**DATA PROCESSING AGREEMENT FOR SPECIALIST SUPPORT UNDER BUILDING BETTER SOMERSET FRAMEWORK**

**CONTENTS**

**Clause Page No.**

**1. Interpretation** ………………………………………. **3**

**2. Purpose** ……………………………………………... **3**

**3. Obligations** …………………………………………. **3**

**4. Data Security Breaches** ………………………….. **4**

**5. Onward Disclosure**………………………………... **5**

**6. Commencement and Period of Operation** ……. **5**

**7. Variation** …………………………………………….. **5**

**8. Subject Access Requests** ……………………….. **5**

**9. Information Assurance** …………………………... **5**

**10. Dispute Resolution** ……………………………… **6**

**11. Governing Law** …………………………………… **6**

The following terms and conditions apply to any and all information provided by Pluss C.I.C to you.

1. **Interpretation**

In this Agreement the following words and phrases will have the following meanings:

"FoIA" means the Freedom of Information Act 2000.

"DPA" means the Data Protection Act 2018.

“GDPR” means the EU General Data Protection Regulation

“Data Controller” has the meaning given in Chapter 2 of the DPA and Article 4 of GDPR

“Processing” & “Process” has the meaning given in Article 4 of the Chapter 2

and the DPA and Article 4 of GDPR

“Personal Data” has the meaning given in Chapter 2 of the DPA and

“Shared Personal Data” Article 4 of GDPR has the meaning given in clause 2.1

“BBS” Building Better Somerset

1. **Purpose**
	1. Somerset Council is the Data Controller and Pluss C.I.C is the Data Processor with third parties being identified as Data Processors under the Data Protection Act 2018.
	2. Information sharing’ is defined as the process of sharing any personal data, using a method

that ensures compliance with the six principles of the DPA (2018) and the guidance provided

by the Information Commissioners Office (ICO) to ensure the share is lawful.

* 1. Any reference in this agreement to the GDPR is effective from the 25 May 2018. The

following additional GDPR provisions will apply:

* 1. Consent must be freely given, specific to the types of processing, informed, and there must

be an indication signifying agreement. GDPR requires the indication must be unambiguous

 and involve a clear affirmative action (Opt-in).

* 1. Records must be retained to demonstrate what the individual has consented to, including

what they were told, when and how they consented.

* 1. Privacy notices shall be updated to identify the lawful basis for processing of personal data.
	2. Compliance with the following Subject rights:
		1. right to be informed;
		2. right of access;
		3. right of rectification;
		4. right to erase (also known as ‘the right to be forgotten’);
		5. right to data portability
		6. right to restrict processing;
		7. right to object; and
		8. rights in relation to automated decision making and profiting
1. **Obligations**
	1. These terms and conditions do not remove or reduce legal obligations or responsibilities, for

example as Data Controllers under the DPA. You agree to comply with the Data Protection

Act 2018 and the GDPR. You agree to adhere to the Data Protection Principles set out in the

Schedule to the DPA and the Sixth Data Protection Principle in particular, which requires that:

Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

* 1. Paragraph 5 of the DPA provides that personal data processing will be legitimised for the purposes of the First Data Protection Principle where; "the processing is necessary (a) for the administration of BBS.” Pluss C.I.C does not indemnify you for any loss caused by a breach of the Data Protection Act or any other law.
	2. You must ensure you have mechanisms in place to address the issues of physical security,

security awareness and training, security management systems development, site-specific

information systems security policy and systems specific security policies and appropriate

security controls.

* 1. Any data used by a third party will only be processed on secure IT equipment (protected

against data corruption, destruction, interception, loss, or unauthorized access). Should there

be a need to transfer Shared Personal Data to a third party controlled IT environment then a

Full Information Security Assessment must be completed and agreed before any transfer

takes place. Any data transfers by email between parties will be secure e-mail.

* 1. You will ensure that data integrity meets existing current legislation and its existing standards

and unless more rigorous or higher standards are required in which case it will seek to attain

such standards.

* 1. Personal Data obtained should not be retained for any longer than is necessary for the

fulfilment of those purposes, when it shall be securely disposed of to comply with Somerset Council requirements.

* 1. Any processing of data is pursuant to the provisions of the Data Protection Act 2018 and shall

be in accordance with the consent obtained by Pluss C.I.C who originally obtained the consent for the use of Personal Data. In the event that consent is withdrawn by a data subject you shall be informed the consent has been withdrawn and all data processing of such data subject’s Personal Data shall cease upon receipt of that notification.

1. **Data Security Breaches**
	1. You will follow your own internal processes on the discovery of a data security breach

escalating to Pluss C.I.C any breaches relating to Personal Data. Pluss C.I.C will escalate these breaches to Somerset Council.

* 1. In compliance with GDPR, a notifiable breach has to be reported to the relevant supervisory

authority within 72 hours of becoming aware of it. The GDPR recognises that it will often be

impossible to investigate a breach fully within that time-period and allows the provision of

information in phases. Pluss C.I.C must be advised of a data security breach within the same

working day of the security breach (within 1 hour of the breach; while some assessment of the

significance of the loss will be apparent in making the initial report; it is important that all

losses or potential losses are reported immediately, without waiting for the results of

investigations or risk assessments. If in doubt, make contact with Information Security

(InfoSec)). Pluss C.I.C will inform the authority within the required 72 hours.

* 1. In the event of a data security breach (or where there is reasonable cause to believe that

such breach may have occurred), data transfers shall cease until the cause or incident is

resolved. If the incident cannot be resolved or if, in the view of Pluss C.I.C, it is very serious, data transfers will stop and will not resume until Pluss C.I.C are satisfied with your security arrangements.

1. **Onward Disclosure**
	1. You shall not disclose the Shared Personal Data received to any third party unless permitted in law, and not without the prior approval of Pluss C.I.C, unless required to do so by law.
	2. You will retain a clear record of any data disclosure and make this available for review at any time by Pluss C.I.C inclusive of obligations under Section 9 to a third party.
2. **Commencement and Period Of Operation**
	1. These terms and conditions shall take effect from receipt of same, and/or on receipt of Shared Personal Data by you.
3. **Variation**

7.1 These terms and conditions, including the Annex, may be varied at any time by Pluss C.I.C.

1. **Subject Access Requests**
	1. In the event you receive a Subject Access Request (SAR) from a data subject, you shall cooperate with Pluss C.I.C in handling, transfer if necessary (effective from 25 May 2018 in compliance with GDPR ‘Data Portability’) and disposing of and must respond to such request promptly and without inordinate delay so as to comply with the SAR time frames and in line with GDPR requirements.
	2. In the event you receive a request under the FoI Act, you shall co-operate with each Pluss C.I.C in handling, transfer if necessary (effective from 25 May 2018 in compliance with GDPR ‘Data Portability’) and disposing of and must respond to such request promptly and in line with the FoI time frame and GDPR requirements.
2. **Information Assurance**
	1. All Shared Personal Data will be managed to the standards identified in Pluss C.I.C Policy
	2. Any data that is necessary to be retained for legal, regulatory and/or compliance purposes will be notified to Pluss C.I.C and will continue to be held in compliance with the GDPR/DPA and retained only as long as necessary and for a period agreed Pluss C.I.C.
	3. The secure destruction or deletion of information will be in a manner that is in agreement with

Pluss C.I.C and as a minimum in compliance with the Somerset Council Requirements. Notification of the completion of secure information destruction or deletion must be given to Pluss C.I.C upon completion.

1. **Dispute Resolution**
	1. The Parties shall each appoint a nominated representative to whom any disputes arising from the operation of this Agreement shall be referred.
2. **Governing Law**

11.1 The formation, existence, construction, performance, validity and all aspects whatsoever these terms and conditions or any term of it (including non-contractual disputes or claims) shall be governed by laws of England and Wales.

**ANNEX A – SHARED PERSONAL DATA**

The personal data to be shared may comprise of the following:

• name

• date of birth

• address

• contact phone number

• email address

Principles relating to processing of personal data

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they

are processed (‘data minimisation’);

1. accurate and, where necessary, kept up to date; every reasonable step must be taken to

ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

1. kept in a form which permits identification of data subjects for no longer than is necessary for

the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

1. processed in a manner that ensures appropriate security of the personal data, including

protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and

confidentiality’).

Processing of special categories of (sensitive) personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or

philosophical beliefs, or trade union membership, and the processing of genetic data, biometric

data for the purpose of uniquely identifying a natural person, data concerning health or data

concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

1. the data subject has given explicit consent to the processing of those personal data for

one or more specified purposes, except where Union or Member State law provide that the

prohibition referred to in paragraph 1 may not be lifted by the data subject;

1. processing is necessary for the purposes of carrying out the obligations and exercising

specific rights of the controller or of the data subject in the field of employment and social

security and social protection law in so far as it is authorised by Union or Member State law or

a collective agreement pursuant to Member State law providing for appropriate safeguards for

the fundamental rights and the interests of the data subject;

1. processing is necessary to protect the vital interests of the data subject or of another

natural person where the data subject is physically or legally incapable of giving consent;

1. processing is carried out in the course of its legitimate activities with appropriate

safeguards by a foundation, association or any other not-for-profit body with a political,

philosophical, religious or trade union aim and on condition that the processing relates solely

to the members or to former members of the body or to persons who have regular contact

with it in connection with its purposes and that the personal data are not disclosed outside

that body without the consent of the data subjects;

1. processing relates to personal data which are manifestly made public by the data subject;
2. processing is necessary for the establishment, exercise or defence of legal claims or

whenever courts are acting in their judicial capacity;

1. processing is necessary for reasons of substantial public interest, on the basis of Union or

Member State law which shall be proportionate to the aim pursued, respect the essence of

Useful materials: • Parental Consent Form • Parental Consent Withdrawal Form EU General

Data Protection Regulation Official Journal of the European Union 4 May 2016 page 9 of 68

the right to data protection and provide for suitable and specific measures to safeguard the

fundamental rights and the interests of the data subject;

1. processing is necessary for the purposes of preventive or occupational medicine, for the

assessment of the working capacity of the employee, medical diagnosis, the provision of

health or social care or treatment or the management of health or social care systems and

services on the basis of Union or Member State law or pursuant to contract with a health

professional and subject to the conditions and safeguards referred to in paragraph 3;

1. processing is necessary for reasons of public interest in the area of public health, such as

protecting against serious cross-border threats to health or ensuring high standards of quality

and safety of health care and of medicinal products or medical devices, on the basis of Union

or Member State law which provides for suitable and specific measures to safeguard the

rights and freedoms of the data subject, in particular professional secrecy;

1. processing is necessary for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes in accordance with Article 89 (1) based on Union or

Member State law which shall be proportionate to the aim pursued, respect the essence of

the right to data protection and provide for suitable and specific measures to safeguard the

fundamental rights and the interests of the data subject.

1. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies