**Schedule 20 (Processing Data)**

# Status of the Controller

 1. The Parties acknowledge that for the purposes of the Data Protection

Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the Data Protection Legislation. A Party may act as:

(a) “Controller” in respect of the other Party who is “Processor”; (b) “Processor” in respect of the other Party who is “Controller”;

1. “Joint Controller” with the other Party;
2. “Independent Controller” of the Personal Data where the other Party is also

“Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

# Where one Party is Controller and the other Party its Processor

1. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
4. a systematic description of the envisaged Processing and the purpose of the Processing;
5. an assessment of the necessity and proportionality of the Processing in relation to the Services;
6. an assessment of the risks to the rights and freedoms of Data Subjects; and
7. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

1. Process that Personal Data only in accordance with Annex 1 *(Processing*

*Personal Data*), unless the Processor is required to do otherwise by Law. If it

is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

1. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
	1. nature of the data to be protected;
	2. harm that might result from a Personal Data Breach;
	3. state of technological development; and
	4. cost of implementing any measures; (c) ensure that :
	5. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
	6. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
		1. are aware of and comply with the Processor’s duties under this Schedule 20, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
		2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
		3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
		4. have undergone adequate training in the use, care, protection and handling of Personal Data;
2. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
	1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or Part 3 of the Data Protection Act 2018) as determined by the Controller;
	2. the Data Subject has enforceable rights and effective legal remedies;
	3. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound,

uses its best endeavours to assist the Controller in meeting its obligations); and

* 1. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
1. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 of this Schedule 20, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

1. receives a Data Subject Access Request (or purported Data Subject Access Request);
2. receives a request to rectify, block or erase any Personal Data;
3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
6. becomes aware of a Personal Data Breach.
7. The Processor’s obligation to notify under paragraph 6 of this Schedule 20 shall include the provision of further information to the Controller, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Schedule 20 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
9. the Controller with full details and copies of the complaint, communication or request;
10. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
11. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
12. assistance as requested by the Controller following any Personal Data Breach; and/or
13. assistance as requested by the Controller with respect to any request from the

Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule 20. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

1. the Controller determines that the Processing is not occasional;
2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
4. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
5. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
6. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
7. notify the Controller in writing of the intended Subprocessor and Processing;
8. obtain the written consent of the Controller;
9. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Schedule 20 such that they apply to the Subprocessor; and
10. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
11. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
12. The Buyer may, at any time on not less than 30 Working Days’ notice, revise this Schedule 20 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
13. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Buyer may on not less than 30 Working Days’ notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

# Where the Parties are Joint Controllers of Personal Data

16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary

to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Schedule 20 (*Processing Data*).

# Independent Controllers of Personal Data

1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Schedule 20 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
5. The Parties shall only provide Personal Data to each other:
6. to the extent necessary to perform their respective obligations under the Contract;
7. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
8. where it has recorded it in Annex 1 *(Processing Personal Data).*
9. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
10. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
11. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **(“Request Recipient”)**:
12. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
13. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
	1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
	2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
2. implement any measures necessary to restore the security of any compromised Personal Data;
3. work with the other Party to make any required notifications to the Information

Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

1. not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
2. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*
3. Personal Data shall not be retained or processed for longer than is necessary to perform each Party’s respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.
4. Notwithstanding the general application of paragraphs 2 to 15 of this Schedule

20 to Personal Data, where the Supplier is required to exercise its regulatory

and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Schedule 20.

# Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer’s Data Protection Officer are: dpo@cabinetoffoce.gov.uk

1.2 The contact details of the Supplier’s Data Protection Officer are: **[Insert** Contact details]

1.3 A Processor shall comply with any further written instructions with respect to Processing by the Controller.

 1.4 Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description**  | **Details**  |
| Identity of Controller for each Category of Personal Data  |  **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of any personal data processed by the Supplier in providing the Services. In particular the Buyer will not be a Controller for any personal data processed by the Supplier in providing helpline or website services |
| Duration of the Processing  | The duration of the contract.  |  |  |

|  |  |  |
| --- | --- | --- |
| Nature and purposes of the Processing  |  | The Supplier will obtain personal information from helpline and website users. This data will involve the personal experiences of individuals which may include physical, emotional and mental abuse directed at an individual or individuals. These may include criminal actions perpetrated by against or even by the users. We anticipate the majority of calls will be requesting help and guidance, with the Supplier recording any such help and guidance given.The provider is required to record to be agreed upon demographic data of callers, such as:* Sexual Orientation
* Gender Identity
* Age
* Race
* Disability

These are voluntary questions only and users are not required to provide answers to any such questions.The Supplier will also be required to take notes of the individuals call/experience, unless asked not to by the user. These are to be grouped by theme of call, using one or more identifiers e.g. tagging experiences such as violence, talk therapy, gender identity etc.This will allow the Supplier to provide statistical reporting on demographic data, the emerging themes of calls, and anonymised case studies, without disclosing to the Buyer user identities. No personal data of those helped is to be passed to the Buyer. The Supplier will not be allowed to utilise the data gathered for any purposes other than to provide the Services, report statistics to the Buyer on an agreed upon schedule and format, and its own efforts to refine, enhance, and further develop the Victim Support Service.The Supplier will be required to securely store and destroy data stored, as described above, in accordance with best practice, legal, and regulatory requirements. If at any time the Supplier is unable to complete the contract and a new tender is required, the Supplier will ensure business continuity in the form of data back ups. This will allow a new supplier to ensure it can continue to provide assistance to repeat callers and ongoing issues without additional disruption.The Supplier will also host the data of its employees, contractors, recruitment processes, suppliers, etc, that are to be expected in the day to day operation of any business or organisation. These must be compliant with the relevant legal, regulatory and best practice regulation. |
| Type of Personal Data  | The Supplier will be expected to store data of staff such as names, date of birth, national insurance numbers, any equality and diversity monitoring, contact details, next of kin, bank details, etc, as required in the course of employing staff and/or contractors.The Supplier will be expected to store the data of Service Users such as names, age, gender identity, sexual orientation, and race, alongside requests for assistance, personal experience etc. |
| Categories of Data Subject  |  |  * Staff (including volunteers, agents, temporary workers etc)
* Customers (Service Users across the helpline and website)
* Suppliers (Office suppliers, website maintenance, and external links to services, for example, Emergency Housing or Counselling services)
* Contractors and Consultants (Web developers, training consultants etc.)
 |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data  |  | The Supplier will be required to preserve the personal data of the specified categories of data subjects in line with legal, regulatory, and best practice requirements. Personal data collected by the Supplier during the course of the contract may be retained by them after the contract ends in order that they can continue to provide support to those who need it. The Supplier will continue to be an independent Controller for any such personal data.] |

# Annex 2 - Joint Controller Agreement 1. Joint Controller Status and Allocation of Responsibilities

1.1 NOT USED.