1 – GRO data protection impact assessment – summary of risks and mitigation to be added (Article 35(7) GDPR.

[Redacted]

Summary

Introduction

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

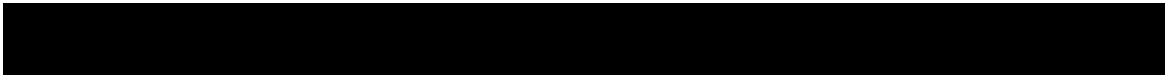
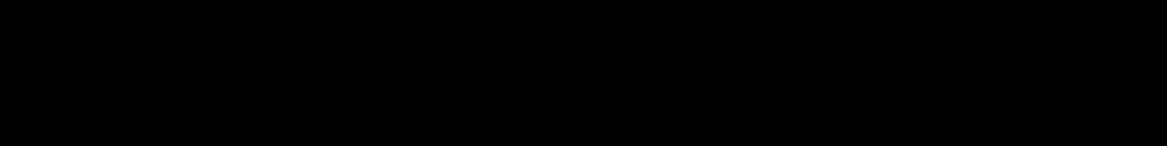
Need for a DPIA

[Redacted]

Approach to the DPIA



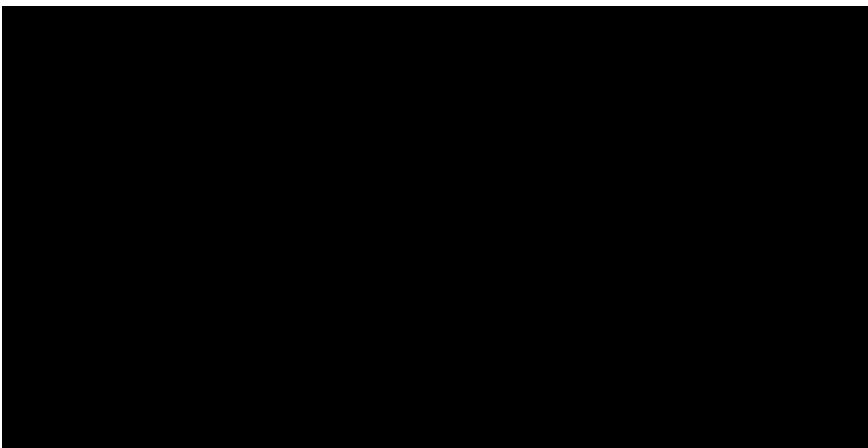
Data Protection Risks and Solutions



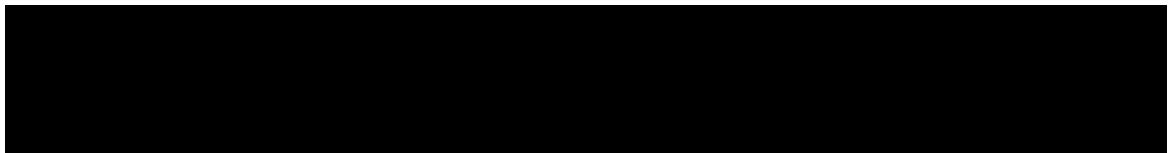
Data Protection Risk	
Risk Name:	
Privacy Principle:	
Risk Rating:	
Description/Impact of risk:	
Mitigation Solution	
Risk Status after Mitigation:	

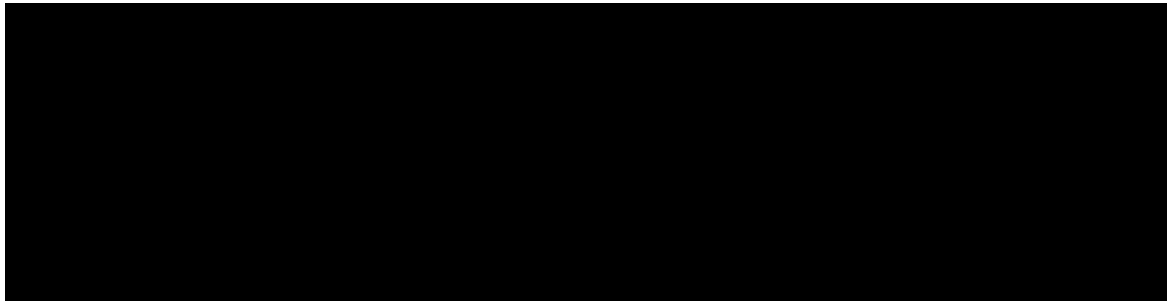
Data Protection Risk	
Risk Name:	
Privacy Principle:	
Risk Rating:	
Description/Impact of risk:	
Mitigation Solution	
Risk Status after Mitigation:	

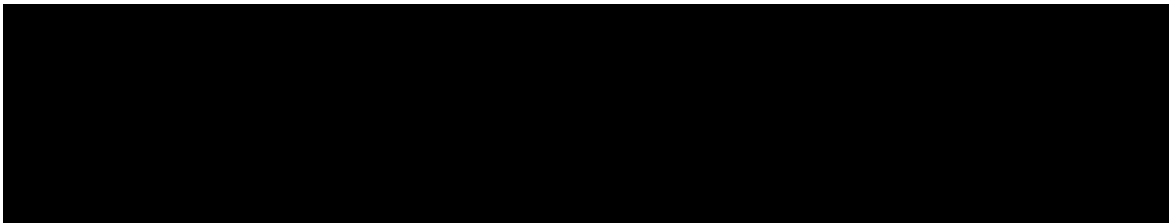
Data Protection Risk	
Risk Name:	

Privacy Principle:	
Risk Rating:	
Description/Impact of risk:	
Mitigation Solution	
Risk Status after Mitigation:	

Conclusion







SCHEDULE 2 – personal data shared and the retention period

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

Data Item	Description	Optional or Mandatory	Purpose	Data Classification
[Redacted]				

Data Item	Description	Optional or Mandatory	Purpose	Data Classification
-----------	-------------	-----------------------	---------	---------------------

[Redacted]

[Redacted]

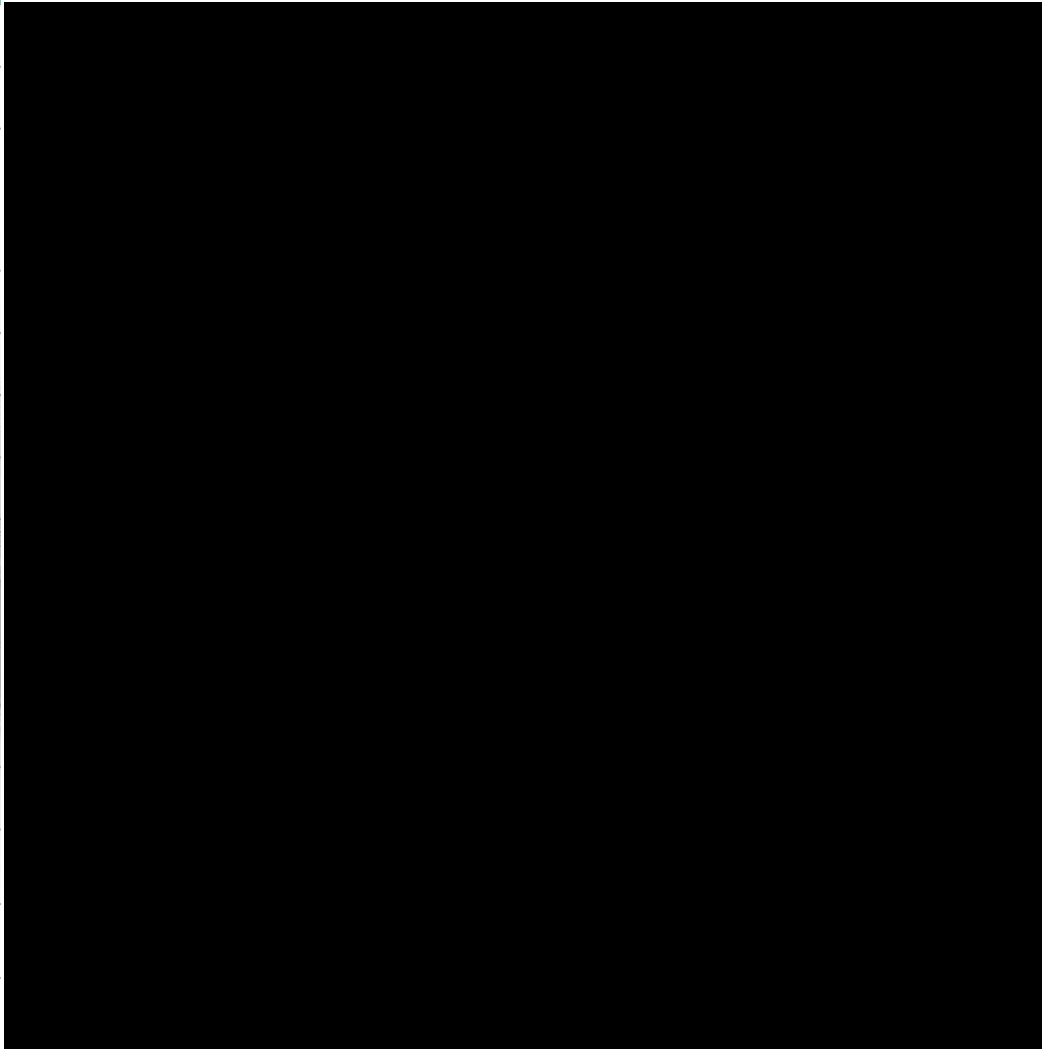
[Redacted]

[Redacted]

[Redacted]

[Redacted]

SCHEDULE 3 - the manner in which personal data is shared

Step #	Description
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	