Appendix B to General Terms and Conditions regarding BIMobject® Cloud:

Data Protection Agreement

This Data Protection Agreement (the "**Agreement**") is agreed to by:

(1) The BIMobject customer identified on the applicable Customer Contract (defined below) for BIMobject services ("**Customer**"); and

(2) BIMobject AB (556856-7696), a Swedish company having its principal place of business at Nordenskiöldsgatan 24, 211 19 Malmö, Sweden ("**BIMobject**")

Individually a "**Party**" and collectively the "**Parties**".

Whereas:

(A) Customer and BIMobject or, BIMobject's subsidiary company, as the case may be, ("**BIMobject Entity**"), have entered into a contract and/or any other ordering document (previously) executed by Customer ("**Customer Contract**") for the provision of certain Services (defined below) by BIMobject, including access to certain features on the BIMobject Cloud Platform.

(B) BIMobject owns and operates the BIMobject Cloud Platform.

(C) Customer's access and use of the Services and BIMobject's provision of the Services result in certain User Personal Data on the BIMobject Cloud Platform being processed by the Customer and BIMobject (and/or its affiliate as the case may be).

(D) This Agreement governs the rights and responsibilities of the Parties in relation to their respective processing of User Personal Data accessed on the BIMobject Cloud Platform.

(E) This Agreement is incorporated into the Customer Contract by reference.

1. Definitions

All capitalized terms used herein, but not otherwise defined, shall have the same meaning afforded to it within the General Terms and Conditions.

1.1 In this Agreement except to the extent expressly provided otherwise:

"**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question and or being processed, including, where applicable, EU Data Protection Law.

"**BIMobject Cloud Platform**" means the software and all functionalities, interfaces, features, solutions, websites, products and services made available by BIMobject and BIMobject Affiliates to customers, Users, visitors and others from time to time from time to time, including but not limited to the Services;

"**Effective Date**" means the date when the Order Form comes into effect either by an order online being completed or an order form, business agreement or similar is duly executed by both Parties, as applicable;

"**EU Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any and all applicable national data protection laws made under or pursuant to (i) or (ii); in each case as may be amended or superseded from time to time;

"**Model Clauses**" means the standard contractual clauses for the transfer of Personal Data to Controllers established in third countries in the form set forth below in Appendix B1 to this Agreement, and as found at Standard Contractual Clauses (MODULE ONE: Transfer controller to controller) in the Annex to the European Commission Decision of April 2, 2021, and as may be amended or replaced by the European Commission from time to time;

"**Permitted Purposes**" has the meaning given in Clause 3.1;

"**Schedule**" means any schedule attached to this Agreement;

"**Security Incident**" means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**Services**" means the services provided to Customer under this Agreement, which may include the Customer's use of BIMobject Cloud, Subscribed Services, and/or any Model Development and/or hosting services provided by BIMobject to Customer through the BIMobject Cloud, and any ancillary products and services provided whether purchased via renewable subscription or as a one-time purchase;

"**User(s)**" means any individual(s) who has/have registered an account on the BIMobject Cloud Platform; and

"**User Personal Data**" means personal data of Users and is more particularly described in Schedule 1 to this Agreement. User Personal Data is included in the general term "personal data".

1.2 In this Agreement:

(a) the expressions "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") "**personal data breach**", "**special categories of personal data**" and "**supervisory authority**" shall have the meanings given in EU Data Protection Law; and

(b) any other terms used but not defined in this Agreement shall have the meaning given to them in the Customer Contract.

2. Term and Termination

2.1 This Agreement shall commence on the Effective Date and shall terminate automatically upon expiry or termination of the Customer Contract.

2.2 Termination of this Agreement shall not affect each Party's responsibility to process personal data it has already accessed or in accordance with Applicable Data Protection Law.

3. Parties' roles and compliance with data protection law

3.1 In the course of providing or receiving the Services, each Party may process User Personal Data for the purposes that are described in Schedule 1 ("**Permitted Purposes**").

3.2 The Parties acknowledge that they shall be independent controllers of the User Personal Data that they each process. In no event shall the Parties process the User Personal Data as joint controllers.

3.3 Each Party shall be individually and separately responsible for complying with the obligations that apply to it as a controller under Applicable Data Protection Law when processing User Personal Data. In particular (and without limitation):

(a) BIMobject shall be responsible for complying with Applicable Data Protection Law requirements (including transparency and lawfulness requirements) in respect of individual data subjects who register with, and use, the BIMobject Cloud Platform including by displaying a publicly-accessible privacy notice on its website at https://accounts.bimobject.com/privacypolicy and https://accounts.bimobject.com/privacynoticeforcaliforniaresidents (and such privacy notice shall notify data subjects that their User Personal Data may be disclosed to BIMobject customers whose "BIM objects" they access or download);

(b) Customer shall be separately and independently responsible for complying with Applicable Data Protection Law in respect of any processing of User Personal Data it obtains through the BIMobject Cloud Platform in particular (and without limitation) if and when processing User Personal Data to contact data subjects for direct marketing purposes;

(c) Data subjects may exercise their data protection rights under Applicable Data Protection Law against the Customer in respect of Customer's processing of the User Personal Data, and against BIMobject in respect of BIMobject's processing of the User Personal Data.

3.4 No Party shall process User Personal Data for any purpose other than the Permitted Purposes except where and to the extent permitted to do so by Applicable Data Protection Law.

4. International transfers

4.1 None of the Parties shall process any User Personal Data (nor permit same to be processed) in a territory outside of the European Economic Area ("**EEA**") unless such Party has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

4.2 Where User Personal Data originating in the EEA is processed by Customer outside the EEA in a territory that has not been designated by the European Commission as ensuring an adequate level of protection pursuant to EU Privacy Law the Model Clauses will be incorporated into this Agreement by this reference and will apply to the Processing as follows:

(a) BIMobject shall be deemed to have entered into the Model Clauses in its own name and on its own behalf in relation to such User Personal Data that it discloses to Customer; and

(b) Customer shall be deemed to have entered into the Model Clauses in its own name and behalf in relation to the User Personal Data that is disclosed to it; and

(c) where and to the extent that the Model Clauses apply pursuant to this Clause 4, if there is any conflict between this Agreement and the Model Clauses, the Model Clauses will prevail.

5. Cooperation

5.1 If Customer receives a communication from a User, supervisory authority or other third party relating to its processing of User Personal Data pursuant to this Agreement it shall promptly, to the extent permitted by applicable law, send a copy of the communication to BIMobject.

5.2 Each Party shall provide reasonable cooperation and assistance in good faith in relation to such a communication in accordance with Applicable Data Protection Law where requested by the other Party.

6. Security

6.1 Each Party shall implement and maintain appropriate technical and organisational security measures to protect the User Personal Data it processes against a Security Incident.

7. Sub-processing

7.1 If any Party appoints third party processors to process User Personal Data for their Permitted Purpose, they shall ensure that such processors:

(a) agree in writing to process User Personal Data in accordance with that Party's documented instructions;

(b) implement appropriate technical and organisational security measures to protect the User Personal Data against a Security Incident; and

(c) otherwise provide sufficient guarantees that they will process the User Personal Data in a manner that will meet the requirements of Applicable Data Protection Law.

8. Changes to Applicable Data Protection Law

8.1 The Parties shall use their best endeavours to agree variations to this Agreement as may be necessary to reflect changes in Applicable Data Protection Laws.

9. General

9.1 No breach of any provision of this Agreement shall be waived except with the express written consent of the Party not in breach.

9.2 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the Parties, in which case the entirety of the relevant provision will be deemed to be deleted).

9.3 This Agreement may not be varied except by a written document signed by or on behalf of each of the Parties.

9.4 No Party may without the prior written consent of the other Parties assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement save that such consent

shall not be required by BIMobject as a result of corporate restructuring in the BIMobject corporate group or assignment to a BIMobject affiliate.

9.5 This Agreement is made for the benefit of the Parties and is not intended to benefit any third party or be enforceable by any third party. The rights of the Parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.

9.6 This Agreement and the Customer Contract shall constitute the entire agreement between the Parties in relation to the subject matter herein, and shall supersede all previous agreements, arrangements and understandings between the Parties in respect of that subject matter.

9.7 In terms of the subject matter of this Agreement (data protection considerations regarding User Personal Data) this Agreement shall prevail in the event of a conflict with the Customer Contract.

9.8 BIMobject reserves the absolute right to delegate to, or to appoint any of its subsidiary corporate entities to engage in the processing of User personal Data on the BIMobject Cloud. In the event that any such BIMobject entity should additionally act as controller of, or engage in the processing of any User Personal Data on The BIMobject Cloud, either alone or together with BIMobject, then, the obligations as set out in this Agreement in respect of the processing of User Personal Data shall where appropriate, apply to such BIMobject entity unless otherwise undertaken by BIMobject.

9.9 This Agreement shall be governed by and construed in accordance with Swedish Law. The courts of Sweden shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement.

SCHEDULE 1 to the Data Protection Agreement:

Data Processing Activities

Categories of personal data

User Personal Data may include:

- Name
- Email address
- Postal code, city and state
- Country name
- Occupation
- Company name
- Employer's details
- Phone number (if provided)
- Picture (if provided)
- Usage and downloads history

Special categories of personal data

- None

Categories of data subjects

- Individual data subjects (Users) who register an account with, and use, the BIMobject Cloud Platform

Purposes of processing ("Permitted purpose")

Processing by Customer:

Customer shall process certain User Personal Data for the purposes of:

(i) receiving the Services in accordance with the Customer Contract (as amended from time to time in accordance with its terms); and

(ii) to connect and communicate with Users on the BIMobject Cloud;

(iii) to market and promote its products to Users;

(iv) as otherwise set out in this Agreement.

Customer shall process the User Personal Data only for as long as is necessary for these purposes.

Processing by BIMobject:

BIMobject shall process User Personal Data for the purposes of:

(i) operating the BIMobject Cloud platform and carrying out processing activities in respect of User Personal Data which are set out in detail in the BIMobject Privacy Policy available at https://accounts.bimobject.com/privacypolicy (as amended from time to time) and the Privacy Notice for California Residents at https://accounts.bimobject.com/privacynoticeforcaliforniaresidents;

(ii) sharing User data with Customers as set out in the BIMobject Privacy Policy;

(iii) providing the Services in accordance with the Customer Contract; and

(iv) as otherwise as set out in this Agreement or as per the BIMobject User Terms of Service

BIMobject shall process the User Personal Data only for as long as is necessary for these purposes.

APPENDIX B1 to the Data Protection Agreement:

CONTROLLER-TO-CONTROLLER SCCS (DATA TRANSFER AGREEMENT)

Commission Decision C(2021) 3972 final

MODULE ONE: Transfer controller to controller

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) [Not used}

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e); and

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 **[Not used]**

[Intentionally left blank]

Clause 10
Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted

by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[6];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue

possibilities

of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal

framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Sweden.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO APPENDIX B1 to the Data Protection Agreement:

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I TO APPENDIX B1 to the Data Protection Agreement:

A. LIST OF PARTIES

Data exporter:

Name: BIMobject AB

Address: Nordenskiöldsgatan 24, SE 211 19 Malmö, Sweden Contact

person's name, position and contact details:

Martin Lindh, CEO
Email: legal@bimobject.com
Tel: +46 40 685 29 00

Activities relevant to the data transferred under these Clauses: See Section B Description of

Transfer

Signature: Martin Lindh Dated: 13 December 2022

Role (controller/processor): Controller

Data importer:

Name: Company name as indicated in Customer Contract

Address: Company address as indicated in Customer Contract

Contact person's name, position and contact details: As identified in the Customer Contract, unless Customer notifies BIMobject of a different contact for the purposes of the Appendix B1.

Activities relevant to the data transferred under these Clauses: See Section B Description of Transfer

Signature: As Agreed and Accepted, upon execution of Order Form / Dated: Effective Date

_____

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Section B(i). Definitions

All capitalized terms used herein, but not otherwise defined, shall have the same meaning afforded to it within the General Terms and Conditions and any Appendix thereto.

The terms "**data importer**" and "**data exporter**" shall have the same meaning as set out in the Controller-to-Controller SCCs (data transfer agreement).

*Defined terms herein shall have the same meaning as in The General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing the Directive (the "**GDPR**") unless otherwise stated to the contrary hereunder:*

BIMobject Cloud: the software and all functionalities, interfaces, features, solutions, websites, products and services made available by BIMobject and BIMobject Affiliates to customers, Users, visitors and others from time to time from time to time, including but not limited to the Services, excluding any third-party links to other domains, collectively or in part(s);

BIMobject Cloud Privacy Policy: the Privacy Policy for BIMobject Cloud (as amended from time to time) located at https://accounts.bimobject.com/privacypolicy and https://accounts.bimobject.com/privacynoticeforcaliforniaresidents;

Customer Contract: any instruction, confirmation, contract, agreement (written or oral), order form, sales paper, proposal, whether physically or electronically executed or any other document, instrument or agreement which governs the provision of the Customer Services to the Customer entered into between the BIMobject Company and the Customer;

Customer Personal Data: Personal Data which Customer uploads or otherwise provides BIMobject on BIMobject Cloud directly, in connection with, or resulting from its use of the Customer Services where Customer determines the purpose of the processing of same and in respect of which Customer is the data controller;

Customer Services: the services provided to Customer under the Customer Contract, which may include the Customer's use of BIMobject Cloud, Subscribed Services, and/or any Model Development and/or hosting services provided by BIMobject to Customer through the BIMobject Cloud, and any ancillary products and services provided whether purchased via renewable subscription or as a one-time purchase;

Data Protection Laws: The General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing the Directive (the "**GDPR**");

Data Subject: Any User(s) and/or any other individuals whose Personal Data are processed on behalf of Customer through the Customer Services;

User(s): Any individual(s) who has/have registered an account on BIMobject Cloud.

Section B(ii). Background

1.1 BIMobject provides unique solutions to support digital construction, development, hosting, maintenance, syndication and publication of the digital replicas of manufactured products – "BIM Objects". In the case of Customer, BIMobject provides the solutions tools and functions in order to provide the Customer Services to the Customer in accordance with and in the manner set out in the Customer Contract and for the purposes determined by the Customer therein.

1.2 Customer understands and accepts that BIMobject is data controller in respect of the Processing of the Personal Data of Data Subjects who register as Users under the BIMobject Cloud. Details of the Processing by BIMobject of User Personal Data is more particularly described in the BIMobject Cloud Privacy Policy.

1.3 Upon download by any User of a Customer BIM Object on the BIMobject Cloud, Personal Data of such User becomes visible to Customer whereupon Customer may choose to contact or otherwise interact with such User in accordance with the Permitted Purposes in Schedule 1 of the Data Protection Agreement. It is acknowledged in such circumstances that Customer determines the purpose of the Processing of such Personal Data and therefore in accordance with Data Protection Laws is the data controller in respect of same.

1.4 The categories of Personal Data processed and the categories of Data Subjects are described hereunder.

Categories of data subjects whose personal data is transferred

Users under the BIMobject Cloud: Users whose Personal Data is accessed by or available to the data importer through the data importer's use of the Customer Services.

Categories of personal data transferred

The Personal Data transferred may concern the following categories of data (which may be updated from time to time on BIMobject Cloud):

- Name
- Email address
- Postal code, city and state
- Country name
- Occupation
- Company name
- Employer's details
- Phone number
- Picture
- Usage and downloads history

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data exporter does not require or intend for Users to provide Sensitive Data to the data exporter for transfer to the data importer. Sensitive data could only be transferred in the event and for any reason any of the categories of Relevant Personal Data above could be deemed to comprise Sensitive Data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of data transfer may be on a continuous basis during the term of the Agreement

Nature of the processing

See Background above.

Purpose(s) of the data transfer and further processing

The transfer is made for the following purposes:

Global accessibility

One of the main features of BIMobject Cloud is that it is globally accessible. Personal Data is transferred cross-border in order that the data exporter can provide, and the data importer can access and receive the global Customer Services under BIMobject Cloud as the case may be.

Data exporter and data importer as controllers

The cross-border transfer of Personal Data is intended to enable:

a. the data exporter to determine the purpose and the means of the processing of personal data where the data exporter determines to provide the globally accessible BIMobject Cloud; and

b. subject to the Permitted Purposes, the data importer determines the purposes and means of the processing of Personal Data by accessing, transferring, exporting and processing Personal Data (including EU Personal Data) globally, across borders and outside the EEA as the case may be.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The Personal Data transferred between the parties may only be retained for the period of time permitted under the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

[_____]

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
Swedish Authority for Privacy Protection

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Only Customers with an active Customer Agreement, including Subscription Services, who log into BIMobject Cloud can access Personal Data. To the extent that the Personal Data remains within the BIMobject Cloud, the below security measures are applicable to both data exporters and data importers. In the event a data importer transfers Personal Data from the BIMobject Cloud, said data importer must supplement this ANNEX II with their own necessary security measures.

BIMobject has taken the following security measures to ensure the safety of Personal Data within the BIMobject Cloud:

- Details on BIMobject's security protocols are set forth at the Security Statement at https://business.bimobject.com/security-statement/?standalone=false
- All infrastructure related to BIMobject Cloud is located in Microsoft Azure Cloud's North Europe datacenter in Ireland. Microsoft Azure datacenters comply with key industry standards for security and reliability and are managed, monitored, and administered by experienced Microsoft operations staff. For more information about Azure security see: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure
- The BIMobject Cloud Production system maintains isolation by limiting access to the operational personnel of BIMobject.
- BIMobject Cloud data is stored in Microsoft SQL Database with redundant file storage in Microsoft Azure Cloud.
- All of the BIMobject Cloud online services are accessible on secured http protocol (HTTPS) and regular penetration tests are carried out to ensure the system is well secured.
- In addition to supporting third party identity providers such as Autodesk, Google and LinkedIn, BIMobject Cloud has its own identity providers whereby Customers log in with username and password. All passwords are stored encrypted in BIMobject's database.
    - All the BIMobject Cloud data and files are backed up daily.
- BIMobject Cloud utilizes an Incident Response Plan (IRL) to address cyber security issues and tests the IRL annually.
    - If Users remove their account from BIMobject Cloud, their Personal Data is anonymized in BIMobject databases. The data importer will receive a unique identification key in their next Personal Data access or export to anonymize the User in their records.

Additional data importer security measures when Personal Data removed from the BIMobject Cloud:

[Placeholder for data importer security measures inserted upon execution of Order Form, as necessary]

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter