



**An Ghníomhaireacht um
Leanaí agus an Teaghlach
Child and Family Agency**

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is dated [] ("**Effective Date**")

BETWEEN

- (1) The Child and Family Agency of Brunel Building, Heuston South Quarter, Dublin 8 ("**Tusla**"); and
- (2) [] (CRO number [] with a registered address at [] (the "**Processor**"),
- (each a "**party**" and together the "**parties**").

RECITALS

- A. Tusla and the Processor have entered into a services arrangement pursuant to which the Processor provides the following services to Tusla:
1. Provision of [Service Assessment Name]
 2. Provision of [Service Assessment Name]
- B. The provision of the Services necessitates the Processing of Personal Data by the Processor.
- C. The Personal Data to be processed may include special categories of personal data.
- D. Tusla and the Processor agree to enter into this Agreement to ensure compliance with Applicable Data Protection Law.

In consideration of the mutual obligations set out herein the parties agree as follows:

1 DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

"Applicable Data Protection Law" means the General Data Protection Regulation ("GDPR") and any applicable EU Member State legislation enacted in conjunction with the GDPR including the Data Protection Act 2018 and all other applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations in any relevant jurisdiction relating to the Processing of Personal Data as may be amended, extended, or replaced from time to time.

“Data Subject Request” means a request by a Data Subject for the exercise of the rights laid down in Chapter III GDPR.

“Personal Data” means any information relating to an identified or identifiable person, a **“Data Subject”**. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

“Process” or **“Processing”** means any operation or set of operations which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

“Services” means the services to be provided by or on behalf of the Processor to Tusla which includes the following:

1. [Description from Service Catalogue]
2. [Description from Service Catalogue]

“Tusla Data” means all personal data that is provided by Tusla to the Processor and all personal data that the Processor may collect and process in furtherance of the provision of the agreed Services.

- 1.2 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.
- 1.3 In the case of conflict or ambiguity between any provision contained in the body of this Agreement and any provision contained in the Schedules, the provision in the body of this Agreement will prevail.

2 PERSONAL DATA

In connection with performing its Services, the Processor will Process Tusla Data on behalf of Tusla as Tusla’s data processor. Details of the processing operations, in particular the categories of Personal Data and the purposes of processing for which the Tusla Data is processed on behalf of the Controller, are specified in Schedule 1 (Scope of Processing).

3 OBLIGATIONS OF TUSLA

- 3.1 Tusla determines the purposes for which Tusla Data are being or will be processed and the manner in which they are being or will be processed by the Processor.
- 3.2 Tusla will comply with Applicable Data Protection Law and shall ensure that any disclosure of Tusla Data made by it to the Processor has been lawfully and validly collected.

4 OBLIGATIONS OF THE PROCESSOR

- 4.1 The Processor is fully responsible for complying with Applicable Data Protection Law when Processing Tusla Data.
- 4.2 The Processor shall Process Tusla Data solely in accordance with Tusla's documented instructions, including those set forth in this Agreement, unless required to do so by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform Tusla of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.
- 4.3 The Processor shall process the Tusla Data only (i) for the specific purpose(s) of the processing, as set out in Schedule 1, unless it receives further instructions from the Controller and (ii) for the duration specified in Schedule 1.
- 4.4 The Processor shall ensure that its personnel engaged in the Processing of Tusla Data are informed of the confidential nature of Tusla Data and are subject to binding confidentiality obligations. The Processor shall actively enforce such obligations and bring them to the attention of its personnel and ensure that such personnel have undergone appropriate data protection training.
- 4.5 The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the Processing of Tusla Data in accordance with Article 32 GDPR specifically:
- (a) the pseudonymisation and encryption of Personal Data;
 - (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and
 - (e) at least the controls specified in Schedule 2 ("**Minimum Control Requirements**").
- In assessing the appropriate level of security, the Processor shall take account of the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.
- If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation ("special categories of personal data") or data relating to criminal convictions and offences, the Processor shall apply specific restrictions and/or additional safeguards.
- 4.6 The Processor shall not disclose or otherwise make available in any form any Tusla Data to any third party without first, except to the extent prohibited by Applicable Data Protection Law:

- (a) notifying Tusla of the anticipated disclosure (so as to provide Tusla the opportunity to oppose the disclosure and obtain a protective order or seek other relief);
- (b) obtaining Tusla's prior written consent to the disclosure; and
- (c) imposing contractual obligations on the third party recipient that are at least equivalent to those obligations imposed on the Processor under this Agreement;

4.7 The Processor shall amend or delete Tusla Data at Tusla's request and shall ensure that all Tusla Data Processed by the Processor is accurate and up to date, informing the Controller without delay if the Processor becomes aware that the Tusla Data it is processing is inaccurate or has become outdated.

4.8 The Processor shall at Tusla's request, provide a copy of Tusla Data held by it in a format or a media reasonably specified by Tusla.

4.9 The Processor shall immediately, and in any event no later than 2 business days, notify Tusla upon receipt of a Data Subject Request relating to Tusla Data. The Processor shall not respond to any Data Subject Request without Tusla's prior written approval and shall provide such assistance by appropriate technical and organisational measures insofar as this is possible to enable Tusla to fulfil its obligations under Applicable Data Protection Law to respond to Data Subject Requests.

4.10 The Processor shall immediately, and in any event no later than 2 business days, notify Tusla upon receipt of any communication from a supervisory authority that the Processor receives which relates to the Processing of Tusla Data or this Agreement, unless prohibited from doing so by law or by the supervisory authority. Tusla shall be responsible for all communications or correspondence with the supervisory authority in relation to Tusla's role as a controller of Tusla Data under Applicable Data Protection Law.

4.11 The Processor shall immediately, and in any event within 24 hours upon the Processor or any authorised sub-processor becoming aware of a Personal Data Breach affecting Tusla Data, notify, and provide, Tusla with sufficient information to allow Tusla to meet any obligations to report or inform supervisory authorities or Data Subjects of the Personal Data Breach under Applicable Data Protection Law. Such notification shall at a minimum:

- (a) describe the nature of the Personal Data Breach, the categories and the numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
- (b) communicate the name and contact details of the Processor's data protection officer and / or other relevant contact from whom more information may be obtained;
- (c) describe the likely consequences of the Personal Data Breach; and
- (d) describe the measures taken or proposed to be taken by the Controller to address the Personal Data Breach.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Processor shall co-operate with Tusla and take such reasonable steps, at its own cost, as are directed by Tusla to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

- 4.12 The Processor shall, at the direction of Tusla, fully cooperate and assist Tusla in conducting a data protection impact assessment and related consultations with any supervisory authority, if applicable, pursuant to Articles 35 and 36 GDPR, respectively.
- 4.13 The Processor shall make available to Tusla all information necessary to demonstrate compliance with the obligations under this Agreement and Article 28 GDPR and shall allow for and contribute to audits, including inspections at the premises or physical facilities of the Processor, which may be carried out by Tusla, or another auditor mandated by Tusla and shall, where appropriate, be carried out with reasonable notice. Tusla may make a written request, or request in the course of an audit or inspection, for a copy of all Tusla Data and related activity logs from the Processor and such information shall be provided by the Processor without unreasonable delay in the format and on media as reasonably specified by Tusla.

5 SUB-PROCESSORS

- 5.1 The Processor shall not subcontract the Processing of Tusla Data without prior written consent of Tusla.
- 5.2 The Processor shall make a written request seeking Tusla's permission to allow the proposed engagement of a sub-processor. Tusla shall establish what requirements are necessary in the circumstances and shall determine what documentary evidence may be required in order to assess the request for the engagement of the proposed sub-processor. Tusla reserves the right to seek further clarification from the Processor.
- 5.3 Tusla has the right to grant or withhold such consent in its sole discretion and may subsequently revoke such consent if the sub-processor's performance, in the reasonable judgment of Tusla, has been unacceptable.
- 5.4 The Processor shall remain fully responsible for fulfilment of its obligations under this Agreement and will remain the primary point of contact regarding any Processing of Tusla Data. The Processor shall be fully responsible and liable for the acts, omissions, or defaults of its sub-processors in the performance (or failure of performance) of the sub-processors' data protection obligations under this Agreement or otherwise as if they were the Processor's own acts, omissions, or defaults. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations.
- 5.5 The Processor shall impose contractual obligations on its sub-processors that are the same or at least equivalent to, and in any event no less onerous than, those obligations imposed on the Processor under this Agreement, including without limitation, a right for Tusla to audit or inspect the premises or physical facilities of sub-processors, with reasonable notice (where appropriate).
- 5.6 Tusla consents to the Processor's use of sub-processors identified in Schedule 3 ("**Approved Sub-processors**").

6 DATA TRANSFER

Subject to the provisions of Clause 10, the Processor shall not transfer, or cause to be transferred, any Tusla Data from one jurisdiction to another without Tusla's prior written consent. Where Tusla consents to such transfer, the transfer shall be in accordance with Applicable Data Protection Law and shall not cause Tusla to be in breach of any Applicable Data Protection Law.

[Make mention of the Adequacy Decision if Tusla Data being processed in UK]

7 WARRANTIES

7.1 The Processor warrants the following:

- (a) It shall Process Tusla Data in compliance with Applicable Data Protection Law;
- (b) It shall implement appropriate technical and organisational measures to protect Tusla Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed;
- (c) No conflict of interest exists in its performance of the obligations under this Agreement;
- (d) It shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Tusla Data, ensuring in each case that access is strictly limited to those individuals who need to know/access Tusla Data as is strictly necessary for the provision of the Services, and ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;
- (e) It is not aware of any previous Personal Data Breaches or, if a Personal Data Breach has occurred, it has disclosed in writing each such Personal Data Breach to Tusla and remedied all related security vulnerabilities and taken appropriate measures to prevent similar Personal Data Breaches from occurring again;
- (f) It shall inform Tusla immediately if it is aware or reasonably suspects that Tusla's instructions regarding the Processing of Tusla Data breach any Applicable Data Protection Law;
- (g) It shall inform Tusla immediately if it becomes aware of any Personal Data Breach affecting Tusla Data; and
- (h) It shall inform Tusla immediately if it becomes aware of any advance in technology and methods of working which mean that Tusla should revise the security and technical measures in place in order to protect Tusla Data as well as the Processing of Tusla Data.

8 RECORDS

8.1 The Processor shall keep at its normal place of business detailed, accurate and up-to-date records relating to the Processing of Tusla Data by the Processor.

8.2 The Processor shall make such records available to Tusla upon request.

9 INDEMNITY

9.1 The Processor agrees to indemnify and keep indemnified and defend at its own expense Tusla against all costs, claims, damages (including non-material damage), fines, penalties, costs, losses or expenses incurred by, awarded against or agreed to be paid by Tusla arising out of or relating to (1) its failure (or that of its employees, sub-processors or agents) to comply with this Agreement and/or Applicable Data Protection Law; and/or (2) any Personal Data Breach. Any limitation of liability set forth in the main Services Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

9.2 For the avoidance of doubt, the appointment of a sub-processor in accordance with Clause 5 shall not dilute, diminish, or alter the indemnity owed by the Processor to Tusla.

10 TERMINATION

10.1 This Agreement shall terminate automatically upon termination or expiry of the Processor's obligations in relation to the Services.

10.2 Tusla shall be entitled to terminate this Agreement by notice in writing to the Processor if

- (i) the Processor is in a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within twenty one (21) days from the date of receipt by the Processor of a notice from Tusla identifying the breach and requiring its remedy; or

- (ii) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations pursuant to this Agreement or Applicable Data Protection Law.

10.3 The Processor shall be entitled to terminate this Agreement insofar as it concerns Processing of Tusla Data under this Agreement where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1(f), the Controller insists on compliance with the instructions.

11 POST-TERMINATION OBLIGATIONS

11.1 Subject to the instructions of Tusla, the Processor and each sub-processor shall promptly and in any event within thirty (30) days of the date of termination of any Services involving the Processing of Tusla Data (the "**Termination Date**");

- (a) return all Tusla Data to Tusla by secure file transfer in such format as is reasonably notified by Tusla to the Processor; or

- (b) delete and procure the deletion of all copies of Tusla Data held by the Processor and each sub-processor.

11.2 The Processor and each sub-processor may retain Tusla Data to the extent required by Applicable Data Protection Law and only to the extent and for such period as required by Applicable Data Protection Law and always provided that the Processor and each sub-processor shall ensure the confidentiality of all such Tusla Data and shall ensure that such Tusla Data is only Processed as necessary for the purpose(s) specified in the Applicable Data Protection Law requiring its storage and for no other purpose.

11.3 The Processor shall provide prompt written certification to Tusla that it and each sub-processor has fully complied with this Clause 11 upon request.

12 WAIVER

- 12.1 Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence will not be construed as a waiver of that party's rights under this Agreement.

13 INVALIDITY

- 13.1 If any term or provision of this Agreement is held to be illegal or unenforceable in whole or in part under any enactment or rule of law, such term or provision or part will to that extent be deemed not to form part of this Agreement but the enforceability of the remainder of this Agreement will not be affected provided however that if any term or provision or part of this Agreement is severed as illegal or unenforceable, the parties will seek to agree to modify this Agreement to the extent necessary to render it lawful and enforceable and as nearly as possible to reflect the intentions of the parties embodied in this Agreement including without limitation the illegal or unenforceable term or provision or part.

14 NOTICES

- 14.1 Notices shall be in writing and shall be sent to the other party by post or by courier to the address set out in this Agreement and marked for the attention of the person at the address set out below. A party may change its address for the purposes of this Agreement by giving notice in accordance with this Agreement.

15 VARIATION

- 15.1 If a change in any Applicable Data Protection Law prevents either party from fulfilling all or part of its obligations under this Agreement, the parties may agree to suspend the processing of the Tusla Data until that processing complies with the new requirements. If the parties are unable to bring the Tusla Data processing into compliance with the Applicable Data Protection Law, either party may terminate this Agreement on not less than [7] working days on written notice to the other party.
- 15.2 No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

16 GOVERNING LAW

- 16.1 This Agreement and any claim or dispute (whether contractual or non-contractual) arising out of or in connection with it will be governed by and construed in accordance with the laws of Ireland and the parties irrevocably agree that the courts of Ireland shall have exclusive jurisdiction to settle any claim or dispute (whether contractual or non-contractual) arising out of or in connection with this Agreement or its subject matter or formation.

This Agreement has been entered into on the date stated at the beginning of it.

Executed for and on behalf of the Child and
Family Agency by an authorised signatory:

Signature

Name (block capitals)

Executed for and on behalf of [] by an
authorised signatory:

Signature

Name (block capitals)

SCHEDULE 1
Scope of Processing

Subject Matter of Processing: The context for the Processing of Tusla's Data is the Processor's provision of the Services.

Duration of Processing: The Processing will begin on the Effective Date and will end upon expiration or termination of the Agreement.

[This section will set out the records retention arrangements for this type of processing.]

Nature and Purpose of Processing: To the extent necessary for the Processor to provide the Services.

Types/Categories of Personal Data:

[_____]

Categories of Data Subjects:

[_____]

Processor Data Protection Officer:

Name: [_____]

Address for correspondence: [Postal or Physical address_____]

SCHEDULE 2

Minimum Control Requirements

The Processor must implement appropriate technical and organisational measures (TOMs) within their own organisation to protect against the unauthorised or unlawful processing and the accidental loss, destruction, damage, alteration, and disclosure of any Personal Data and/or Special Categories of Personal Data which is shared under this Agreement.

At a minimum, the Processor must implement the following TOMs:

1. Ensure that the data processing environment is understood, and applicable data sharing or data processing agreements are in place.
2. Ensure that strong and robust access controls are in place to manage and protect both on-site and remote access to Personal Data and Special Categories of Personal Data.
3. Ensure that all on-site and remote access to Personal Data and Special Categories of Personal Data stored electronically, is controlled by strong unique passwords and all such access is logged appropriately.
4. Ensure that all Mobile Computer Devices which are used to Process and/or store Personal Data and Special Categories of Personal Data have strong Encryption facilities available which permit the encryption of the Mobile Computer Device and/or the Encryption of the Personal Data and Special Categories of Personal Data at a file or folder level.
5. Ensure that all Computer Devices which are used to Process or store Personal Data and/or Special Categories of Personal Data have real-time protection Anti-Malware Software installed which is updated on a regular basis.
6. Ensure that all Personal Data and Special Categories of Personal Data which is Processed or stored off-site or within a Cloud Computing solution by a Third Party, on behalf of a Party, is Encrypted at rest using strong Encryption protocols.
7. Ensure that documented IT and information security policies, which define how the Party's employees, contractors and Third Parties are to manage, process and secure the Party's data, are in place and kept current.
8. Ensure that all Personal Data and/or Special Categories of Personal Data transmitted outside an organisation, via electronic means, is sent through secure channels (for example, VPN, Secure FTP, TLS) or encrypted email using strong encryption protocols.
9. Ensure that all Personal Data and/or Special Categories of Personal Data is backed up on a regular basis and that backup copies of the data are tested on a frequent basis to ensure the data can be restored in the event of a hardware or software crash or a cybersecurity Incident.
10. Ensure that all Servers, with the exception of those which are owned or controlled by Tusla, which are used by the Processor to process, or store Tusla Personal Data are backed up on a daily basis. Where the Processor backs up the Servers onto backup media, the Processor must ensure the following:
 - a. The backup media is stored a sufficient distance away from the Server, for example, in another building on-site under the control of the Processor or off-site in a building or facility controlled by the Processor or a contracted third party.
 - b. When not in use, the backup media is protected from damage caused by fire, heat, humidity, water, and exposure to strong magnetic fields.
 - c. The backup media is password protected by strong unique passwords.
 - d. The backup media is encrypted using strong encryption.
 - e. Access to the backup media is limited to the Processor's employees, contractors and/or, as applicable, Sub-Processors who are involved in the backup process.
 - f. When in transit, the backup media is protected at all times from damage, theft, interference and loss.
 - g. The backup media is tested by the Processor on a regular basis.
 - h. All old, obsolete, and damaged backup media which was used to backup Tusla Personal Data is physically destroyed.

11. Ensure that all Servers used by the Processor to process, or store Tusla's Personal Data have logging enabled, and the Server logs must be monitored by the Processor on a regular basis.
12. Ensure that appropriate patch management procedures are in place for managing the timely application of relevant security software updates and patches to all IT devices, mobile computer devices, Servers, and other critical IT equipment, used by the Processor to process, or store Tusla's Personal Data.
13. The Processor must have documented disaster recovery plans in place which detail how, in the event of a physical or technical security breach, it will restore the availability of, and access to any Servers, used by it to process or store Tusla Personal Data.
14. The Processor must have appropriate asset management procedures in place which allow for the management and recording of all IT hardware and software assets used to process or store Tusla's Personal Data.
15. The Processor must have appropriate procedures in place for the timely decommissioning and secure wiping or destruction, i.e., the process that renders data unrecoverable, of all old, obsolete, and damaged IT devices, mobile computer devices, Servers, software, and other critical IT equipment, with the exception of those which are owned or controlled by Tusla, used by the Processor to process, or store Tusla's Personal Data.
16. The Processor must have appropriate separation controls in place which provide for the separation of different customer's data on its IT hardware and software and ensure Tusla's Personal Data is processed by the Processor as separately as possible other customer's data.
17. The Processor must ensure full separation, where applicable, of its production and development / test / training environments.
18. The Processor must have appropriate procedures in place for the vetting of all new employees and contractors who will have access to Tusla's Personal Data and ensure that all contracts of employment contain binding non-disclosure and confidentiality clauses.
19. The Processor must have appropriate procedures in place to ensure that all employees and contractors have access only to personal data required for them to do their jobs and that controls are in place to prevent unauthorised access to the Shared Data
20. The Processor must ensure that where legally required to do so, it has appointed a Data Protection Officer in accordance with Article 37 of the GDPR.
21. The Processor must have appropriate procedures in place which allow for the Processor to regularly, test, assess and evaluate the effectiveness of the technical and organisational measures they have implemented to ensure the security of Tusla's Personal Data which they process on behalf of Tusla.

SCHEDULE 3
Approved sub-processors

[]