



ABU DHABI, UAE

Help Information Technology Consultancy LLC

Etisalat T&A Building, 6th Floor

Old Airport Road, Opposite to HSBC Bank

PO Box 37195 Abu Dhabi, UAE



800 HELPAG (800 435 724)



HELP AG

an **e&enterprise** company

HELP AG DATA PROCESSING AGREEMENT (DPA)

REFERENCE	VERSION	ISSUE DATE
[Reference]	1.0	05/10/2022

Document Control

AUTHOR	REVIEWER	VERSION
Hemen Goradia	Soeren Kroh	0.1
Hemen Goradia	Soeren Kroh	1.0

Revision History

VERSION	DATE ISSUED	STATUS	REASON FOR CHANGE	CHANGED BY
0.1	04/09/2022	DRAFT	Initial Draft Document	Hemen Goradia
1.0	05/09/2022	FINAL	Final Document	Soeren Kroh

Reviewers

DEPARTMENT	NAME
Data Protection Office	Hemen Goradia – Data Protection Officer (DPO)
Help AG Management	Soeren Kroh – Chief Operating Officer (COO)

Intellectual Property Rights

This document contains valuable trade secrets and confidential information of Help AG and its suppliers and partners. Any content shall not be disclosed to any person, organization or entity unless such disclosure is subject to the products provisions of a written non-disclosure agreement and proprietary rights agreement, or intellectual property license agreement approved by Help AG. The distribution of this document does not grant any license or rights in whole or in part to the content, the product(s), technology or intellectual property described herein.



ABU DHABI OFFICE

Help Information Technology Consultancy LLC

Etisalat T&A Building, 6th Floor
Old Airport Road, opposite to HSBC Bank
PO Box 37195 Abu Dhabi, UAE

+971 2 644 3398
+971 2 639 1155
www.helpag.com
info@helpag.com

CONTENTS

A.1	Data Protection	1
A.2	Data Processing Agreement (DPA)	1
A.3	Annex 1: Description of Personal Data Processing [to be completed by the Third Party].....	7
A.4	Annex 2: Description of the Processor's Security Measures [to be completed by the Third Party]	8

A.1 Data Protection

Below clauses to be included in the main body of the contracts with Third Parties (as applicable)

1. In the course of provision of the Services to the Client pursuant to this Agreement, the Service Provider may process or handle personal data on behalf of the Client. The Service Provider agrees to comply with the provisions as set out in [\[reference the section where Data Processing Agreement is placed\]](#) with respect to any personal data collected and processed for or behalf the Client in relation to the Services.
2. The Service Provider further represents and warrants that:
 - a. it complies with all applicable data protection laws and regulations, and has a privacy policy in place governing the use of personal data that meets or exceeds the applicable Data Protection Laws and Regulations; and
 - b. no personal data originating from the European Economic Area (EEA) and the United Kingdom shall be processed or otherwise shared with the Client in respect to any of the Services to be provided under this Agreement. (where applicable)

A.2 Data Processing Agreement (DPA)

Below DPA to be included in the contracts with Service Providers (as applicable)

1. This Data Processing Agreement ("DPA") forms part of the services agreement between [\[insert name of company\]](#) (the "Processor") and HELP AG (the "Controller") dated [\[insert date\]](#) bearing the reference number [\[insert reference number\]](#) (the "Agreement") to reflect the Parties' agreement with regard to the processing of Client Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.
2. In the course of providing the Services to the Controller pursuant to the Agreement, the Processor may Process Personal Data on behalf of the Controller. The Processor agrees to comply with the following provisions with respect to any Personal Data submitted by or for the Controller or collected and processed by or for the Controller for the duration of the provision of the Services.
3. If there is any inconsistency between the documents comprising the Agreement and this DPA relating to the Processing of Personal Data, the terms and conditions of this DPA shall take priority.

DEFINITIONS

4. The definitions that are set out in this DPA:
 - (i) shall apply to this DPA only and to the exclusion of any same or similar terms used in other documents which form part of the Agreement
 - (ii) do not replace, amend or take priority over the same or similar terms when used in the context of documents other than this DPA which make up the Agreement; and
 - (iii) in the event of a conflict or inconsistency between such definitions and the Data Protection Laws and Regulation, the Data Protection Laws and Regulations shall take precedence.

5. In this DPA, save where the context requires otherwise, the following words and expressions have the following meaning:

"Affiliates" means (i) in relation to the Controller all other Departments or entities owned by or associated with HELP AG, and (ii) in relation to the Processor, any companies controlling, being controlled by, or under common control with the Processor, whether directly or indirectly.

"Client Data" means any Personal Data provided by the Controller to the Processor or collected by the Processor on the Controller's behalf, including Personal Data uploaded to or created on a platform provided by the Processor or accessed by the Processor on the Controller or third-party systems.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws and Regulations" or "Regulations" means all applicable data protection and privacy laws.

"Data Subject" means the individual to whom Personal Data relates, being affected by the Processing.

"Good Industry Practice" means standards, practices, methods, and procedures conforming to the degree of skill and care, diligence, and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances.

"Personal Data" means any information, including Client Data, which alone or in combination with other information can be used to identify a living individual where protected under Data Protection Laws and Regulations, where such data is Processed by the Processor; an identifiable person is one who can be identified, directly or indirectly, notably but not limited to, by reference to a user identification such as a name, an identification number, geo-location data, an online user identification, or by reference to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity;

"Process" (or "Processed" or "Processing") means any operation or set of operations which is performed upon Personal Data (in general, any use of Personal Data), whether by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, disclosure or otherwise making available, duplication, transmission, combination, blocking, redaction, erasure, or destruction.

"Security Breach" means actual or reasonably suspected accidental, unauthorized, or unlawful access, acquisition, alteration, loss, destruction or disclosure of Client Data by the Processor or its Sub-processors (if any).

"Services" means the services to be performed by the Processor under the Agreement.

"Sub-processor" means any Data Processor engaged by the Processor; and

"Supervisory Authority" means any independent and competent public regulatory authority including data protection authorities and law enforcement agencies.

PROCESSING OF PERSONAL DATA

6. The Parties acknowledge and agree that with regard to the Processing of Personal Data, the Controller is the Data Controller, the Processor is a Data Processor, and that the Processor may engage Sub-processors pursuant to the requirements set forth in Clauses 14, 15 and 16 (Sub-processors) below.

7. The Parties agree that the Processor shall Process Personal Data (including Client Data) for the purposes and for the provision of the Services. [\[Annex 1\]](#)- (Description of Personal Data Processing) of this DPA sets out a description of the Personal Data Processing undertaken by the Processor.
8. The Processor shall:
 - i. Process Personal Data only as necessary to perform the Services or otherwise as expressly authorized in writing by the Controller.
 - ii. comply with the terms of this DPA and all applicable Data Protection Laws and Regulations relating to the collection or use of Personal Data.
 - iii. only Process Personal Data in accordance with the Agreement.
 - iv. agree and hereby agrees that the Controller is the sole owner and controller of Personal Data and has the sole right to determine the purposes for which the Processor may Process Personal Data; and
 - v. only Process Personal Data as a Data Processor acting in accordance with the instructions of the Controller.
9. The Processor shall notify the Controller in writing of any changes to the Services which will prevent the Processor from complying with its obligations under this DPA or significant changes to the functionality of the contracted Service which may impact the Processing of Personal Data

TRANSFER OF PERSONAL DATA

10. If any Client Data originates from any country with one or more laws imposing data transfer restrictions or prohibitions, Processor shall ensure appropriate transfer mechanism (satisfying the country's data transfer requirement(s)) is in place, before transferring or accessing Customer Data outside of such country.

RIGHTS OF DATA SUBJECTS

11. To the extent the Controller, in its use of the Services, does not have the ability to correct, amend, block, or delete Personal Data, as required by Data Protection Laws and Regulations, subject to applicable law and any confidentiality obligations, the Processor shall use reasonable endeavors to comply with any commercially reasonable request by the Controller to facilitate such actions.
12. The Processor shall, to the extent legally permitted, promptly notify the Controller if it receives a request from a Data Subject for access to, correction, amendment, or deletion of that person's Personal Data. The Processor shall not respond to any such Data Subject request without the Controller's prior written consent except to confirm that the request relates to the Controller. The Processor shall provide the Controller with all commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent the Controller does not have access to such Personal Data through its use of the Services.

PROCESSOR'S PERSONNEL

13. The Processor shall:
 - i. ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have agreed in writing to maintain the confidentiality of Client Data.

- ii. take commercially reasonable steps to ensure the reliability of any of the Processor's personnel engaged in the Processing of Personal Data.
- iii. ensure that the Processor's access to Personal Data is limited to those personnel who require such access to perform the Agreement; and
- iv. appoint a data protection officer where such appointment is required by Data Protection Laws and Regulations. The Processor shall notify the Controller of any such appointment and provide the Controller with the contact information of the appointed data protection officer.

SUB-PROCESSORS

14. The Controller acknowledges and agrees that: (a) the Processor's Affiliates may be retained as Sub-processors, and (b) the Processor and its Affiliates respectively may engage third party Sub-processors in connection with the provision of the Services, subject to compliance with the requirements of Clauses 16 and 17 below.
15. To the extent the Processor uses Sub-processors to Process Client Data, the Processor shall make available to the Controller a current list of Sub-processors (including the Processor's Affiliates) for the respective Services with the identities of those Sub-processors, including full details of the Processing to be undertaken by the Sub-processors ("Sub-processor List"). The Processor shall provide the Controller with a mechanism to subscribe to updates to the relevant Sub-processor List and shall provide such updates before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services. If Controller notifies Processor in writing of any objections to any Sub-processors appointed or proposed to be appointed by the Processor:
- a) Processor shall work with Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that Sub-processor; and
 - b) where such a change cannot be made within thirty (30) days from Processor's receipt of Controller's notice, notwithstanding anything contrary in the Agreement, Controller may by written notice to Processor with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.
16. The Processor shall be liable for the acts and omissions of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

DATA SECURITY REQUIREMENTS

17. The Processor shall implement reasonable technical and organizational measures to:
- i. protect Personal Data against accidental loss or damage and unauthorized access, use, disclosure, alteration, or destruction.
 - ii. ensure the confidentiality, security, integrity, and availability of Personal Data; and
 - iii. securely dispose of Personal Data and tangible property containing Personal Data (as and when required), taking into account available technology so that such information cannot be practicably read or reconstructed,
 - iv. such technical and organizational measures are described in further detail in [\[Annex 2\]](#) - (Description of the Processor's Security Measures).

18. The Processor shall adopt reasonable technical and organizational measures to fulfil its obligations in accordance with Good Industry Practice, which shall include but not be limited to the security requirements set out in or referred to in this DPA or otherwise agreed in writing by the Controller.
19. The Processor shall document, in a written security policy, Personal Data handling procedures designed to implement technical and organizational measures to protect Personal Data as required by the applicable Data Protection Laws and Regulations and this DPA.
20. Upon the Controller's prior written request, the Processor shall provide details of the Processor's information security measures and controls applicable to the provision of the Services under the Agreement and sufficient to demonstrate compliance with applicable Data Protection Laws and Regulations and this DPA.
21. The Processor shall document its policies and procedures to recover Personal Data and the Services following an unplanned event resulting in an interruption of or inaccessibility to Personal Data and the Services.
22. Access to Personal Data must only be granted to the Processor's personnel that:
 - i. the Processor has taken reasonable steps to ensure the reliability of.
 - ii. are granted the minimum access level(s) necessary to perform their job function.
 - iii. have been trained in the proper handling of Personal Data; and
 - iv. are subject to written obligations of confidentiality in respect of Personal Data.
23. The Processor shall implement logging and auditing techniques for the Personal Data Processing it undertakes, in relation to access to Personal Data that are in accordance with Good Industry Practice.
24. The Processor must encrypt all Personal Data it Processes on behalf of the Controller where such Processing takes place using laptops or other electronic portable devices

SECURITY AND BREACH NOTIFICATION

25. The Processor shall maintain appropriate security incident management policies and procedures.
26. The Processor shall:
 - i. promptly notify the Controller (and in all cases no later than 48 hours of becoming aware) of any Security Breach of which it becomes aware.
 - ii. provide reasonable cooperation with the Controller's investigation into the Security Breach and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation, and remediation of each such Security Breach; and
 - iii. unless legally required by Data Protection Laws and Regulations or compelled under a subpoena, court order or similar legal document issued by a court or Supervisory Authority, the Processor agrees that it will not disclose the Security Breach to any third party without first obtaining the Controller's prior written consent.
27. Each Party shall reasonably cooperate with the other Party to facilitate compliance with Data Protection Laws and Regulations, including but not limited to notification of affected individuals and Supervisory Authorities.

NOTICES

28. The Processor shall immediately notify the Controller (unless legally prohibited) of any request for disclosure of Client Data by any law enforcement or other government authority. The Processor shall cooperate fully with the Controller in relation to requests for the disclosure of Client Data and where legally permitted shall delay the disclosure of Client Data pursuant to such requests to enable the Controller to investigate and respond to the request for Client Data.
29. The Processor shall promptly notify the Controller if, at any time, it is unable to comply with the terms of this DPA or Data Protection Laws and Regulations. Any failure by the Processor to comply with the terms of this DPA or Data Protection Laws and Regulations shall be considered a material breach of the Agreement and the Controller may terminate in accordance with the Agreement.

RETURN AND DELETION OF THE CLIENT DATA

30. The Processor shall return all Client Data to the Controller and delete Client Data in accordance with the Controller's instructions. The Parties agree that a certificate of deletion of Personal Data (including Client Data) shall be provided by the Processor to the Controller.
31. The Processor shall at the request of the Controller provide reasonable assistance in the transfer or migration of Personal Data to a new service provider.

AUDITS AND CERTIFICATIONS

32. The Parties agree that the Controller shall have the right to audit the Processor's compliance with the terms of this DPA and Data Protection Laws and Regulations in accordance with the following procedure:
- i. upon the Controller's prior written request, the Processor shall make available to the Controller (or the Controller's independent, third-party auditor) information sufficient to establish the Processor's compliance with the obligations set forth in this DPA and Data Protection Laws and Regulations ("Compliance Obligations"); and
 - ii. such information shall include documentation reasonably necessary to confirm the Processor's compliance with its Compliance Obligations.

LIABILITY AND INDEMNITY

33. The Processor shall defend, indemnify and hold harmless the Controller, its personnel, representatives and its Affiliates (the "Indemnified Persons") from and against any and all claims, damages, liabilities, losses (including any loss of, or damage to, any property of, or injury to or death of, any person) and expenses of any kind whatsoever (including the costs in connection with defending against any of the foregoing or in enforcing this indemnity) incurred or suffered by the Indemnified Persons arising from or in connection with any breach of this DPA and/or the Data Protection Laws and Regulations by the Processor.
34. The Processor's obligations under the clauses of this DPA shall survive the termination of the Agreement.

(Please briefly outline the purposes that Personal Data is Processed for under the Agreement. The purposes will generally align with the description of the Services being provided under the Agreement and the functionality of the system the Personal Data will be Processed in.)

Brief Description of Services:

(Please provide a brief overview of the Service being provided as it relates to or require the Processing of Personal Data, please include an overview of the types of Processing operations and/or how the Personal Data will be Processed.)


Time Frame for the Services:


(Please outline the time frame that Personal Data will be Processed for as part of the Services.)

A.4 Annex 2: Description of the Processor's Security Measures [to be completed by the Third Party]




 **ABU DHABI OFFICE**
Help Information Technology Consultancy LLC
Etisalat T&A Building, 6th Floor
Old Airport Road, opposite to HSBC Bank
PO Box 37195 Abu Dhabi, UAE

 +971 2 644 3398

 +971 2 639 1155

 www.helpag.com

 info@helpag.com

