An Rialálaí Carthanas
Charities Regulator

# DATA PROCESSING AGREEMENT BETWEEN THE CHARITIES REGUALTOR AND (Insert Third Party)

# Contents

# Data Processing Agreement – Controller Processor Contract

This Data Processing Agreement ("this Agreement"), between (Third Party), a company having its principal place of business at (Insert Address) ( ('the Processor') and the Charities Regulatory Authority, having its principal place of business at 03 Georges Dock, IFSC, D01 X5X0 (**"**the Controller") ("the Charities Regulator") forms part of the 'Contract for Services' between (Third Party), and the Charities Regulator (each a "Party", together "the Parties") dated xx/xx/xxxx.

This Agreement applies to the processing of personal data by the Processor on behalf of the Controller insofar as such activities are required by the Contract for Services. This Agreement is made necessary by changes to the law introduced as a consequence of the European Union General Data Protection Regulation (GDPR).

In consideration of the mutual obligations set out in the Contract for Services the Parties hereby agree that the terms and conditions set out hereunder shall be added to the Contract for Services.

This Agreement comes into effect on the date it is signed by the last Party to sign it (as indicated under that Party's signature).

## 01. Definitions

- "the Agreement" means this Data Processing Agreement;
- "Contract for Services" means the contract between (Third Party), and the Charities Regulator dated 3 January 2018.
- the "Data Protection Acts" means the Data Protection Act 1988 – 2018 and General Data Protection Regulations (GDPR) referred to as Data Protection Legislation;
- "EEA" means the European Economic Area;
- "GDPR" means the European Union General Data Protection Regulation;
- "Governing Law" means the GDPR, the Data Protection Acts and, to the extent applicable, the data protection or privacy laws of any other country;

- The terms “personal data”, “Controller”, “Processor”, “personal data breach”, “processing” shall have the same meaning as in the GDPR.

## 02. Subject Matter, Nature and Purpose of Processing and Duration

The Controller provides (Insert information in relation to the processing activities).

The Agreement shall continue in effect until the termination of the Contract for Services. The Processor may have additional requirements to retain any data provided as part of the contract for an additional period to ensure compliance with other legal requirements.

## 03. Types of Personal Data and Categories of Subjects to Whom the Data Relates

The personal data which the Processor shall process in accordance with the Contract for Services is data relating to: Insert details of the personal data being processed:

- Name
- Date of birth
- Data relating to employment
- Contact details
- Health data

The categories that this data relates to includes staff, employees and job candidates.

## 04. Processor’s Obligations

### 4.1 Compliance

Nothing in this agreement shall relieve the Processor of the Processor’s responsibilities and liabilities under the Governing Law and data protection legislation.

### 4.2 Security arrangements

The Processor shall implement appropriate, adequate technical and organisational measures as referred to in Article 32(1) GDPR, to safeguard the confidentiality measures including, integrity and availability of the personal data and to guard against any unlawful access to or processing of (including unauthorised disclosure, deterioration, alteration or disclosure of personal data) personal data under the Contract for Services, taking account of the nature of the personal data concerned, the accessibility of the data, the nature, scope, context and purpose of the processing, any risks to the rights and freedoms of individuals arising from the processing concerned, the likelihood of any risks arising and the severity of such risks, the state of the art and cost of implementation and any guidelines, recommendations and

descriptions of best practice issued by the European Commission or the European Data Protection Board.

- The Processor shall review the administrative, physical and technical safeguards regularly and shall inform the Controller where more effective measures have been identified.

- The Processor shall document the implementation of the technical and organisational measures in accordance with the requirements of the GDPR.

- The Processor shall maintain administrative, physical and technical safeguards designed for the protection and security, confidentiality and integrity of the personal data being processed under the Contract for Services as set out in the Annex to this Agreement.

## 4.3 Acting on instructions only

The processing of the personal data by the Processor shall take place within the terms of the Contract for Services and only to the extent that the Controller has instructed the Processor to do save insofar as the Processor is required by the law to act otherwise. If the Processor is required by law and/or an order of any court or competent jurisdiction or any regulatory, judicial or governmental body to disclose the personal data, the Processor shall, except where prohibited by law, first:

- give the Controller the details of the proposed disclosure.

- give the Controller a reasonable opportunity to take any steps it considers necessary to protect the confidentiality of the personal data including but not limited to seeking such judicial redress as the Controller may see fit in the circumstance.

- The Processor shall not process the personal data for any other purpose than as described in the Contract for Services.

## 4.4 Subcontracting

- The Processor shall not subcontract its obligations in relation to the processing of data under the terms of the Contract for Services save with the prior written agreement of the Controller.

- Where the Processor proposes the engagement of a subcontractor the Processor shall carry out adequate due diligence to ensure that the subcontractor is capable of providing the level of protection required by this Agreement.

- Where the Controller agrees to the subcontracting of any of the processing obligations of the Processor, the Processor shall ensure that the subcontractor is

bound by terms and conditions that offer at least the same level of protection for the personal data as this Agreement and Article 28(3) GDPR.

- Where the Processor engages a subcontractor and the subcontractor fails to fulfil its data protection obligations, the Processor shall remain liable to the Controller for the performance of those obligations.

## 4.5 Confidentiality

- The Processor shall keep confidential all personal data processed. The Processor shall take steps to ensure the reliability of any employee or agent who may have access to the personal data. The Processor shall ensure that access to the personal data is limited to those individuals who are required to have access to the data in order to give effect to the Contract for Services. The Processor shall ensure that all such employees or agents who have access to the personal data are subject to an undertaking of confidentiality or professional or statutory obligation of confidentiality.

- This duty of confidentiality shall not apply where the Controller has expressly authorised the furnishing of such personal data to third parties or if there is an obligation under the law to make the information available to a third party.

## 4.6 Data subject's rights

- The Processor shall promptly notify the Controller if the Processor receives a request to exercise his or her rights from a data subject in respect of the personal data being processed under the Contract for Services. The Processor may notify the data subject of the Controller's responsibility in respect of the data subject's request.

- The Processor shall not respond to the request unless on the written instructions of the Controller or as may be required by law in which case the Processor shall, to the extent permitted by law, inform the Controller of the legal requirement before the Processor responds to the request.

- The Processor shall assist the Controller in safeguarding the rights of data subjects concerning access to, and the correction, deletion or erasure of, personal data by making available any information requested by the Controller, immediately implementing any instructions of the Controller and implementing appropriate measures, as far as possible, to enable the fulfilment by the Controller of its obligation to respond to requests by data subjects to exercise their rights under the Governing Law.

## 4.7 Erasure or return of data

- Save as may be provided by law the Processor shall erase or return to the Controller in a secure manner, at the election of the Controller, all the personal data processed

by the Processor upon the termination of the Contract for Services and shall erase any copy of the personal data unless required by law to retain the data.

- The Processor shall provide written certification to the Controller that it has complied with a requirement to erase the personal data within 30 days of the instruction to erase.

## 4.8 Demonstrating compliance

- The Processor shall make available to the Controller upon request all information necessary to demonstrate compliance with this Agreement and the Governing law.

- The Processor shall immediately inform the Controller if, in its opinion, an instruction of the Controller would breach the Governing Law.

- The Processor shall cooperate with the Controller or any independent third party appointed by the Controller for the purpose, in the conduct of an audit, including an inspection, carried out to verify compliance with the Governing Law in the processing of the personal data the subject of the Contract for Services. The Controller and any third party appointed shall abide by the Processor's reasonable security requirements, and will not interfere unreasonably with the Processor's business activities.

- The Controller shall give the Processor reasonable notice of any proposed audit or inspection. The findings of any audit or inspection shall be discussed and evaluated by the Parties and, where applicable, implemented, as appropriate, by one of the Parties or jointly by both Parties.

- The Controller shall bear the costs of the audit.

## 4.9 Data Breach

The Processor shall notify the Controller as soon as it becomes aware but no later than 24 hours of becoming aware of a personal data breach affecting the personal data processed in accordance with the Contract for Services and shall provide the Controller with sufficient information to meet any obligations of the Controller to inform the data subjects and the relevant data protection authorities. The Processor shall, at a minimum:

- describe the nature of the personal data breach, the categories and numbers of data subjects affected and the categories and numbers of personal data records concerned;
- describe the cause or suspected cause if not known of the breach;
- describe the likely consequences of the personal data breach;
- describe the measure taken or proposed to be taken to address the personal data breach, and

- communicate the name and contact details of the Processor's Data Protection Officer (DPO) and any other relevant contact persons.

The Processor shall cooperate with the Controller and take such reasonable steps as are necessary to assist in the investigation, mitigation and remediation of any personal data breach.

The Controller shall determine whether or not to inform the data subject(s) and/or the relevant data protection authority(ies) and the Processor shall cooperate with the Controller in notifying the relevant authority(ies) and/or the data subject(s).

## 4.10 Transfer out of European Union

The Processor shall not transfer the personal data to a country outside the EEA without the prior written agreement of the Controller. Where the Processor seeks the Controller's prior written agreement, the Processor shall assist the Controller in establishing whether the transfer of the data to a country outside the EEA may be done in a manner that satisfies the Governing Law.

## 4.11 Data protection impact assessment

The Processor and any subcontractor who may be engaged in accordance with this Agreement shall provide reasonable assistance to the Controller with any data protection impact assessments, prior consultations with supervising authorities or other competent authorities, which the Controller reasonably considers to be required by Article 35 and 36 GDPR, in each case solely in relation to the processing of the personal data under this Agreement and taking account of the nature of the processing and information available to the Processor and any subcontractor engaged in accordance with this Agreement.

## 4.12 Use of Artificial Intelligence (AI)

The Processor shall not use Artificial Intelligence (AI) systems or tools in connection with the processing of Personal Data under this Agreement without the prior written authorisation of the Controller. Where AI is used, the Processor shall ensure that such use:

- Is compliant with all applicable data protection legislation, including the GDPR and, where relevant, the EU Artificial Intelligence Act
- Adheres to principles of transparency, fairness, and accountability, including ensuring that any automated decision-making is explainable and contestable where required under Article 22 GDPR
- Does not involve the use of Personal Data for training AI models unless explicitly authorised in writing by the Controller
- Implements appropriate technical and organisational measures to mitigate risks to the rights and freedoms of data subjects
- Is documented in a Data Protection Impact Assessment (DPIA) where required.

## 5. Miscellaneous

The Controller warrants that it has a legal basis upon which to process the personal data. The Controller indemnifies the Processor of all claims and actions of third parties related to the processing of personal data without a legal basis under this Data Processing Agreement.

All personal data processed on behalf of the Controller shall remain the property of the Controller and/or the relevant data subjects.

The Processor undertakes to cooperate in amending and adjusting this Data Processing Agreement in the event of new privacy legislation.

The Processor shall indemnify the Controller against any and all losses, expenses (including reasonable legal fees), damages, costs, penalties and losses incurred by the Controller arising from or in connection with the Processor acting outside or contrary to the lawful instructions of the Controller and/or any other breach by the Processor of its obligations under this agreement.

## 6. Status of Agreement

The terms of this Agreement, to the extent that they impose obligations on the Processor in order to comply with the Governing Law, are essential and fundamental terms, the breach of which shall result in the termination of the Contract for Services, as amended by this Agreement.

**IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorised representatives.**

(Third Party)

_____/_____/_____
*Date*

_____
*Name [Block Capitals]*

_____
*Signature*

**Charities Regulatory Authority**

_____/_____/_____
*Date*

_____
*Name [Block Capitals]*

_____
*Signature*

# 7. IT Annex

**Technical and Organisational Measures Required**

The following is a description of the measures expected to be implemented by the Data Processor in accordance to Article 32 of the GDPR:

1. **Physical Security**
   - Secure destruction of data bearing devices
   - Physical security measures to control access to ICT areas including Data Centre

2. **Security & Privacy**
   - Users have a unique logon and password that must be reset regularly
   - Password protection of all devices
   - Implementation of firewalls and filtering systems to mitigate against attacks
   - Regular Penetration testing across the environment
   - Logical data separation governed by access control lists
   - Secure remote access via a secure portal
   - Restricted use of storage media

3. **Practices**
   - Change Management Procedures
   - Business Continuity Processes & Guidelines
   - Governance to oversee ICT Processes
   - Project Management Methodology
   - Appropriate staff training – Security & GDPR
   - Detailed procedures if the personal data is processed using any Artificial Intelligence (AI) software

4. **Policies and Procedures**
   - ICT Security Policies, including Acceptable usage policy
   - Compliance with Official Secrets Act for both staff and contractors
   - ICT Services delivered in line with ISO/IEC 2700:2005

5. **Roles & Responsibilities**
   - Data Protection Officer (if necessary)
   - Security Officer

# 8. Notes

1. Assumption has been made that there is already a contract or a service level agreement in place for the Processor to provide services to the Charities Regulator and the draft agreement is an addendum to that other contract or service level agreement. If and when new contracts/service level agreements are being entered it will be possible to combine the usual commercial/service level agreement terms with these specific data protection provisions.

2. The draft contract is a generic one. Included (in blue) the type of detail that might be provided by the Charities Regulator in relation to the processing of personal data relating to applicants for international protection so as to give an idea of the level of detail that seems to be required by the General Data Protection Regulation and the Data Protection Bill.

3. The draft agreement follows the sequence of Article 28 to enable anyone using this template to be sure they have met the requirements of the GDPR.

4. Technical safeguards will need to be considered by the Charities Regulators IT Section. It seems that in relation to private sector GDPR agreements there is an expectation that there will be agreement on technical, security measures to allow for the secure transfer and processing of data.

5. Clause 5 of the draft contract is intended to make clear that a breach by the Processor of any provisions of the agreement, which is required by law, is a material breach, which will lead to the termination of the contract. It would be advisable for the Charities Regulator when using this template contract to check that the services contract contains a termination clause.