Data Processing Agreement Template

Controller to processor terms for commissioned services, technology and professional suppliers

Document control	Details
Organisation	Community Integration & Recovery Centre (CIRC) C.I.C.
Document owner	Director and Data Protection Lead
Effective date	17 September 2026
Next review	17 September 2027
Status	Approved website version

Purpose and status. This document sets the standard expected by Community Integration & Recovery Centre (CIRC) C.I.C.. It should be read with applicable law, contractual requirements, local safeguarding procedures and related operational procedures. It does not replace professional judgement or legal advice in a specific case.

This template is not complete until the parties sign it and complete Schedules 1 to 4. It may be used as a standalone agreement or incorporated into a main services agreement. The commercial terms, liability position and sector-specific requirements should be reviewed for each engagement.

Parties and context

Field	Details
Controller	[Full legal name, company number and address]
Processor	[Full legal name, company number and address]
Main agreement	[Title and date]
Effective date	[Date]
Term	For the term of the main agreement and while the processor holds controller personal data.

The parties agree that the entity determining the purposes and essential means of processing is the Controller and the entity processing personal data only on documented instructions is the Processor. If the factual roles differ for a particular activity, the parties must record the correct allocation in Schedule 1.

1 Definitions and interpretation

“Applicable Data Protection Law” means the UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003, Data (Use and Access) Act 2025 to the extent in force and applicable,

and related binding law. “Controller Personal Data” means personal data processed by the Processor on behalf of the Controller. Other capitalised data-protection terms have the meanings given by Applicable Data Protection Law. If this Agreement conflicts with the Main Agreement on data protection, this Agreement prevails for that conflict.

2 Processing instructions

The Processor shall process Controller Personal Data only on the Controller’s documented instructions, including the instructions in Schedule 1, unless UK law requires otherwise. Where legally permitted, the Processor shall tell the Controller before carrying out legally required processing. The Processor shall promptly notify the Controller if it considers an instruction infringes Applicable Data Protection Law and may suspend the affected processing while the parties resolve the issue.

3 Confidentiality and personnel

The Processor shall ensure that each person authorised to process Controller Personal Data is bound by confidentiality obligations, receives proportionate data-protection and security training, and accesses only the information necessary for assigned duties. The Processor remains responsible for its personnel.

4 Security

Taking account of the state of the art, implementation cost, nature, scope, context and purposes of processing, and risks to individuals, the Processor shall maintain appropriate technical and organisational measures. The minimum measures are in Schedule 2. The Processor shall not materially reduce protection during the term and shall provide relevant assurance evidence on reasonable request.

5 Subprocessors

The Controller gives [specific/general] written authorisation for subprocessors listed in Schedule 3. Under general authorisation, the Processor shall give at least [30] days’ written notice of a proposed addition or replacement so the Controller can object on reasonable data-protection grounds. The Processor shall impose materially equivalent data-protection duties by written contract and remains fully liable to the Controller for each subprocessor’s performance.

6 International transfers

The Processor shall not transfer Controller Personal Data outside the United Kingdom, or permit remote access from another country, without the Controller’s prior written authorisation and a valid transfer mechanism. The parties shall document adequacy, the UK IDTA, UK Addendum or other lawful safeguard, complete required risk assessments and implement supplementary measures.

7 Individual rights

Taking account of the nature of processing, the Processor shall assist the Controller through appropriate technical and organisational measures to respond to requests to exercise data-subject rights. The Processor shall forward any request received directly without undue delay and shall not respond except on the Controller’s documented instructions or as required by law.

8 Compliance assistance

The Processor shall provide reasonable assistance with security, breach assessment and notification, data-protection impact assessments, prior consultation, records of processing, regulator enquiries and other Controller compliance duties, taking account of the nature of processing and information available to the Processor.

9 Personal data breaches

The Processor shall notify the Controller without undue delay and, where practicable, within [24] hours after becoming aware of a personal data breach affecting Controller Personal Data. The notice shall describe the nature of the breach, affected people and records, likely consequences, measures taken or proposed, and a contact point. Information may be supplied in phases. The Processor shall preserve evidence, mitigate harm, cooperate with the Controller and not notify individuals or regulators without authorisation unless legally required.

10 Audit and information

The Processor shall make available information reasonably necessary to demonstrate compliance and allow audits or inspections by the Controller or an independent auditor bound by confidentiality. Except after an incident, regulator request or credible compliance concern, audits will normally occur on reasonable notice during business hours and avoid unnecessary disruption. Relevant, current independent assurance may be accepted where appropriate.

11 Return and deletion

At the Controller's choice on termination or earlier written instruction, the Processor shall securely return or delete Controller Personal Data and existing copies, unless law requires retention. The Processor shall isolate retained data, process it only for the legal retention purpose and delete it when that duty ends. On request, an authorised representative shall certify completion.

12 Records and accountability

The Processor shall maintain records required by law, cooperate with the Information Commissioner and provide current contact details for its privacy and security leads. Each party is responsible for its own compliance, notices, lawful bases and regulatory fees.

13 Liability and indemnity

Liability is governed by the Main Agreement except that nothing limits liability where limitation is prohibited by law. Each party shall promptly take reasonable steps to mitigate loss. Any indemnity, insurance or liability cap must be expressly stated in the Main Agreement and legally reviewed for the specific arrangement.

14 Termination and survival

A material breach of this Agreement that is not remedied within a reasonable written cure period permits the Controller to suspend affected processing or terminate the affected service, subject to the Main Agreement. Confidentiality, audit, return or deletion, liability and any provisions intended to survive remain effective while data is retained.

15 General

No variation is effective unless recorded in writing by authorised representatives. Invalid provisions are severed to the minimum extent necessary. The governing law and courts are those stated in the Main Agreement, or England and Wales if the Main Agreement is silent.

Schedule 1 Processing details

Required detail	Agreed description
Subject matter and service	[Describe the service and why processing is required]
Duration	[Start, end and deletion timetable]
Nature and operations	[Collect, record, host, access, transmit, analyse, support, erase]
Purposes	[Specific purposes; no open-ended wording]
Categories of individuals	[Participants, beneficiaries, representatives, staff, applicants and website users.]
Personal data	[Identity, contact, programme and support records, workforce data and technical logs.]
Special category or criminal-offence data	[Specify or state none; identify Article 9 and Schedule 1 DPA 2018 conditions]
Controller instructions	[Main agreement, policies, tickets and named authorised contacts]
Return and deletion	[Method, format, deadline, backups and certification]

Schedule 2 Minimum technical and organisational measures

- documented security governance, risk assessment and named accountability;
- least-privilege access, unique accounts, prompt joiner-mover-leaver controls and multifactor authentication where proportionate;
- encryption in transit and at rest where proportionate, with managed keys;
- secure configuration, vulnerability management, malware protection, patching and logging;
- tested backup, restoration, availability and business-continuity arrangements;
- secure development and change management where software is supplied;
- physical security, device management and secure disposal;
- staff vetting where appropriate, confidentiality and regular training;
- incident response, breach escalation and evidence preservation;
- periodic testing, audit and remediation of controls.

Schedule 3 Approved subprocessors

Subprocessor and location	Service	Data and individuals	Transfer safeguard
[Name and country]	[Function]	[Scope]	[Adequacy or contractual safeguard]

Schedule 4 Contacts and signatures

Role	Controller	Processor
Data protection contact	[Name, role, email, telephone]	[Name, role, email, telephone]
Security incident contact	[24-hour route]	[24-hour route]
Authorised signatory	Name: _____ Role: _____ Signature: _____ Date: _____	Name: _____ Role: _____ Signature: _____ Date: _____

Authoritative sources

This document was prepared with reference to the following official sources. The online version of each source should be checked at review or following a material legal or regulatory change.

Information Commissioner's Office. Guide to data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
Information Commissioner's Office. Contracts and liabilities between controllers and processors. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/contracts-and-liabilities-between-controllers-and-processors-uk-gdpr/
UK legislation. Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents
UK legislation. Data Use and Access Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents