



UNHCR

United Nations High Commissioner for Refugees
Haut Commissariat des Nations Unies pour les réfugiés

Representation for Italy, the Holy See and San Marino

Via Leopardi, 24
00185 Roma, ITALIA

Tel.: +39 06802121
Fax: +39 0680212325
Email: dati@unhcr.org

Letter of Appointment of the External Data Processor

(hereinafter, the “**Letter of Appointment**”)

between

The Office of the United Nations High Commissioner for Refugees in Italy, with registered office at Via Leopardi 24, Roma (RM), registered Italian Tax code No. 80233930587, in its quality of controller of the personal data operated by the same (hereinafter, the “**Controller**”)

and

[•], with registered office in Italy, at [•], registered in [•] with Italian Business Register ID [•], Italian Tax and VAT No. [•], in its quality of processor of the personal data operated by the same (hereinafter, the “**Processor**”)

(hereinafter the Controller and the Processor are jointly referred to as the “**Parties**” or, individually, as a “**Party**”)

whereas:

- A. the Controller and the Processor entered into an agreement (hereinafter, the “**Agreement**”) governing the relationship of the Parties since [•] and contemplating, *inter alia*, the entrustment of certain personal data processing activities, which requires stipulation of a separate agreement for the appointment of an external personal data processor on behalf of the Controller and/or on behalf of the Controller’s client companies, i.e. third party companies, which for the sake of simplicity will be both referred to, for the purposes of this Letter of Appointment, as the Controller;
- B. the Processor declares that it is compliant with Regulation (EU) 2016/679 of the European Parliament and the Council dated 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, the “**Regulation**”) and other applicable rules regarding personal data protection; UNHCR declares it applies data protection rules, regulations and policies reflecting the fundamental principles of the Regulation;
- C. the Controller has identified the Processor as the person with the experience, reliability and capabilities necessary to perform the function of data processor pursuant to Article 28 of the Regulation;
- D. the Processor declares and warrants to have the competence and technical knowledge needed in respect of the purposes and methods of the processing, as well as in relation to the security measures to be adopted to guarantee confidentiality, completeness and integrity of the data processed;
- E. this Letter of Appointment supersedes and replaces any other preceding deed and/or agreement, written and/or oral, between the Parties in relation to the appointment of an external data processor.

In view of the above, the Parties agree as follows.

1. RECITALS AND EXHIBITS

- 1.1 The recitals and exhibits form an integral and essential part of this Letter of Appointment and constitute the exclusive terms of reference for the definition and interpretation of the respective obligations.

2. DEFINITIONS

- 2.1 In addition to the terms expressly defined in other clauses of this Letter of Appointment, the following terms will have the meaning attributed to them below:
- **“Personal Data”**: means, in accordance with Article 4(1) of the Regulation, “any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”
 - **“Data Subject”**: means, in accordance with Article 4(1) of the Regulation, an individual identified or identifiable, directly or indirectly, with particular reference to any of the Personal Data.
 - **“Data Protection Authority”**: competent authority for personal data protection.
 - **“Persons Authorized to Process Personal Data”**: means individuals who, under the applicable legislation, are qualified as “person in charge of the processing” or, according to the provisions of the Regulation, “persons authorised to process personal data”, i.e. those individuals who “operate under the direct authority of the controller or processor, in compliance with the instructions provided”.
 - **“Processing”**: means, in accordance with Article 4(2) of the Regulation, “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

3. SCOPE

- 3.1 Pursuant to this Letter of Appointment, the Processor undertakes to carry out the following Personal Data Processing operations on behalf of the Controller, in compliance with the applicable legislation and, in particular, with the Regulation, according to the terms and conditions provided below.

	Kind of Processing operations	Processing Operations	Purpose of Processing	Categories of Data Subjects	Categories of Personal Data	Storage Period of Personal Data
1.	TBD	TBD	TBD	TBD	TBD	TBD

- 3.2 The Parties agree that the Processor shall not carry out processing operations other than those necessary for the performance and execution of the assigned activities and achievement of the purposes listed in Article 3.1 hereof (hereinafter, the “**Purposes**”). In this regard, the Processor is absolutely forbidden to make copies, partial or total, on paper or magnetic media, of personal data and the database in which they are organized. It is also prohibited to draw up, modify, adapt or translate the data contained in the database by any means and in any form, and to extract and redeploy them, except for the performance of the required activities. Finally, the Processor may not use such data for its own purposes, or assign them for use to third parties, for any reason and on any device.

4. DURATION OF THE LETTER OF APPOINTMENT AND WITHDRAWAL

- 4.1 This Letter of Appointment shall take effect from the date of its execution and shall be in force until the end of the Personal Data Processing activity entrusted under the Agreement, as defined in Recital B. It is understood that upon completion of such activities, this Letter of Appointment will cease to be effective and the Processor shall cease any Personal Data processing on behalf of the Controller.
- 4.2 The Controller may withdraw from this Letter of Appointment during the validity period hereof by written communication to the Processor to be sent by registered letter with return receipt and/or certified e-mail (PEC) with 30 days' prior notice.

5. PROCESSOR'S OBLIGATIONS AND WARRANTIES

- 5.1 Pursuant to this Letter of Appointment, the Processor undertakes to comply with the following provisions in the performance of the Personal Data Processing operations entrusted to the same. In particular, the Processor warrants:
- (a) to carry out every operation necessary to ensure compliance with the provisions established by the Regulation and the applicable personal data protection legislation;
 - (b) that Personal Data Processing performed on behalf of the Controller will be executed with sufficient guarantees through the implementation of technical and organizational measures appropriate for the Purposes, so that each Processing meets the requirements of the Regulation and guarantees the protection of the rights of the Data Subject. The Processor undertakes to adopt all the security measures required pursuant to Article 32 of the Regulation, as well as by other applicable laws. In particular:
 - i. ensure Personal Data pseudonymization and encryption;
 - ii. ensure confidentiality, integrity, availability and resilience of Processing systems and services;
 - iii. promptly restore the availability of and the access to Personal Data in the event of a physical or technical incident;
 - iv. regularly test and evaluate the technical and organizational measures adopted to ensure a high standard of Processing security;
 - v. adhere to codes of conduct and obtain certificates from approved bodies, if available, to demonstrate compliance with the requirements set forth in the Regulation;
 - (c) to perform Personal Data Processing strictly following all the instructions set forth by this Letter of Appointment, as well as any further instructions given by the Controller from time to time;
 - (d) to execute directly, through its organizational structure, all Processing operations entrusted, adhering to the express prohibition to use third-party facilities. If the needs of technical nature, specialization or compliance with the agreed timing or quality of service require intervention of third parties for Personal Data Processing, the Processor, upon written authorization of the Controller, may engage third parties, appointing them as responsible for the processing, in compliance with the provisions of Article 9.2 of this Letter of Appointment;
 - (e) to carry out Personal Data Processing operations in compliance with the provisions of this Letter of Appointment, with full autonomy in management, also from an economic perspective. It is understood that the Controller shall not be required to pay or reimburse any expenses the Processor incurs to comply with the provisions of this Letter of Appointment and the Regulation;
 - (f) to observe utmost confidentiality and professional secrecy of the Personal Data it becomes aware of in the context of its capacity as data processor. Herewith the Processor undertakes to comply with this rule of conduct even after the validity term of this Letter of Appointment;

- (g) to observe the prohibition of communication or disclosure of Personal Data processed; the Processor also warrants that Persons Authorized to Process Personal Data shall make every effort to observe confidentiality or be under an appropriate legal obligation of confidentiality regarding such Personal Data.
- 5.2 The Processor undertakes to keep a record in writing, including in electronic format, of all the Processing activities carried out on behalf of the Controller, in compliance with the provisions of Article 30(2) of the Regulation. The Processor also undertakes to promptly provide, an extract, complete or partial, from such register at Controller's request.
- 5.3 The Processor undertakes to provide the Controller with all references and a copy of the deed of appointment of the Data Protection Officer, in compliance with the provisions of Articles 37 to 39 of the Regulation; otherwise, it undertakes to provide the Controller with a copy of the minutes of the meeting of the management board that issued a resolution containing assessment on failure of appointing the Data Protection Officer.
- 5.4 The Processor undertakes to process the Personal Data only upon documented instruction of the Controller, including in case of transfer of Personal Data to a non-EU country or an international organization, unless required by EU or national law applicable to the Processor; in this case, the Processor shall be required to inform the Controller about such legal obligation before Processing, unless the law prohibits such reporting for reasons of overriding public interest.
- 5.5 The Processor undertakes to cooperate with the Controller in responding to the requests of the Data Protection Authority, in the event of checks and inspections carried out by the latter, as well as contribute to auditing activities, including inspections, carried out by the Controller or another party engaged by the latter. The Processor is obliged to inform the Controller immediately if it considers that an instruction violates the Regulation or other provisions of national or EU law on Personal Data protection.
- 5.6 The Processor undertakes to collaborate with the Controller, with appropriate technical and organizational measures, in the management of relationships with any Data Subject advancing claims arising from the exercise of the rights referred to in Chapter III of the Regulation, providing timely feedback in compliance with methods prescribed therein and the timing identified by the Controller. The Processor undertakes, in particular, to comply with any Data Subject's requests for data portability, to put in place and use technological tools appropriate for Personal Data transmission in a structured and commonly used format readable by an automatic device.
- 5.7 The Processor undertakes to assist the Controller in ensuring compliance with the Personal Data security obligations referred to in Articles 32 to 36 of the Regulation, taking into account the nature of the Processing and the information available to the Processor. In case of Personal Data breach, the Processor undertakes to inform the Controller promptly, as soon as it becomes aware thereof, providing all available information and support, including operational, to enable the Controller to notify the data breach to the Data Protection Authority in accordance with the terms and conditions set forth in Article 33 of the Regulation. The Processor is responsible for any security incidents in relation to the Contract execution to the extent that such incidents are not caused by the Controller. In the event of a security incident, the Processor shall:
- a) provide, immediately and in any case within - four (4) hours from the occurrence, all the information to the Controller with as much detail known at the time as possible and update the latter, in writing and regularly, on the nature of compromised or potentially compromised or threatened data, as well as all the events that may negatively affect the Processor's ability to perform the Agreement;
 - b) provide, within -forty-eight (48) hours, all the information referred to in Article 33 of the Regulation and in particular:

- nature of the breach, categories and number of the data subjects involved, categories and amount of personal data violated;
 - possible consequences of the breach, indicating, where possible, the risks for the rights and freedoms of the data subjects involved;
 - measures proposed to remedy the breach and, where appropriate, mitigate its possible adverse effects;
- c) carry out all the necessary measures to restore the security of compromised systems, files and information;
- d) amend the related policies and procedures to prevent the occurrence of similar events and provide a copy of such amendments to the Controller to obtain the relevant approval.

The Processor also undertakes to keep the Controller informed at all times about any assessments and action plans undertaken in response to any security issue concerning Personal Data.

The Processor undertakes to identify an internal flow of rapid and effective communication of the event, identifying a contact person responsible for receiving the report and initiating the verification of the case and the assessment of the need for notification in favor of the Controller. In the event that the Processor does not communicate a Personal Data breach promptly and in any event no later than the above term, and in any case when it fails to take appropriate technical and organizational measures to ensure adequate security of the Processing as per Article 32 of the Regulation, the Processor shall be liable vis-à-vis the Controller.

- 5.8 The Processor undertakes to promptly inform the Controller of everything of relevance for the purposes of proper compliance with the Personal Data Processing legislation.
- 5.9 The Processor undertakes to indemnify and hold the Controller harmless against any violation concerning Personal Data Processing directly attributable to the Processor and/or third parties appointed as data processors by the Processor.
- 5.10 The Processor also undertakes to indemnify and hold harmless the Controller against any damage, injury, encumbrance, charge, expense, cost or penalty borne by the latter as a result of any kind of breach, directly attributable to the Processor and/or third parties relating thereto, of this Letter of Appointment, the applicable Personal Data protection legislation and/or orders issued by the Data Protection Authority and/or other public bodies, except:
- where the Processor has acted in accordance with the Controller's instructions, this DPA, the Data Protection Laws or other applicable laws; and
 - to the extent that Controller or any third party acting on behalf of the Controller has breached this DPA or any Data Protection Laws to the extent applicable.
- 5.11 Neither party will be liable under this DPA for any loss of actual or anticipated income or profits, loss of contracts or for any special, indirect or consequential loss or damage of any kind howsoever arising and whether caused by tort (including negligence), breach of contract or otherwise, whether or not such loss or damage is foreseeable, foreseen or known.

6. INSTRUCTIONS AND RULES OF CONDUCT FOR THE PROCESSOR

- 6.1 Pursuant to this Letter of Appointment, the Processor undertakes to comply with the following instructions and rules of conduct in the performance of the entrusted Processing operations:

- (a) define the procedures for Personal Data Processing in compliance with what set forth by the Regulation;
- (b) ensure logistical and physical organization of the Personal Data processed, as well as establish the sequence of Processing operations to be carried out;
- (c) identify the Persons Authorized to Process Personal Data and cause formalization of the relevant deed of appointment, accompanied by adequate instructions, with regard to security measures, supervising their work and the correct application of the instructions given and establishing that they have access only to the Personal Data strictly necessary to fulfill the tasks assigned thereto;
- (d) pursuant to the General Provision of the Data Protection Authority dated 27 November 2008 – Measures and precautions prescribed to the holders of processing with electronic tools relating to the functions of system administrator, as amended by the general provision of the Data Protection Authority issued on 25 June 2009 (as subsequently amended):
 - i. identify – by adopting criteria for the assessment of compliance with the requirements of experience, capability and reliability appropriate for ensuring full compliance with the Personal Data Processing provisions in force – and individually designate the persons, in the framework of Processing, to act as system administrator. The written designation shall contain the analytical listing of the permitted areas of operation according to the authorization profile assigned to the individual system administrator;
 - ii. prepare and keep updated at all times a document – to be delivered in copy to the Controller, where expressly required – containing the list of the identifying details of the individuals designated as system administrators with details of the functions assigned to them;
 - iii. monitor the practices of system administrators, at least annually, verifying compliance of their activities with the organizational, technical and security measures concerning Personal Data Processing envisaged by the legislation in force. Such checks may also be carried out by the Controller directly;
 - iv. adopt adequate systems for registration of logical access (computer authentication) to processing systems and electronic archives by system administrators, ensuring that such access logs are complete, inalterable and allow verification of their integrity to the extent required for achievement of their purpose. Such access logs shall include time references and the description of the event that generated them and be kept for a period of no less than 6 (six) months.

7. DATA STORAGE PERIOD

- 7.1 The Processor warrants that, at the time of termination of each Processing operation, for any reason and in any case no later than the expiration date of this Letter of Appointment, it shall delete or return to the Controller, at the discretion and on the indication of the latter, all Personal Data processed, as well as delete the existing copies, in accordance with the terms indicated in Article 3.1 hereof, unless an additional period for the storage of Personal Data is established by a rule of international, EU or national law. In this regard, the Processor undertakes to provide a written declaration concerning the elimination of the Personal Data and/or return of the Personal Data with elimination of all existing copies thereof no later than seven (7) days from the expiry of the Letter of Appointment.

8. CONTROLLER'S POWERS AND OBLIGATIONS

- 8.1 In carrying out the activities hereunder, the Controller undertakes to comply with the fundamental principles in the field of Personal Data protection applicable on the basis of its internal rules, regulations and procedures. The Controller, as subsidiary organ of the United Nations General Assembly, by virtue of its privileges and immunities set forth in the UN

Charter and the 1946 Convention on the Privileges and Immunities of the United Nations, is not subject to the Regulation or national data protection laws.

- 8.2 The Controller may perform, directly and/or indirectly, control and supervisory activities, also by means of periodic checks, with regard to compliance with the obligations and instructions relating to the Processor and/or any Sub-Processor as defined below pursuant to this Letter of Appointment, as required by Article 28(h) of the Regulation.

9. NO ASSIGNMENT OR SUBCONTRACTING

- 9.1 This Letter of Appointment may not be assigned, even partially, to third parties.
- 9.2 The Processor may use another data processor (hereinafter, the “**Sub-Processor**”) for the execution of specific Processing activities on behalf of the Controller, provided that all the following conditions are met:
- (a) the Processor shall enter into a specific agreement with each Sub-Processor reflecting the same data protection obligations as those contained in this Letter of Appointment, providing sufficient guarantees that the Sub-Processor will put in place appropriate technical and organizational measures for the Processing to meet the requirements of the Regulation as well as this Letter of Appointment and provisions of Articles 5.6 and 5.7 hereof;
 - (b) the Processor shall obtain Controller’s prior written authorization to entrust the Sub-Processor with the performance, even partial, of specific Processing activities.
- 9.3 In the event that the Processor entrusts the Processing operations under this Letter of Appointment, in whole or in part, to third parties in a manner not compliant with one or more of the requirements indicated above under letters (a) and (b) such conduct may be considered as a ground for termination of the contractual relationship with the Processor under the Agreement, as well as this Letter of Appointment, with immediate effect.
- 9.4 Should the Sub-Processor fail to fulfill its Personal Data protection obligations, the Processor remains fully liable vis-à-vis the Controller for the fulfillment of these obligations.

10. EXPRESS TERMINATION CLAUSE

- 10.1 The Agreement may be terminated by the Controller with immediate effect, , without prejudice to the right to claim damages, by written notice with registered letter with return receipt, if the Processor fails to comply with any of the obligations set out in Articles 3, 5, 6, 7, 9, 12 or 13 hereof.
- 10.2 The Agreement shall be automatically terminated upon receipt of a notice sent by the party intending to enforce this termination clause, subject to the right to claim damages.

11. CONSIDERATION

- 11.1 The Parties agree that the consideration for the performance of the functions of the data processor by the Processor pursuant to this Letter of Appointment is included in the amount the Controller is required to pay in favor of the Processor, according to the terms and the conditions set forth in the Agreement mentioned under Recital B hereof. Therefore, the Processor acknowledges and agrees that no additional compensation is due in respect of the appointment hereof.

12. CONFIDENTIALITY OBLIGATIONS

- 12.1 The Parties reciprocally undertake, on their own behalf and on behalf of their employees and/or collaborators, to comply with and to cause compliance with the confidentiality obligation with regard to all the information, data, documentation and news, provided in any form, that are deemed confidential and not intended for dissemination to the public.
- 12.2 For the purpose indicated in the previous paragraph, the Parties will take all the necessary preventive measures and, in particular, all legal actions necessary to prevent the disclosure or use of information deemed confidential.
- 12.3 If the disclosure to third parties of information deemed confidential has been caused by acts or facts directly attributable to one of the Parties, such Party shall compensate the other Party for any damage related to the breach of the confidentiality obligation.
- 12.4 The confidentiality obligation referred to in this article shall survive the termination of this Letter of Appointment, on any ground.

13. CODE OF ETHICS AND CODES OF CONDUCT

- 13.1 The Processor represents and warrants that all the activities under this Letter of Appointment will be carried out in compliance with the laws in force.
- 13.2 Any violation by the Processor may therefore determine, in the most serious cases, the termination of this Letter of Appointment and may entail compensation for any damage suffered by the Controller.
- 13.3 For the purposes of interpretation of this Letter of Appointment, with reference to the obligations of the Processor, reference will be made to Italian law.

14. NOTICES

- 14.1 All notices relevant for the purposes of this Letter of Appointment are valid and effective only if made in writing and sent by e-mail to the following addresses:

- For the Processor:
- For the Controller:

or at a different address each of the Parties may communicate to the other in accordance with the provision above, it being understood that the addresses indicated above, or different addresses that may be communicated in the future, are elected by the Parties as addresses for service for any purposes related to this Letter of Appointment, including court documents.

15. DISPUTE SETTLEMENT

- 15.1 The Parties undertake to settle amicably and with the spirit of collaboration any disputes that may arise during the performance of this Letter of Appointment.
- 15.2 Amicable Settlement: The Parties shall use their best efforts to amicably settle any dispute, controversy, or claim arising out of the Contract or the breach, termination, or invalidity

thereof. Where the Parties wish to seek such an amicable settlement through conciliation, the conciliation shall take place in accordance with the Conciliation Rules then obtaining of the United Nations Commission on International Trade Law ("UNCITRAL"), or according to such other procedure as may be agreed between the Parties in writing.

- 15.3 Arbitration: Any dispute, controversy, or claim between the Parties arising out of the Contract or the breach, termination, or invalidity thereof, unless settled amicably under Article 15.1, above, within sixty (60) days after receipt by one Party of the other Party's written request for such amicable settlement, shall be referred by either Party to arbitration in accordance with the UNCITRAL Arbitration Rules then obtaining. The decisions of the arbitral tribunal shall be based on general principles of international commercial law. The arbitral tribunal shall be empowered to order the return or destruction of goods or any property, whether tangible or intangible, or of any confidential information provided under the Contract, order the termination of the Contract, or order that any other protective measures be taken with respect to the goods, services or any other property, whether tangible or intangible, or of any confidential information provided under the Contract, as appropriate, all in accordance with the authority of the arbitral tribunal pursuant to Article 26 ("Interim Measures of Protection") and Article 32 ("Form and Effect of the Award") of the UNCITRAL Arbitration Rules. The arbitral tribunal shall have no authority to award punitive damages. In addition, unless otherwise expressly provided in the Contract, the arbitral tribunal shall have no authority to award interest in excess of the London Inter-Bank Offered Rate ("LIBOR") then prevailing, and any such interest shall be simple interest only. The Parties shall be bound by any arbitration award rendered as a result of such arbitration as the final adjudication of any such dispute, controversy, or claim.

16. PRIVILEGES AND IMMUNITIES:

- 16.1 Nothing in or relating to the Contract shall be deemed a waiver, express or implied, of any of the privileges and immunities of the United Nations, including its subsidiary organs or of UNHCR (as a subsidiary organ of the United Nations).

17. FINAL PROVISIONS

- 17.1 Waiver by one of the Parties of the other Party's failure to comply with any of the provisions of this Letter of Appointment shall not constitute or be interpreted as a waiver in relation to subsequent contractual breaches attributable to the same Party.
- 17.2 Should one of the clauses of the Letter of Appointment be declared void or unenforceable, this Letter of Appointment shall continue to be fully and completely effective, except in relation to the said clause. The Parties shall negotiate in good faith one or more clauses replacing the void, invalid or unenforceable clause to reflect the original intent of the Parties to the fullest extent possible.
- 17.3 The Parties acknowledge that all the clauses of this Letter of Appointment have been fully negotiated between them, therefore, the provisions of Articles 1341 ff. of the Italian Civil Code shall not apply.