|  |
| --- |
| sportscotland |
| SGBs data processing agreement [TEMPLATE] |
|  |

*This template agreement wording is intended for use by SGBs when engaging third parties to process personal data on behalf of the SGB. It can also be entered into within group SGB structures – for example, between the SGB and any subsidiaries or a British governing body.*

***Except where highlighted in the template wording, SGBs should not amend the text without first obtaining legal advice.***

# Data Processing Agreement [TEMPLATE]

between

[INSERT NAME OF SGB]

and

[INSERT NAME OF SUPPLIER]

This Agreement is between:

1. [INSERT REGISTERED NAME OF SGB], [a company incorporated under the Companies Act 2006 (Company Number [INSERT NUMBER]), a registered Scottish Charity (Charity Number [INSERT NUMBER])], having its registered office at [INSERT REGISTERED ADDRESS] (the “**Customer**”); and
2. [INSERT REGISTERED NAME OF SUPPLIER], a company incorporated under the Companies Act 2006 (Company Number [INSERT NUMBER]), having its registered office at [INSERT ADDRESS] (the “**Supplier**”),

together referred to as the “**Parties**” and separately as a “**Party**”.

Background:

1. The Customer is the Controller in respect of the Customer Personal Data.
2. The Supplier has agreed to carry out certain Processing functions in respect of the Customer Personal Data and to act as a Processor in respect of the Customer Personal Data.
3. The Parties have therefore entered into this Agreement to regulate the Processing of the Customer Personal Data by the Supplier in terms of the Data Protection Legislation.

It is agreed as follows:

1. **Definitions and Interpretation**
	1. The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

“**Agreement**” means this agreement, including the Schedule;

1. "Applicable Law" means:
	1. any law, legislation, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;
	2. the common law and laws of equity as applicable to the parties from time to time;
	3. any binding court order, judgment or decree; and
	4. any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party’s assets, resources or business;

“**Business Day**” means a day (other than a Saturday, Sunday or public holiday) when banks in Edinburgh are open for business;

“**Commencement Date**” means [INSERT DATE];

“**Controller**” has the meaning set out in the Data Protection Legislation;

“**Customer Personal Data**” means any Personal Data received from or on behalf of the Customer, or otherwise obtained, created, generated or compiled in connection with this Agreement, including the categories Personal Data which the Customer has identified for Processing by the Supplier under this Agreement, short particulars of which are set out in Part 1 of the Schedule;

1. “Data Protection Communication”means a complaint, communication or request (other than a Data Subject Request) relating to either party’s obligations under Data Protection Legislation relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from the Information Commissioner’s Office;

“**Data Protection Impact Assessment**”, “**Data Subject**”, “**Information Commissioner’s Office**”, “**Personal Data**” and “**Process**” (including any derivatives thereof) have the meanings set out in the Data Protection Legislation;

1. “Data Protection Legislation” means all Applicable Law relating to the Processing, privacy, and/or use of Personal Data, as applicable to either party or the Purpose, including:
	1. the GDPR;
	2. the Data Protection Act 2018;
	3. any laws which implement or supplement any such laws; and
	4. any laws which replace, extend, re-enact, consolidate or amend any of the foregoing;
2. “Data Subject Request” means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Legislation (but excluding any compensation claim from a Data Subject);

“GDPR” means the General Data Protection Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

1. “Personal Data Breach” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data;

“**Processor**” has the meaning set out in the Data Protection Legislation;

“**Purpose(s)**” means the purpose as determined by the Customer and set out in Part 2 of the Schedule;

“**Schedule**” means the schedule attached as relative to this Agreement;

1. “Sub-Processor” means any third party (other than an employee of the Supplier or of any sub-contractor where that employee is subject to an enforceable obligation of confidence with regards to the Customer Personal Data) engaged by the Supplier or any sub-contractor for carrying out any Processing activities in respect of the Customer Personal Data;
2. “Territory” means the United Kingdom; and
3. “Transfer” (including any derivatives thereof) shall be construed to have the same meaning as the word ‘transfer’ in Article 44 of the GDPR as if references in that Article to ‘personal data’ were to Customer Personal Data as defined in this Agreement. Without prejudice to the foregoing, this term also includes directly or indirectly transferring, disclosing or permitting access to any Customer Data to any International Recipient (including all Transfers from one International Recipient to any other International Recipient).
	1. In this Agreement:
		1. the singular includes the plural and vice versa;
		2. references to statutes, any statutory instrument, regulation or order shall be construed as a reference to such statute, statutory instrument, regulation or order as amended or re-enacted from time to time;
		3. unless a right or remedy of a Party is expressed to be an exclusive right or remedy, the exercise of it by a Party is without prejudice to that Party’s other rights and remedies;
		4. a person includes a corporate or unincorporated body (whether or not having separate legal personality); and
		5. any phrase introduced by the words “including” or “includes” or similar shall be construed as illustrative and shall not limit the generality of the related general words.
4. **Term**

This Agreement shall commence on the Commencement Date and shall continue in full force and effect until completion of the Purpose(s) (the “**Term**”), unless terminated earlier in accordance with Clause 8.

1. **Processor and Controller**
	1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller of the Customer Personal Data and the Supplier is the Processor of the Customer Personal Data.
	2. The Supplier shall comply with all Data Protection Legislation in connection with the Processing of Customer Personal Data and the exercise of its respective rights and obligations under this Agreement and shall not by any act or omission cause the Customer (or any other person) to be in breach of any Data Protection Legislation.
	3. The Customer shall comply with all legally binding Data Protection Legislation in respect of the performance of its obligations under this Agreement.
	4. The Supplier warrants and represents to the Customer that all information it has provided or shall at any time provide to the Customer regarding:
		1. each Sub-Processor (and proposed Sub-Processor);
		2. the security of the Customer Personal Data and any Personal Data Breach; or
		3. any other matter relating to Clauses 3 to 12 (inclusive),

is in all cases true, accurate, complete and not misleading.

1. **Processing instructions**
	1. In respect of the Processing of the Customer Personal Data during the Term, the Supplier undertakes:
		1. unless required to do otherwise by Applicable Law, to Process the Customer Personal Data strictly in accordance with this Agreement, the Customer’s instructions from time to time and the Data Protection Legislation and notify the Customer immediately if it considers that any of the Customer’s instructions infringe Data Protection Legislation;
		2. if Applicable Law requires the Supplier to Process the Customer Personal Data other than in accordance with the Customer’s instructions or is likely to have a substantial adverse effect on the performance of the Supplier’s obligations and commitments in respect of the Customer Personal Data under this Agreement or otherwise prevents it from fulfilling the instructions received from the Customer under this Agreement, to notify the Customer of any such requirement before Processing the Customer Personal Data;
		3. to maintain records of all activities carried out by the Supplier in relation to the Customer Personal Data. Such records shall be in the form prescribed by and contain the information described in the Data Protection Legislation; and
		4. not to disclose or allow access to the Customer Personal Data to any Data Subject or third party other than at the explicit request of the Customer or as may be specifically provided for in this Agreement.
2. **Technical and organisational measures**
	1. The Supplier shall implement and maintain (and at all times comply with) appropriate technical and organisational measures to ensure appropriate security of the Customer Personal Data and safeguard against any unauthorised and unlawful Processing of, and against accidental loss or destruction of, or damage to, the Customer Personal Data, all to the reasonable satisfaction of the Customer. Such measures shall include, but are not limited to:
		1. appropriate measures to ensure the ongoing confidentiality, integrity, availability and resilience of the Supplier’s systems and services;
		2. appropriate measures to restore the availability and access to the Customer Personal Data in a timely manner in the event of a physical or technical incident;
		3. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Customer Personal Data; and
		4. insofar as possible, appropriate measures to assist the Customer in the fulfilment of the Customer’s obligations to respond to Data Subject Requests relating to the Customer Personal Data.
	2. The Supplier shall ensure that on request from the Customer it shall provide an up-to-date copy of the Customer Personal Data (or any part(s)), on such media and within such reasonable time periods as required by the Customer (and in any event within twenty-four (24) hours of request).
	3. Except as agreed by the Parties as a written variation of this Agreement, the Supplier may not make any change to the security measures it applies to the Customer Personal Data from time to time.
3. **Breach notification**
	1. In respect of any Personal Data Breach, the Supplier shall promptly:
		1. notify the Customer immediately (and in any event within twenty-four (24) hours) after becoming aware of the Personal Data Breach; and
		2. provide the Customer immediately (and in any event within twenty-four (24) hours) after becoming aware of the Personal Data Breach with such details as the Customer reasonably requires regarding:
			1. the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Customer Personal Data records concerned;
			2. any investigations into such Personal Data Breach;
			3. the likely consequences of the Personal Data Breach (including details regarding the likely consequences for the Customer and Data Subjects); and
			4. any measures taken, or that the Supplier recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if the Supplier cannot provide all of these details within the timeframes set out in this Clause 6.1.2, it shall (before the end of such timeframes) provide the Customer with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the Customer regular updates on these matters.

* 1. If a Personal Data Breach occurs the Supplier shall (without prejudice to any other right or remedy of the Customer) take such steps and do all acts and things as the Customer requires in order to mitigate the effects of the Personal Data Breach.
	2. In the event that any Customer Personal Data is lost, stolen or subjected to unauthorised access or becomes damaged, corrupted, destroyed or unusable, the Supplier shall restore such Customer Personal Data promptly at its own expense.
1. **Using staff and Sub-Processors**
	1. The Supplier shall not assign, sub-contract or otherwise deal with its obligations under this Agreement without the prior written consent of the Customer.
	2. The Suppler shall not engage (or permit any Sub-Processor to engage) any Processor (or any replacement) for carrying out any Processing activities in respect of the Customer Personal Data without the Customer’s specific prior written authorisation in accordance with Clause 7.3. As at the Commencement Date, the Customer has authorised (and only authorised) use of those Sub-Processors listed in Part 3 of the Schedule.
	3. The Supplier shall submit any request for specific authorisation of an additional Sub-Processor after the Commencement Date at least three (3) months prior to the proposed date of engagement of the relevant Sub-Processor (unless the Customer otherwise agrees). The Customer may withhold, condition or delay any authorisation of the Sub-Processor at its absolute discretion and such authorisation may only take effect by way of a duly binding prior written variation to this Agreement.
	4. Where authorisation is given by the Customer, the Supplier shall ensure that the Sub-Processor is subject to written contractual obligations concerning the Customer Personal Data which are no less onerous than those imposed on the Supplier under this Agreement, such written contract to be entered into before any Customer Personal Data is passed to the Sub-Processor.
	5. The Supplier shall promptly upon request by the Customer provide a copy and all relevant details of any contract entered into under Clause 7.4 to the Customer.
	6. The Supplier shall immediately cease using a Sub-Processor upon receiving written notice from the Customer requesting that the Sub-Processor ceases Processing Customer Personal Data for security reasons or concerns about the Sub-Processor’s ability to carry out the relevant Processing in compliance with Data Protection Legislation or this Agreement.
	7. The Supplier shall ensure that any of its employees who will have access to the Customer Personal Data have undergone data protection training and are aware of their obligations under the Data Protection Legislation, including but not limited to, a duty of confidentiality in respect of the Customer Personal Data.
	8. At all times:
		1. the Supplier shall be liable for the acts and omissions of each Sub-Processor and each of its employees as if each Sub-Processor’s and each employee’s acts or omissions were the Supplier’s acts or omissions (including that where any Sub-Processor fails to fulfil its obligations in accordance with any contract with the Supplier, the Supplier shall remain fully liable to the Customer for the performance of that Sub-Processor’s obligations);
		2. any obligation on the Supplier to do, or to refrain from doing, any act or thing under this Agreement or otherwise shall include an obligation upon the Supplier to procure that all Sub-Processors and the Supplier’s employees also do, or refrain from doing, such act or thing; and
		3. the appointment of any Sub-Processor shall not relieve the Supplier of its obligations under this Agreement.
2. **Data protection assistance and Data Subject Rights**
	1. The Supplier shall:
		1. in the case of each Data Subject Request the Supplier receives:
			1. immediately record it; and
			2. refer it to the Customer within two (2) Business Days of receipt;
		2. provide such information and co-operation and take such action as the Customer reasonably requests in relation to each Data Subject Request or other communication relating to the Customer Personal Data;
		3. not respond to any Data Subject Request or communication relating to the Customer Personal Data without the Customer’s prior written approval;
		4. provide the Customer with such information as the Customer may require to satisfy itself that the Supplier is complying with its obligations under the Data Protection Legislation, including contributing to audits and inspections conducted by the Customer or another party authorised by the Customer under Clause 10;
		5. notify the Customer immediately (and in any event within twenty-four (24) hours) if it receives a complaint, notice or any other communication concerning the Supplier’s Processing of the Customer Personal Data;
		6. to assist the Customer with any notifications to the Information Commissioner’s Office or Data Subjects where required under the Data Protection Legislation;
		7. to provide the Customer with such assistance as the Customer reasonably requires in relation to the carrying out of a Data Protection Impact Assessment relating to the Processing of the Customer Personal Data, including where the Customer engages in a consultation with the Information Commissioner’s Office in relation to the Supplier’s Processing of the Customer Personal Data; and
		8. restrict any Processing, return or delete the Customer Personal Data immediately as directed by the Customer.
3. **International transfers**

The Supplier shall not (and shall ensure each Sub-Processor shall not) Transfer nor permit any Transfer of any Protected Data to any country or territory outside the Territory or to any organisation that is located or operates outside the Territory without the Customer’s prior written authorisation. The Supplier acknowledges that at the Commencement Date no such written authorisation has been granted by the Customer. The parties agree that no future written authorisation shall be effective for the purposes of this Clause 9 unless made as a written variation of this Agreement.

1. **Audits**
	1. The Customer is entitled to appoint an auditor (whether internal or independent), to inspect the Supplier’s compliance with this Agreement and the Data Protection Legislation at any time during the Term provided that the Customer ensures that any such auditor:
		1. has, in the view of the Customer, the necessary professional qualifications to conduct such an audit; and
		2. is bound by a duty of confidentiality in relation to the Customer Personal Data.
2. **Confidentiality**
	1. Subject to Clause 11.2, the Supplier shall keep confidential and shall not disclose to any other person the Customer Personal Data except as expressly permitted under this Agreement. The Supplier may disclose Customer Personal Data to its employees and Sub-Processors on a need-to-know basis and only to the extent necessary for the purposes of this Agreement and in each case only to the extent such disclosure does not conflict with any other provision of this Agreement. To the extent the Supplier is permitted to disclose any Customer Personal Data to any Sub-Processor or employee it shall (without prejudice to any other obligation under this Agreement) do so under conditions of confidentiality substantially the same as in this Clause 11.
	2. Clause 11.1 shall not apply to information that is required to be disclosed in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure.
3. **Warranties and Indemnities**
	1. Each Party warrants that it has full legal authority to enter into this Agreement.
	2. The Supplier undertakes and warrants that it will:
		1. collect and Process the Customer Personal Data in compliance with the Data Protection Legislation and this Agreement;
		2. ensure that the Customer Personal Data is kept secret and confidential; and
		3. fully assist the Customer in ensuring compliance with the obligations under the Data Protection Legislation and within the timescales required by the Data Protection Legislation.
	3. The Supplier agrees to indemnify and keep indemnified the Customer fully on demand against all losses arising from any breach by the Supplier or any Sub-Processors or third parties engaged by the Supplier, of this Agreement and/or as a result of any claim made or brought by an individual or other legal person in respect of any loss, damage or distress caused to them as a result of the Supplier’s unauthorised Processing, unlawful Processing, destruction of and/or damage to any Customer Personal Data Processed by the Supplier or any Sub-Processors or third parties engaged by the Supplier.
4. **Ownership**

All right, title and interest in the Customer Personal Data shall vest solely in the Customer.

1. **Termination**

This Agreement may be terminated with immediate effect by the Customer giving written notice to the Supplier where the Supplier is in breach of any material obligation under this Agreement and, where the breach is capable of remedy, the Supplier has failed to remedy the breach within fourteen (14) days of receipt of notice so to do.

1. **Consequences of termination**
	1. The Parties agree that on expiry of the Term or earlier termination of this Agreement (howsoever caused), the Supplier and any Sub-Processor shall, at the choice of the Customer, either:
		1. return all the Customer Personal Data transferred including any data storage media supplied to the Supplier, including all Customer Personal Data created for the performance of this Agreement, and the copies thereof to the Customer within any timescales specified by the Customer and the Supplier warrants that it will guarantee the confidentiality of the Customer Personal Data transferred and will not actively Process the Customer Personal Data anymore; or
		2. destroy all the Customer Personal Data and certify to the Customer that it has done so within any timescales specified by the Customer, unless legislation imposed upon the Supplier prevents it from returning or destroying all or part of the Customer Personal Data. In that case, the Supplier warrants that it will guarantee the ongoing confidentiality of the Customer Personal Data retained and will not actively Process the Customer Personal Data transferred anymore other than for the purpose to enable it to comply with such legislation.
2. **Waiver**

Failure by either Party to exercise or enforce any rights or remedies available to that Party or any delay in exercising the same shall not be construed as a waiver thereof under this Agreement.

1. **No Variation**

This Agreement shall not be amended and no variation to its terms shall be effective unless such amendment or variation is in writing by a document expressed to be supplemental to this Agreement and is signed by authorised representatives of each of the Parties.

1. **Invalidity**

The invalidity, illegality or unenforceability in whole or in part of any of the provisions of this Agreement shall not affect the validity, legality and enforceability of the remaining part or provisions of this Agreement.

1. **Notices**
	1. Any notice to, or demand to be served by, one Party on another Party in terms of this Agreement may be delivered or sent by first-class recorded delivery post to that Party at its address appearing in this Agreement or at such other address as it may have notified to the other Party in accordance with this Clause 19, or as a signed document sent in PDF format by email to such email address as may be intimated by each Party to the other from time to time.
	2. Any such notice or demand shall be deemed to have been served:
		1. if delivered, at the time of delivery;
		2. if posted, at 10am on the second day after it was put into the post;
		3. if emailed within the Business Day, on that Business Day; or
		4. if emailed after 5pm, on the next Business Day.
	3. In proving service of a notice or demand, it shall be sufficient to prove that delivery was made or that the envelope containing the notice or demand was properly addressed and posted as a pre-paid first-class recorded delivery letter, as the case may be.
2. **Governing Law**
	1. This Agreement and any disputes or claims arising out of or in connection with it, its subject matter or formation (including non-contractual disputes or claims) is governed by, and shall be construed in accordance with, Scots law.
	2. The Parties submit to the exclusive jurisdiction of the Scottish courts for all purposes relating to this Agreement and any disputes or claims arising out of, or in connection with it, its subject matter or formation (including non-contractual disputes or claims).

IN WITNESS WHEREOF these presents typewritten on this and the [eight (8)] preceding pages, together with the Schedule attached as relative hereto, are executed as follows:

|  |  |
| --- | --- |
| Subscribed for and on behalf of [INSERT REGISTERED NAME OF SGB]  |  |
| at |  |
| on | [Director / Authorised Signatory] |
| before |  |
|  | Witness (Signature) |
|  | Witness Name (Please Print) |
|  | Witness Address |
|  |  |

|  |  |
| --- | --- |
| Subscribed for and on behalf of [INSERT REGISTERED NAME OF SUPPLIER]  |  |
| at |  |
| on | [Director / Authorised Signatory] |
| before |  |
|  | Witness (Signature) |
|  | Witness Name (Please Print) |
|  | Witness Address |
|  |  |

This is the Schedule referred to in the foregoing agreement between [INSERT REGISTERED NAME OF SGB] and [INSERT REGISTERED NAME OF SUPPLIER].

Schedule Part 1

Personal Data

The Customer has defined that the following categories of Personal Data will be collected and Processed by the Supplier under this Agreement:

* [INSERT TYPES OF DATA TO BE PROCESSED BY THE SUPPLIER]
* [name and title];
* [addresses];
* [date of birth];
* [telephone number];
* [professional, commercial or business e-mail address]; and
* [Sensitive Personal Data and Special Categories Personal Data (information about race and ethnic origin, political opinions, religious or philosophical convictions, trade union membership, health or sexuality)].

The Customer has defined the following Data Subject categories from who the Customer Personal Data will be collected and Processed by Supplier under this Agreement:

* [INSERT CATEGORIES OF DATA SUBJECT E.G. MEMBERS]; and
* [INSERT].

Schedule Part 2

Purpose

[INSERT PURPOSE(S) OF PROCESSING CUSTOMER PERSONAL DATA]

**Schedule Part 3**

**Authorised Sub-Processors**

[INSERT LIST OF AUTHORISED SUB-PROCESSORS AT START OF AGREEMENT]