

GDPR Data Processing Agreement/Addendum (“DPA”)

Data Protection Addendum

This Data Protection Addendum (this “Addendum”) is made and entered into as of the date appearing on the signature page hereto (the “Effective Date”) by and between MICT - Media in Cooperation & Transition gGmbH (“Company”) and the Supplier named on the signature page hereto, and upon execution shall be incorporated by reference into each agreement for services (“Services Agreement”) pursuant to which Supplier may Process (as defined below) Personal Data (as defined below) for, from, or on behalf of Company.

A. Personal Data Protection

For the purposes of this Addendum, the terms “Controller”, “Data Subjects”, “Personal Data”, “Personal Data Breach”, “Processor” and “Process” shall have the meaning as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (“GDPR”) or any successor European Union data protection framework.

The parties agree that to the extent Supplier, in the context of performing the agreed services, processes any Personal Data of Company, Supplier shall be the Processor and Company shall be the Controller of such Personal Data. Notwithstanding any obligations of Company as Controller under applicable data protection law, Supplier undertakes the following as Processor:

- (a) to process any Personal Data only on behalf and in accordance with Company’s documented instructions and not for any purposes other than those described in this Addendum, unless (i) Company has given its express prior consent or (ii) Supplier is strictly required to do so under applicable European Data Protection Law (as defined below); in such a case, Supplier shall inform Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are further specified in Exhibit 1 to this Addendum.
- (b) to comply with (i) the GDPR and any applicable European data protection laws and regulations (collectively “European Data Protection Law”), and (ii), in case Supplier is certified under the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, or any successor program recognized under European Data Protection Law to provide for an adequate level of data protection, the principles of such applicable Privacy Shield Framework or successor program, and (iii) all other applicable data protection and privacy laws and regulations ((i) to (iii) collectively “Data Protection Laws”).
- (c) to implement appropriate technical and organizational measures in such a manner that the Processing, including by any Sub-Processors (as defined below), will meet the requirements under Data Protection Laws and ensure

the protection of the rights of the Data Subjects, and to regularly test, assess and evaluate the effectiveness of and, as necessary, improve and update these measures. The measures shall ensure a level of data security appropriate to the risks for the rights and freedoms of the Data Subjects. In particular, Supplier shall protect the personal data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

- (d) to keep Personal Data strictly confidential and to ensure, and be able to demonstrate on request, that (i) only those persons have access to the Personal Data who are authorized by Supplier and have a strict need to know the data for the purposes under this Addendum, and (ii) all persons with access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (e) to disclose Personal Data to third parties, including affiliated companies, and/or to engage another Processor for the Processing of Personal Data (“Sub-Processor”) only with Company’s express prior consent. Where Supplier is authorized to engage another Sub-Processor for carrying out Processing activities on behalf of Company, Supplier shall enter into a written contract with the Sub-Processor which (i) imposes on the Sub-Processor the same data protection obligations as set forth in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements under Data Protection Laws, and (ii) grants Company the right to directly audit the Sub-Processor as set forth under Section A(j). Supplier shall promptly send a copy of any sub-processor agreement it concludes under this Section A(e) to Company. Supplier shall select the Sub-Processor diligently, taking into account the technical and organizational measures it has implemented, and ensure, by carrying out audits before and regularly after the commencement of the data processing by such Sub-Processor, that it maintains appropriate technical and organizational measures to safeguard an adequate level of data protection within the meaning of European Data Protection Law. Supplier shall remain fully liable to Company for the performance of this Agreement and be responsible and liable for any act or omission of the Sub-Processor with respect to its data protection obligations.
- (f) to assist Company, including by appropriate technical and organizational measures, insofar as this is possible and taking into the nature of the processing, in fulfilling its obligations in relation to requests from Data Subjects for exercising their Data Subject’s rights under Data Protection Laws, including, but not limited to, the Data Subject’s right of access, right to rectification and erasure, right to restriction of processing, right to data portability and right to object, as provided for under the GDPR.
- (g) to assist Company, taking into account the nature of the processing and information available to Supplier, in ensuring compliance with the obliga-

tions under applicable Data Protection Laws, including, in particular, by providing all information and assistance to enable Company (i) to comply with applicable data security obligations, (ii) to carry out a data protection impact assessment or prior consultation with the supervisory authority, as required under European Data Protection Law, and (iii) to respond promptly and properly to any enquiries concerning the Processing of Personal Data and cooperate in good faith with the supervisory authorities, the Data Subjects or any third party within a reasonable time. Supplier shall not communicate with any supervisory authority, Data Subject or any third party in connection with the Processing of Company's Personal Data without prior approval from Company, except as expressly permitted in this Section A.

- (h) to notify Company, without undue delay, in writing or via e-mail (i) of any intended change of the locations currently set out in Exhibit 1 to this Addendum for the Processing of Personal Data, (ii) in case of a dispute, claim or request brought by a Data Subject directly against Supplier, (iii) in the event of any measure, request or other communication by a supervisory authority, including about any legally binding request for access or disclosure of Personal Data by a public authority (unless otherwise legally prohibited, in which case the Supplier will use its best efforts to obtain the right to waive this prohibition), and provide reasonable assistance if Company wishes to contest the request, and (iv) of any suspected or actual Personal Data Breach, any breach of applicable Data Protection Laws or of this Addendum. Supplier shall promptly remedy any breach and cooperate with Company in the investigation and remedy of such breaches and provide all reasonable assistance and information to enable Company to comply with, or, as applicable, to avoid, any data breach notification obligations vis-à-vis supervisory authorities and/or Data Subjects. Supplier shall further immediately inform Company if, in its opinion, an instruction infringes Data Protection Laws and/or Supplier becomes aware of the existence of any local laws that would have a substantial adverse effect on the guarantees and undertakings provided for under this Addendum.
- (i) at the choice of Company, to return to Company (in a standard format facilitating portability) and/or to securely delete/destroy all Personal Data, including all existing copies thereof, in accordance with Company's instructions, within thirty (30) days upon Company's request or after the end of the provision of the services relating to Processing, and to certify to Company in writing that it has done so. Supplier shall not be obliged to delete/destroy all copies of the Personal Data where a longer storage by Supplier is required under European Data Protection Law, in which case Supplier shall inform Company accordingly, including about the legal grounds for, and the term of, any further storage;
- (j) to make available to Company all information necessary to demonstrate compliance with the obligations under Data Protection Laws applicable

to Company and to allow for and contribute to audits, including on-site inspections, conducted by Company or another auditor mandated by Company. (k) to enter into any further agreements that may be required under Data Protection Laws relating to Personal Data, and to provide all other assistance and support to Company.

B. Changes to this Addendum

The parties agree that, to the extent required under applicable Data Protection Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from the competent supervisory authorities or the European Commission, including, without limitation, the adoption of standards for contracts with processors according to Art. 28(7) or (8) GDPR or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission in relation to international data transfers on the basis of Art. 45(3) or Art. 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the EU Standard Contractual Clauses or similar transfer mechanisms, Company may request reasonable changes or additions to this Addendum to reflect applicable requirements.

C. Third party beneficiary clause

The parties agree that affiliates of the Company shall be entitled under and can enforce the terms of this Addendum against Supplier as third-party beneficiaries.

D. Termination

In the event of Supplier's violation of any obligation under Data Protection Laws or this Addendum, Company, without prejudice to any other rights which it may have, shall be entitled to terminate any Services Agreement forthwith. Any terms of this Addendum that by their nature extend beyond the termination of the Services Agreement, including without limitation this Addendum, Section A(i), shall remain in effect.

E. Precedence

In the event of a conflict between this Addendum and other provisions of the Services Agreement, this Addendum shall prevail.

[Signature page follows.]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed as of _____, _____, 20____ by their respective officers thereunto duly authorized.

COMPANY:

MICT - Media in Cooperation & Transition gGmbH

By:
Name:
Title:

SUPPLIER:

By:
Name:
Title:

Exhibit 1 to Data Protection Addendum

Description of Processing

A. Subject-matter, nature and purpose of the Processing

Supplier provides certain services to Company, including *[insert general description of services relating to processing of personal data]*, as further specified in the Services Agreement. In the context of performing the obligations under the Services Agreement, Supplier may Process certain of Company's Personal Data as necessary for the purposes of *[insert purposes of Processing]*, as further specified in the Services Agreement. Such processing may include: *[insert description of relevant data processing activities/operations]*.

B. Duration of the Processing

[insert duration of data processing, e.g.: "The agreed Processing of Personal Data shall commence upon the effective date of the Services Agreement and be carried out for the term of the Services Agreement. The services relating to Processing of Personal Data shall automatically end in case the Services Agreement is effectively terminated or expires, in which case the Personal Data shall be handled in accordance with Section A(i). To the extent the Processing of Personal Data by Supplier is necessary for the winding-up of the Services Agreement, e.g. with respect to returning the Personal Data, the provisions of Section A shall continue to apply until the completion of the winding-up."]

C. Categories of Data Subjects

The Processing will concern the following categories of Data Subjects: *[insert categories of data subjects concerned, e.g.: a. Company employees and job candidates b. Managers, employees, agents or other contact persons at business partners c. Company customers that are natural persons d. Patients, research subjects or other customers of Company's clients]*

D. Types of Personal Data

The Processing will concern the following types of Personal Data *[insert types of Personal Data concerned, e.g.:]*

- **a) Company employees and job candidates:**
name, contact details (address, phone number and direct line, e-mail address), birth date/ country, gender, education (e.g., highest education level, country, degree, certificates), job information about current and previous employment (position, kind of work, work location, salary, replacement, company, location, department, position, function, grade, supervisor, employee class, grade and labor start/ entry date, labor agreement, business title, full or part-time, shifts, working hours), professional skills, CV and resume, training, compensation and remuneration (e.g., compensation rate, salary, target bonus, incentives, benefits), individual development plan, performance goals and assessment, position in company, bank account number and corporate credit card number, national ID and social security number, information about an immigration background.
- **b) Managers, employees, agents or other contact persons at business partners:**
contact details (name, address, phone number and direct line, e-mail address).
- **c) Company customers that are natural persons:**
name, contact details (address, phone number and direct line, e-mail address), information regarding purchases of such customers, bank account details, credit information, information about such customers' interest in Company products.
- **d) Patients, research subjects or other customers of Company's clients:**
[insert the type of data in this category that your service providers might handle]

The Processing will concern the following special categories of data¹:

[...]

The Processing will include Personal Data relating criminal convictions and offenses relating to:

[...]

¹ "Special categories of data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.