Materialise Confidential and Proprietary

Version Date: 7 December 2022

EU GENERAL DATA PROTECTION REGULATION (GDPR) DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**Agreement**") between the Materialise entity indicated on the Order Form, on behalf of itself and its affiliates ("**Materialise"**) acting as **"Data Processor"**, and the Customer indicated on the applicable Order Form, hereafter the **"Data Controller"**.

Materialise and Customer are collectively referred to as the "**Parties**" and individually as a "**Party**" in this Agreement.

RECITALS

(A) The Data Controller and the Data Processor have concluded a Software-as-a-Service Agreement as indicated on the applicable Materialise Order Form entered into between Materialise and the Customer (**"Order Form"**) by which the Data Processor has undertaken the provision of specific services involving the processing of Personal Data, on behalf of the Data Controller (hereinafter, the '**Service Agreement**').

(B) Both Parties have agreed to comply with their obligations with respect to the processing of the Personal Data, as described in the present Data Processing Agreement (hereinafter, the '**Processing Agreement**') which is subject to **EU and National Data Protection law**, including but not limited to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the '**General Data Protection Regulation**' or the '**GDPR**'), and acknowledge that the Processing Agreement and the content of the Service Agreement shall constitute the complete written instructions of the Data Controller.

(C) Any terms not otherwise defined in this Processing Agreement shall have the meaning given to them in the Service Agreement. Except as modified below, the terms of the Service Agreement shall remain in full force and effect. Other terms used in this Processing Agreement that have meanings ascribed to them in the EU Data Protection law, including but not limited to 'processing', 'Personal Data', 'Data Controller' and 'Processor', shall carry the meanings set forth under EU Data Protection law.

(D) Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection law on behalf of the Data Controller in the course of the performance of the Service Agreement with the Data Controller, the terms of the present Processing Agreement shall apply. In the event of a conflict between any provisions of the Service Agreement and the provisions of this Processing Agreement, the provisions of the Processing Agreement shall govern and control. An overview of the categories of Personal Data, the categories of Data Subjects, and the nature and purposes for which the Personal Data are being processed is provided in Annex 2**: Types of Personal Data, Categories of Data Subjects, Nature and Purposes of the Data processing**.

AGREEMENT

1. Subject matter of this Data Processing Agreement

1.1 This Processing Agreement applies to the processing of Personal data subject to EU Data Protection law in the scope of the Service Agreement between the Parties. It contains the written instructions of the Data Controller towards the Data Processor with regards to the processing of Personal Data for those services for which Materialise qualifies as a Data Processor.

2. Obligations applicable to the Data Controller

2.1 Information to the Data Subjects. The Data Controller is responsible for ensuring that all necessary privacy notices required under Articles 13 and/or 14 of the GDPR have been provided at the time of the data collection to the Data Subjects of whom the Personal Data is processed according to the Processing Agreement.

2.2 Lawfulness. The Data Controller expressly acknowledges and warrants that it has all necessary rights to provide the Personal Data to the Data Processor, and that one or more lawful bases set forth in EU Data Protection law support the lawfulness of the processing in relation to the Services.

Unless another legal basis set forth in EU Data Protection law supports the lawfulness of the processing, the Data Controller shall undertake that any required Data Subjects' consent to the processing is obtained and ensure that a record of such consents is maintained. Should such a consent be revoked by a data subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and the Data Processor remains responsible for implementing the Data Controller's instruction with respect to the processing of that Personal Data.

2.3 Sensitive Data. The Data Controller undertakes not to submit, store, or send any sensitive data or special categories of Personal Data (collectively, **"Sensitive Data"**) to the Data Processor without documented explicit consent thereto by the data subject, or only insofar as the processing of such data complies with one of the lawful grounds under Article 9, §2, of the GDPR. The Data Controller expressly agrees to disclose this documentation to the Data Processor upon request.

2.4 Purposes and means. When providing the Personal Data to the Data Processor, the Data Controller shall determine the scope, purposes, and means by which the Personal Data may be accessed or processed by the Data Processor under the Processing Agreement.

2.5 Processing by the Data Controller. Insofar that employees of the Data Controller are required to process the Personal Data themselves, the responsibility and obligation to comply with the Applicable Legislation will remain incumbent on the Data Controller instead of the Data Processor.

3. Obligations applicable to the Data Processor

3.1 Documented instructions. The Data Processor undertakes to the Data Controller that it shall process the Personal Data only on behalf of and according to the documented instructions of the Data Controller (which include the terms of this Processing Agreement and the Service Agreement), including regarding transfers of Personal Data to a third country. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller's documented instructions.

3.2 Legally required international transfers. In case the Data Processor is required to transfer the Personal Data outside the EEA by European Union or EU Member State law to which it is subject, the Data Processor shall inform the Data Controller of that legal obligation and seek

explicit authorization from the Data Controller before undertaking such processing, unless that law prohibits such information on important grounds of public interest.

3.3 Confidentiality. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall undertake to implement necessary and adequate measures to restrict the access to the Personal Data based on a strict need-to-know basis. Moreover, the Data Processor shall treat all Personal Data as confidential and it shall inform all its employees, agents and/or approved Subprocessors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

3.4 Audit rights. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to Article 4.1 and shall allow the Data Controller to audit and test such measures to ascertain the Data Processor's compliance with the Processing Agreement. The Data Controller shall be entitled on giving at least 21 days' notice to the Data Processor to carry out, or have carried out by a trusted third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor's premises and operations relating to the Personal Data processed under the present Processing Agreement.

The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller by granting the Data Controller's auditors reasonable access to any premises and devices involved with the processing of the Personal Data, and disclosing to the Data Controller and/or the Data Controller's auditors any information relating to the processing of the Personal Data as may be reasonably required by the Data Controller.
In addition, The Data Controller may request that the Data Processor audit a Subprocessor (if any) or provide confirmation that such an audit has to ensure compliance with its obligations imposed by the Data Processor in conformity with this Processing Agreement.

3.5 Data transfers. The Data Processor shall promptly notify the Data Controller of any planned permanent or temporary transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection, and shall only perform such a transfer after obtaining authorization from the Data Controller and where the transfer is based on an adequate data transfer mechanism. Annex 4: **Authorized Subprocessors and International data transfers**provides a list of transfers for which the Data Controller grants its authorization upon the conclusion of this Processing Agreement.

In addition, the Data Processor shall implement adequate organizational and security measures to protect the Personal Data, taking into account the duration of the data transfer, the country of origin and country of destination, as well as the general and sectoral regulations in place.
To the extent that the Data Controller or the Data Processor are relying on a specific mechanism to justify international data transfers and that mechanism is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

3.6 Data subjects requests. With regard to the protection of Data Subjects' rights pursuant to the EU Data Protection law, the Data Processor shall facilitate by appropriate technical and organizational measures, insofar as this is possible, the fulfilment of Data Subjects requests for exercising their rights of access, rectification, erasure, restriction of processing, data portability and objection to automated decision-making by the Data Controller.

Should the Data Processor be contacted directly by a Data Subject as regards the exercise of one of its rights, the Data Processor will promptly direct the requesting Data Subject to the Data Controller, which shall remain responsible for the proper handling of the request. The Data

Controller acknowledges that a request to erasure by a Data Subject does not imply an obligation on behalf of the Data Processor to remove the Personal Data from all its back-ups if such removal would be deemed impossible or require a disproportionate effort.

3.7 Assistance to the Data Controller. Taking into account the nature of the processing and the information available to him, the Data Processor shall assist the Data Controller in ensuring compliance with obligations pursuant to Articles 32 to 36 of the GDPR, including notifications to the Supervisory Authority and the Data Subjects in case of Data Incident, the process of undertaking a Data Protection Impact Assessment, and the prior consultation with Supervisory Authorities. Both Parties shall agree on the Data Processor's right to invoice such assistance at a reasonable rate.

3.8 Back-up of Personal Data. Insofar as it is necessary for the provision of the services under the present Processing Agreement, the Data Controller allows the Data Processor to perform incremental back-ups of the Personal Data being processed, which shall benefit from the same level of confidentiality and protection as the original Personal Data.

3.9 Data Protection Officer. Insofar it is required to appoint a Data Protection Officer under the EU or National Data Protection law, the Data Processor communicates the contact details of its Data Protection Officer to the Data Controller by using the contact form in Annex 1**: Contact information of the Data Protection Officers**.

3.10 Training. The Data Processor undertakes to inform and train its employees and/or agents regarding the latest developments of the applicable Data Protection law at both EU and national level. The Data Processor shall maintain the necessary documentation to demonstrate its compliance with this provision and disclose said documentation at the request of the Data Controller.

3.11 Unlawful instructions. The Data Processor shall immediately notify the Data Controller if, in its opinion, any instruction infringes this Regulation or other Union or Member State Data Protection provisions. Such notification will not constitute a general obligation on the part of the Data Processor to monitor or interpret the laws applicable to the Data Controller, and such notification will not constitute legal advice to the Data Controller.

4. Common obligations

4.1 Technical and organizational security measures. 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, the Data Controller and Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include, at a minimum, the security measures agreed upon by the Parties in Annex 3**: Security Measures**.

4.2 Written security policies. Both the Data Controller and the Data Processor shall maintain written security policies that are fully implemented and applicable to the processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the Personal Data, conducting appropriate background checks, requiring employees, Vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the processing.

4.3 Improvements to security. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4.1 on an ongoing basis in order to maintain compliance with the requirements set out in Article 4.1.

The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in EU Data Protection law or by Data Protection authorities of competent jurisdiction.
Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in EU Data Protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

4.4 Data Incident. If the Data Processor becomes aware of or reasonably suspects a Data Incident, it will notify the Data Controller without undue delay and no later than [24] hours after discovering the Incident and will take reasonable steps to minimize harm and secure the Personal Data.

Notifications will be sent to the employee of the Data Controller whose contact details are provided in Annex 1 and will describe, to the extent possible, the nature of the incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal data records concerned; the likely consequences of the incident; the measures taken or proposed to be taken by the Data Processor to address the Data Incident, including measures to mitigate its possible adverse effects.
The Data Processor will not assess the contents of any Customer Data in order to identify information that may be subject to specific legal requirements.

4.5 Notification of the Data Incident. The notification of or response to a Data Incident by the Data Processor under Article 4.4 will not constitute the Data Processor's acknowledgement of fault or liability with respect to the Data Incident. The Data Controller expressly acknowledges that it remains solely responsible for complying with any incident notification laws that may apply to it, and to fulfilling any third-party notification obligations related to any Data Incident(s).

4.6 Register of processing activities. Both the Data Controller and the Data Processor shall maintain a Register of the processing activities falling under their responsibility, in compliance with Articles 30(1) and 30(2) of the GDPR, respectively.

5. Contracting with Subprocessors

5.1 Prior Specific Authorization by the Data Controller. The Data Processor shall not subcontract any of its data processing activities related to the provision of the services described in Annex 2**: Types of Personal Data, Categories of Data Subjects, Nature and Purposes of the Data processing** to other Subprocessors (hereinafter referred to as: '**Third party Subprocessors**') than those specifically listed in Annex 4**: Authorized Subprocessors and International data transfers**, without the Data Controller's prior written authorization.

Without prejudice to the above, the Data Processor shall inform the Data Controller in writing of any addition or replacement of the Subprocessors listed in Annex 4**: Authorized Subprocessors and International data transfers**, in a timely manner, giving the Data Controller an opportunity to object in writing to such changes within [10] business days after being notified by the Data Processor.
The Data Controller expressly agrees that any objection shall always be motivated with documentary legal or material evidence that reasonably shows that said Subprocessor does not or cannot comply with the requirements set forth in this Processing Agreement. If both parties

do not remedy or provide a good-faith workaround for the objection within a reasonable time, the Data Controller may, as its sole remedy and its sole liability for the objection, terminate the Agreement without further liability to either party. In such case, the Data Processor will not owe the Data Controller a refund of any fees paid in the event the Data Controller decides to terminate the Agreement pursuant to the present Article.

5.2 Subprocessors outside the EEA. Without prejudice to Article 3.5, the Data Processor shall not rely on the services of a Subprocessor located outside the EEA without the Data Controller's prior written authorization. In addition, the Data Processor shall only subcontract trusted Subprocessors who have demonstrated adequate organizational and security measures. In the absence of such measures, the Data Processor shall not engage the Subprocessor without implementing sufficient contractual assurances or obtaining the explicit consent of the Data Subjects concerned.

5.3 Liability of the Data Processor for the Subprocessing. The Data Processor remains the sole contact point for the Data Controller during the entire duration of the subprocessing and ensures that each Subprocessor shall be bound by Data Protection obligations compatible with those of the Data Processor under this Processing Agreement. Moreover, the Data Processor shall monitor compliance of the subprocessing and impose on its Subprocessors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU Data Protection Law.

Notwithstanding any authorization by the Data Controller within the meaning of the preceding Articles, the Data Processor shall remain fully liable towards the Data Controller for the performance of any such Subprocessor that fails to fulfill its Data Protection obligations.

6. Duration and Termination of the Data Processing Agreement

6.1 Duration. The present Processing Agreement comes into effect on the Effective Date as indicated on the applicable Order Form. The Data Processor shall process the Personal Data until the date of expiration or termination of the Service Agreement, unless instructed otherwise by the Data Controller, or until such Data is returned or destroyed on instruction of the Data Controller according to the Article 6.2.

6.2 Return or Deletion of Personal Data. Upon termination of this Processing Agreement, upon the Data Controller's written request, upon fulfilment of all purposes agreed in the context of the Service Agreement whereby no further processing is required, or upon fulfilment of any and all legal and/or regulatory obligations the Data Processor shall, at the sole discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies. Insofar as returning the Personal Data proves impossible, the Data Controller may request evidence or a certificate for the destruction of all copies of the Personal Data.

The Data Processor shall notify all Subprocessors supporting its own processing of the Personal Data of the termination of the Processing Agreement and ensure that all such Subprocessors shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

7. General Provisions

7.1 Liability of the Parties. The liability of each Party towards the other shall be governed by the relevant provisions of the Service Agreement. The Data Controller expressly recognizes that the Data Processor shall only be held responsible for the processing of the Personal Data under the present Processing Agreement and according to the instructions of the Data Controller. The Data Processor shall not be held liable for all other processing activities, including but not limited to

the initial collection of the Personal Data by the Data Controller, processing for purposes not further disclosed to the Data Processor, or processing by another Processor or by a Third party Subprocessor.

7.2 Variations to the Agreement. No variations may be made to this Processing Agreement other than with the written agreement of both Parties. Whenever the Data Controller intends to request a new processing service from the Data Processor or insofar as the purpose of the initial processing service needs to be modified, the Parties agree to conclude an additional Processing Agreement, either replacing or to be attached as an Addendum to the current Processing Agreement.

7.3 Variations to the Applicable Data Protection law. In the event of any changes to the Data Protection law applicable in the jurisdiction of the Data Controller or the Data Processor, which require changes to the obligations set out in this Processing Agreement in order for the Data Controller or Data Processor to maintain compliance with the applicable Data Protection law, the Parties shall use reasonable endeavours to agree such changes. Until such changes have been agreed in writing by the Parties, this Processing Agreement shall be deemed to be amended to the extent necessary to give effect to such changes.

Annex 1: Contact information of the Data Protection Officers

Contact information of the Data Protection Officer / Compliance Officer of the Data Controller.

[Please Complete with Contact information]

Contact information of the Data Protection Officer of the Data Processor.

Mrs. Miet JANSSEN
Miet.Janssen@materialise.be
+3216660473
Technologielaan 15 – 3001 Leuven BE

Annex 2: Types of Personal Data, Categories of Data Subjects, Nature and Purposes of the Data processing

Types of Personal Data that will be processed in the scope of the Service Agreement.

Personal Data

Categories of Data Subjects.

Data Subject (Category)

Nature and Purpose of the Data processing.

Nature	*Purpose*

Annex 3: Security Measures

The Data Processor shall:

- ☐ ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2**: Types of Personal Data, Categories of Data Subjects, Nature and Purposes of the Data processing** of this Data Processing Agreement;
- ☐ take all reasonable measures to prevent unauthorized access to the Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;
- ☐ build in system and audit trails;
- ☐ use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;
- ☐ account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;
- ☐ ensure pseudonymisation and/or encryption of Personal Data, where appropriate;
- ☐ maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ☐ maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- ☐ implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;
- ☐ monitor compliance on an ongoing basis;
- ☐ implement measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;
- ☐ provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

Annex 4: Authorized Subprocessors and International data transfers

Subprocessors within the European Economic Area for which the Data Controller has granted its authorization:

Subprocessor Name	EEA Country
Subprocessor Name	EEA Country

Transfers to Subprocessors in third countries outside of the European Economic Area without an adequate level of protection, for which the Data Controller has granted its authorization:

Subprocessor Name	Non-EEA Country	Transfer Mechanism
Subprocessor Name	Non-EEA Country	Transfer Mechanism

Annex 5 – Definitions

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.
EEA	The 'European Economic Area', which comprises the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others**, determines the purposes and means of the processing of Personal Data**; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Processing	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.
Subprocessors	Third parties authorized under these Terms to have logical access to and process Personal Data provided by the Data Controller in order to provide parts of the Services.
Sensitive data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as 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.
Anonymous data	Aggregated data or data that can no longer be attributed to a specific data subject.
Pseudonymous data	Personal data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
Service Agreement	The agreement concluded between MATERIALISE and the Data Controller regarding the Subscription Services, Documentation and Software as indicated and defined on the Order Form.
Data Incident	A breach of the Data Processor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data from the Data Controller on systems managed by or otherwise controlled by the Data Processor. 'Data Incidents' will not include unsuccessful attempts or activities that do not compromise the security of the Data Controller's data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.