AUTODESK

BINDING CORPORATE RULES CONTROLLER POLICY

PART 1 – INTRODUCTION AND SCOPE

1. BACKGROUND

European Data Protection Law restricts the transfer of personal data to countries, territories or international organisations outside Europe that do not ensure an adequate level of protection for personal data. The legal systems in some of the countries in which Autodesk operates do not provide an adequate level of data protection in accordance with European Data Protection Law.

Autodesk wishes to ensure that the transfer of Personal Data between Autodesk Companies complies with European Data Protection Law. The purpose of this Binding Corporate Rules Controller Policy and its Appendices (together the "**Policy**"), therefore, is to set out a framework based on European Data Protection Law that provides an overall adequate level of protection for Personal Data processed and transferred within Autodesk.

2. OPERATION OF THE POLICY

The Policy is divided into four sections:

Part 1 – Introduction and Scope

Part 2 – The Rules: contains 17 Rules that identify specific obligations with which each Autodesk Company must comply with when processing Personal Data under this Policy.

Part 3 – Third Party Beneficiary Rights: confers enforceable rights on data subjects regarding the processing of their Personal Data under the Policy.

Part 4 – Practical compliance: deals with internal mechanisms implemented within Autodesk to facilitate compliance with European Data Protection Laws.

3. ACCESS TO THE POLICY

The list of Autodesk Companies bound by the Policy and their contact details are contained at Appendix 1 of this Policy. The Policy will be published on the website accessible at Privacy | Autodesk Trust Center.

4. DEFINITIONS

In addition to other definitions provided under this Policy, the following further terms shall have the meanings ascribed to them:

(a) "**Autodesk**" means, collectively, Autodesk, Inc. and each Autodesk Company;

(b) "**Autodesk Company**" means, individually, Autodesk, Inc. (ultimate parent company of the Autodesk Group), and each subsidiary of Autodesk, Inc. which is a signatory to the Intra-Group Agreement relating to the Policy;

(c) "**controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data;

(d) **"Competent Supervisory Authority" means the** supervisory authority (defined below) competent for the Exporting Entity.

(e) **"Data Processing Agreement"** means a contract or any other type of legal instrument containing data processing terms and conditions, whether as part of a contract for professional services or otherwise;

(f) "**Data Protection, Use & Ethics team**" means the team at Autodesk responsible for providing legal counsel, policy and strategic advice on global laws, regulations and best practices concerning data protection, data use and ethics;

(g) "**Europe**" means the countries in the European Economic Area ("**EEA**"), UK, and Switzerland.

(h) "**European Data Protection Law**" means the European Union (EU) Regulation 2016/679 (the General Data Protection Regulation) ("**GDPR**") and any data protection law of a European Member State, UK and Switzerland, including local legislation implementing the requirements of the GDPR and subordinate legislation, in each case as amended from time to time;

(i) "**Exporting Entity**" means an Autodesk Company established in Europe that is processing Personal Data as a controller and transferring such Personal Data to an Importing Entity under this Policy;

(j) "**Importing Entity**" means an Autodesk Company established in a country outside Europe which has not been regarded by the European Commission as providing such an adequate level of data protection for personal data and which receives Personal Data directly from an Exporting Entity or via another non-European Autodesk Company under this Policy;

(k) "**Non-European Countries**" means any country other than countries members of the European Economic Area, Switzerland or the United Kingdom;

(l) **"Personal data"** means any information which relates to an identified or identifiable natural person (each referred to as a "**data subject**" in this Policy);

(m) "**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

(n) "**process**"/ "**processing**" means any operation that Autodesk performs on Personal Data, whether manually or by automatic means. References to the "transfer" of Personal Data fall within the definition of processing;

(o) **"Processing Workers"** means employees, officers, directors, and contingent workers at Autodesk who in the course of their work process personal data;

(p) **"processor"** means the entity which processes personal data on behalf of the controller;

(q) "**special categories of Personal Data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying an individual, data concerning health or data concerning a natural person's sex life or sexual orientation;

(r) "**supervisory authority**" means an independent public authority established in a European jurisdiction which is responsible for monitoring the application of European Data Protection Law in order to protect the fundamental rights and freedoms of data subjects in relation to processing;

(s) "**supplementary measures**" means contractual, technical or organisational measures which, if combined with the safeguards contained in this Policy, are put in place to ensure that the Personal Data transferred to an Importing Entity is afforded a level of protection essentially equivalent to that guaranteed within Europe in those (rare) cases where the Policy may not be an effective transfer tool due to the Importing Entity's national legislation applicable to the transfer;

(t) "**Third Party Entity**" means an entity which is not an Autodesk Company;

(u) "**Trust Organization**" means the team at Autodesk under the leadership of the Senior Vice President, Chief Trust Officer, responsible for security, privacy, compliance, risk management, Trusted AI, and resiliency; and

(v) "**workers**" means employees, officers, directors and contingent workers at Autodesk.

5. SCOPE OF THE POLICY

This Policy puts into practice in a legally binding manner the approach taken by Autodesk to the protection and management of Personal Data by Autodesk when such Personal Data is processed by and/or transferred from Exporting Entities to Importing Entities located in the third countries set out in Appendix 1 of this Policy, in all cases where Autodesk Companies act as controllers or, as applicable, as processors on behalf of a controller Autodesk Company.

In particular, Personal Data under this Policy relates to the categories of data subjects whose Personal Data is transferred for the purposes set out at Appendix 2 of this Policy.

For completeness, Autodesk Companies must comply with the Binding Corporate Rules Processor Policy when processing Personal Data as processors or sub-processors for Third Party Entities.

6. COMMITMENT TO THE POLICY

Pursuant to a legally binding mechanism between Autodesk Companies, each Autodesk Company processing Personal Data under the Policy must comply with and respect this Policy and ensure that their respective workers are legally bound to respect the requirements of this Policy.

When an Autodesk Company processes Personal Data as a processor on behalf of another Autodesk Company, it must comply with and respect the Rules in this Policy to the extent that such Rules set out in this Policy apply to the processing.

7. RELATIONSHIP BETWEEN NATIONAL LAWS AND THIS POLICY

Subject to Rule 6 and Rule 14 in Part 2, Autodesk Companies shall comply with applicable local law when processing Personal Data.

Where there is no applicable local law or if the standards required by local law are lesser than or do not meet the standards set out in this Policy, Autodesk Companies shall process Personal Data in accordance with this Policy. Where applicable local law requires a higher level of protection for Personal Data than is provided for in this Policy, the higher level of protection will take precedence over this Policy and should be applied to the processing of Personal Data.

Where national legislation prevents Autodesk Companies from fulfilling or has a substantial adverse effect on their ability to comply with, their obligations under this Policy, Autodesk Companies will follow the process set out in Rule 14 of Part 2.

8. FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues in relation to the Policy, you can contact using the following contact details:

Attention: Richard Greene
Director, EMEA Privacy Counsel & Data Protection Officer ("DPO")

E-mail: privacy.questions@autodesk.com

Post: 2nd Floor
1 Windmill Lane
Dublin
D02 F206
Ireland

Telephone: (01) 571 8800

Autodesk's Director, EMEA Privacy Counsel & DPO and other privacy professionals may be directly contacted using the contact details provided above.

PART 2 – THE RULES

RULE 1 – FAIRNESS AND LAWFULNESS

Autodesk Companies will ensure that their processing of Personal Data is fair and lawful, and that a legal basis for processing Personal Data exists. In particular, unless otherwise permitted or required by any specific provisions of a particular European Union or Member State law, Autodesk Companies will only process Personal Data where:

- the data subject has given **consent** to the processing of his or her Personal Data and that consent meets the required standards under European Data Protection Law; or
- it is **necessary for the performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject before entering into a contract; or
- it is **necessary for compliance with a legal obligation** to which the Autodesk Company is subject where that legal obligation derives from European law or the law of a European Member State; or
- it is **necessary in order to protect the vital interests** of the data subject or of another individual; or
- it is **necessary for the purposes of the legitimate interests pursued by an Autodesk Company or by a third party**, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Where the processing of Personal Data relates to criminal convictions and offences or related security measures, an Autodesk Company will not carry out such processing otherwise than under the control of official authority or when the processing is authorised by European Union or Member State law that provides appropriate safeguards for the rights and freedoms of data subjects.

RULE 2 – PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Processing of special categories of Personal Data is only permitted on certain grounds, with the following being most relevant to the processing undertaken by Autodesk:

- Autodesk has obtained explicit consent to the processing of any special category of Personal Data relating to a data subject for one or more specified purposes, unless European Data Protection Law provides that the prohibition to processing special category data may not be lifted by a data subject; or
- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Autodesk or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of data subjects; or
- the processing relates to Personal Data that are manifestly made public by the data subject; or
- the processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in a judicial capacity; or
- the processing is necessary for reasons of substantial public interest on the basis of European Union or Member State law provided that it is proportionate to the aim pursued, respects the essence of data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject; or

- the processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or Member State law provided that the processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under European Union or Member State law or by rules established by national competent bodies.

RULE 3 – TRANSPARENCY

Autodesk will ensure that data subjects are able to access this Policy on its website at Privacy | Autodesk Trust Center.

Autodesk Companies will ensure that data subjects are informed in a concise, transparent, intelligible and easily accessible form, using clear and plain language, about how their Personal Data will be processed.

When Autodesk Companies obtain Personal Data directly from the data subject, they must provide such data subjects with at least all information required by European Data Protection Laws, including:

- the identity and contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer;
- the purposes of the processing as well as the legal basis for processing. Where any Personal Data is processed on the basis of legitimate interests, Autodesk Companies will provide details about the legitimate interest on which basis they process Personal Data;
- the recipients or categories of recipients of Personal Data;
- information about the safeguards in place to protect Personal Data when it is transferred internationally and how to obtain a copy of such safeguards. In the case of transfers of Personal Data under this Policy, the information provided will include reference to this Policy and how to access it;
- the length of time for which Personal Data will be retained, or the criteria applied to calculate this;
- data subjects' rights to: access, rectify, erase, restrict, object to the processing of Personal Data, data portability, complain to a supervisory authority; and, where processing is based on consent, the right to withdraw consent;
- whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into contract, as well as whether the data subject is obliged to provide the Personal Data and the consequences of the failure to provide Personal Data in such circumstances;
- at least where required by European Data Protection Law, details of the processing of Personal Data for automated decision-making, including profiling, and at least in cases where such decisions produce legal effects concerning the data subject or similarly significantly affect the data subject, or are based on special categories of Personal Data, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The above information will be provided at the time when Personal Data is obtained by Autodesk Companies from the data subjects.

When Autodesk obtains data subjects' Personal Data from a source other than the data subject, Autodesk will provide the above information to the data subject, together with information about the source and categories of Personal Data received from third parties, as follows:

- within a reasonable period of time after Personal Data is collected, but at the latest within one month;
- if the Personal Data is to be processed for communication with the data subject, at the latest at the time of the first communication to that data subject; or,
- if it is to be disclosed to a third party, no later than the time when the data is first disclosed.

Where, in accordance with Rule 4, an Autodesk Company intends to further process Personal Data for a purpose other than that for which it was originally collected, the Autodesk Company will provide the data subject, before the further processing begins, with information on that other purpose and with any relevant further information as described above.

Autodesk will follow this Rule 3 unless not providing the above information is specifically permitted by European Data Protection Law.

RULE 4 – PURPOSE LIMITATION

Autodesk will process Personal Data only for specific, explicit and legitimate purposes as notified to data subjects in accordance with Rule 3.

If Autodesk Companies wish to process Personal Data for a different or new purpose other than that notified to data subjects, they will not further process that information in a way incompatible with the purpose for which it was collected. In order to ascertain whether processing for a different or new purpose is compatible with the purpose for which the Personal Data are initially collected, Autodesk Companies will take into account, amongst other considerations, the following:

- any link between the purposes for which the Personal Data have been collected and the purposes of the intended further processing;
- the context in which the Personal Data have been collected, in particular regarding the relationship between data subjects and Autodesk Companies;
- the nature of the Personal Data, in particular whether special categories of Personal Data are processed, or whether Personal Data related to criminal convictions and offences are processed;
- the possible consequences of the intended further processing for data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

In certain cases, the data subject's consent to the new processing may be necessary, unless the processing is based on the law of the European Union or a Member State which constitutes a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest.

RULE 5 – DATA MINIMISATION AND ACCURACY

Autodesk will only process Personal Data which is adequate, relevant and limited to what is necessary for the purposes of such processing.

Autodesk will keep Personal Data accurate and up to date. For that purpose, Autodesk Companies shall actively encourage data subjects to inform the Autodesk Companies with which they interact when their Personal Data changes. Having regard to the purposes for which Personal Data is processed, Autodesk Companies will take every reasonable step to ensure that Personal Data that is inaccurate is erased or rectified without undue delay.

Autodesk manages Personal Data centrally with relevant Autodesk Companies accessing and maintaining such databases as appropriate (e.g. changes to Personal Data will be recorded in a central database so that relevant Autodesk Companies will have access to the updated Personal Data as soon as the change has been made). This helps ensure that Personal Data is kept accurate and up to date.

RULE 6 – LIMITED STORAGE PERIODS

Autodesk Companies will comply with their respective record retention policies and schedules, as revised and updated from time to time, to ensure that Personal Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which that Personal Data is processed.

Records shall be retained in accordance with the respective record retention policies and schedules and, unless there is a new legal basis for further compatible processing of Personal Data (as set out in Rule 4) which therefore requires a different retention period than that of the initial purpose), shall be destroyed at the conclusion of the relevant retention period. Any changes to the relevant retention schedule must be approved by the legal department.

Managers are responsible for maintaining processes and procedures to ensure compliance with their respective record retention policies and schedules.

RULE 7 – SECURITY

Rule 7A – Autodesk Companies will keep Personal Data secure

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, Autodesk will implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of Personal Data over a network, and against all other unlawful forms of processing.

Autodesk Companies will comply with their respective IT security policies as revised and updated from time to time, together with any other security procedures relevant to a particular business area or function. Additional information about Autodesk' security procedures is publicly available at Autodesk Trust Centre at https://www.autodesk.com/trust/overview.

Rule 7B– Autodesk Companies will ensure that contracts with all Autodesk Companies and/or Third Party Entities acting as processors on behalf of Autodesk Companies comprise all requirements set out in European Data Protection Law.

Autodesk Companies which appoint an Autodesk Company and/or a Third Party Entities as processors to process Personal Data on their behalf will comply with their respective due diligence processes for the selection of the processor to ensure that the processor can provide sufficient

guarantees that they will put in place appropriate technical and organisational security measures in such a manner that processing will meet the requirements of this Policy and European Data Protection Laws, and ensure the protection of the rights of data subjects.

Autodesk Companies acting as controllers must impose strict contractual obligations evidenced in writing in line with the requirements set out in European Data Protection Law in the form of a Data Processing Agreement, including the following requirements:

- details of the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects and the obligations and rights of the controller;
- commitments on the part of the processor:
    - to act only on Autodesk's instructions when processing Personal Data including with regard to transfers of such Personal Data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest;
    - to ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    - taking into account the nature of the processing and insofar as this is possible, to assist the Autodesk Company by appropriate technical and organisational measures in relation to the fulfilment of that Autodesk Company's obligations: i) to respond to requests from individuals relating to their rights under European Data Protection Law; and ii) relating to the security of processing, the notification of Personal Data breaches, and the requirements to carry out data protection impact assessments and for prior consultation with supervisory authorities;
    - at the choice of the Autodesk Company, to delete or return to that Autodesk Company all Personal Data processed on behalf of the Autodesk Company after the end of the provision of the services provided under the Data Processing Agreement, and delete existing copies unless European Union or Member State law requires storage of such Personal Data;
    - to make available to Autodesk Company all information necessary to demonstrate compliance with the obligations imposed upon the processor under the Data Processing Agreement, and allow for, and contribute to, audits, including inspections, conducted by the Autodesk Company, or another auditor mandated by the Autodesk Company;
    - to immediately inform the Autodesk Company if, in the processor's opinion, an instruction infringes European Data Protection Laws.
    - to comply with the Autodesk Company's documented instructions in relation to the appointment of sub-processors and, in particular, not to engage another processor without the prior specific or general written authorisation of Autodesk, and in the case of general written authorisation, the processor shall inform Autodesk of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes; and
    - where the processor engages another processor for carrying out specific processing activities on behalf of Autodesk, to include the same data protection obligations as are set out in the Data Processing Agreement in a contract or other legal act under European Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational

measures in such a manner that the processing will meet the requirements of European Data Protection Law Where the other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to Autodesk for the performance of that other processor's obligations.

Where one Autodesk Company (processor) is processing Personal Data as a processor on behalf of another Autodesk Company (controller):

- the subject-matter and duration of the processing, the nature and purpose of the processing, the types of Personal Data and the categories of data subjects will be set out in a document agreed between the parties substantially in the form set out in Appendix 3;
- the processor will act only on documented instructions of controller as may be set out in Appendix 3; and
- the processor will comply with the obligations set out in Part 2 of Appendix 3 or, as appropriate, a contract or legal act entered into between controller and processor in relation to such processing which is consistent with European Data Protection Law in so far as it relates to the engagement of a processor.

Rule 7C – Autodesk Companies will adhere to their respective data breach notification policies

Autodesk Companies will adhere to their respective data breach notification policies (as revised and updated from time to time) which set out the process that Autodesk Companies must follow, in accordance with European Data Protection Laws, to notify without undue delay:

- Autodesk Ireland Operations Unlimited Company and the Incident Response Team at Contact Us | Autodesk Trust Center.
- The Autodesk Company acting as a controller when an Autodesk Company acting as a processor becomes aware of a data breach;
- the Competent Supervisory Authority and, where feasible, not later than 72 hours after having become aware of the personal data breach affecting Personal Data, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects; and
- data subjects in cases where the personal data breach is likely to result in a risk to the data subjects' rights and freedoms, unless such notification is not required under European Data Protection Law.

Autodesk Companies will maintain a documented record of any personal data breaches involving Personal Data, comprising at least a description of the facts, the effects and the remedial action which has been or will be taken. Such documentation will be made available to the Competent Supervisory Authority on request.

RULE 8 – TRANSFERS AND ONWARD TRANSFERS

Autodesk Companies will only transfer Personal Data to Third Party Entities outside Europe if adequate protection for Personal Data is ensured as provided for under European Data Protection Laws, such as by:

- confirming that the Third-Party Entity is in a country which the European Commission has found to offer an adequate level of protection for the personal data transferred; or
- signing up to the European Commission approved Standard Contractual Clauses; or

- obtaining the explicit consent of data subjects, after they have been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards; or

- ensuring that the transfer is necessary for:

    - the performance of a contract between the data subject and the Exporting Entity or for the implementation of pre-contractual measures taken at the data subject's request;

    - the conclusion or performance of a contract concluded in the interest of the data subject between the Exporting Entity and another party.

    - important reasons of public interest as laid down by European Union or Member State law;

    - the establishment, exercise or defence of legal claims.

    - the protection of the vital interests of the individual or of another individual and where the individual is incapable of giving consent.

Autodesk Companies acting as processors on behalf of other Autodesk Companies will only transfer Personal Data to a Third-Party Entity outside Europe in accordance with the instructions of the controller Autodesk Company in accordance with Rule 7B.

RULE 9– RIGHTS OF DATA SUBJECTS

On request, data subjects whose Personal Data is processed under this Policy are entitled to exercise their right to:

- be informed by Autodesk Companies whether any Personal Data is being processed by them and, if Autodesk Companies do process their Personal Data, they are entitled to access such Personal Data and be given a description of how Autodesk Companies process such information (this is known as the right of access);

- request rectification, completion, erasure, or restriction of their Personal Data and notification regarding rectification or erasure or restriction;

- portability in relation to their Personal Data;

- object to the processing of their Personal Data including processing for direct marketing purposes and to profiling to the extent that it is related to such marketing; and

- not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless one of the following exception applies: the processing is authorised under European Data Protection Law; the decision is necessary for entering into a contract between the data subject and Autodesk or the data subject has given their explicit consent. Where an exception applies, Autodesk will put in place measures to protect the rights and freedoms and legitimate interests of data subjects (such as the right for an individual to obtain human intervention in the decision, to express his or her point of view, and to contest the decision.

European Data Protection Law to which the Autodesk Companies are subject may restrict the exercise of data subject rights when such a restriction is necessary and proportionate to safeguard: national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest; the

protection of the data subject or the rights and freedoms of others; or the enforcement of civil law claims.

Autodesk Companies will comply with their respective policies dealing with rights of data subjects whose Personal Data is processed under this Policy, as revised and updated from time to time.

Requests from data subjects relating to the rights described in this Rule may be made via email at privacy.questions@autodesk.com.

If an Autodesk Company receives any request from a data subject relating to the rights described above, this must be passed to a Data Privacy Manager from the Trust Organization, who will coordinate a response. A Data Privacy Manager from the Trust Organization will acknowledge receipt of a data subject request to the data subject concerned within five working days.

The Data Privacy Manager will refer the matter to the Director, EMEA Privacy Counsel & DPO who will investigate and make a substantive response within one month. If, due to the complexity of the request and number of requests, a substantive response cannot be given within this period, the Data Privacy Manager will advise the data subject of the reason for the delay within one month of receipt of the request, and provide a reasonable estimate (not exceeding two further months from the date on which the individual was notified of the extension) for the timescale within which a response will be provided.

In addition, Customers can request a copy of the Personal Data in their account and request deletion of Personal Data by submitting an online form which can be accessed via the Autodesk Privacy Statement available at https://www.autodesk.com/company/legal-notices-trademarks/privacy-statement. Such requests will be managed by an automated process.

Where Autodesk Companies act as processors on behalf of other Autodesk Companies, the Autodesk Companies acting as processors will act in accordance with the lawful instructions of the controller Autodesk Company and will undertake any reasonably necessary measures to enable that controller to comply with its duty to respect the rights of data subjects.

RULE 10 – ACCOUNTABILITY

Autodesk Companies will be responsible for and able to demonstrate compliance with this Policy and Autodesk Companies will have appropriate staff and support to ensure and oversee compliance with this Policy throughout the business.

RULE 11 – RECORDS OF PROCESSING ACTIVITIES

Autodesk Companies will maintain a written (including in electronic form) record of all categories of processing activities and make that record available to competent supervisory authorities on request.

The data processing records maintained by Autodesk Companies will contain:

- the Autodesk Company's name and contact details and, where applicable, the joint controller, the Autodesk Company's representative and the data protection officer;
- the purposes for which Personal Data is processed;
- a description of the categories of data subjects about whom Personal Data is processed and the Personal Data processed;
- the categories of recipients to whom Personal Data have been or will be disclosed including recipients in third countries or international organisations;

- details of the third country or countries to which Personal Data is transferred, including the identification of that third country or international organisation and the documentation of suitable safeguards in the event of transfers under the second subparagraph of Article 49(1) of the GDPR;

- where possible, the period for which Personal Data will be retained; and

- where possible, a general description of the technical and organisational security measures used to protect Personal Data.

RULE 12 – DATA PROTECTION IMPACT ASSESSMENTS

Autodesk Companies will assess the impact of any new processing of Personal Data and, in the case, it involves high risks to the rights and freedoms of data subjects, Autodesk Companies will carry out data protection impact assessments (DPIA).

DPIAs will be conducted by the Data Protection, Use & Ethics team, collaborating with the business team involved in the processing activity that triggered the DPIA. The Data Protection, Use & Ethics team will assess the risk considering impact and likelihood, and suggest mitigating measures to each of the risks identified. Those risks and measures to be implemented will be communicated to the business team responsible for such activity, and a deadline for implementation will be provided and monitored. If the activity involved processing personal data of workers, the Autodesk Company responsible for such processing activity may consult with the local workers council, if applicable.

When conducting DPIAs, Autodesk Companies should, whenever possible and without compromising the DPIA's role in identifying and mitigating risks to data subjects, in accordance with European Data Protection Law, consider requirements from other European law that may also necessitate impact assessments. Autodesk Companies should aim to obtain a comprehensive understanding of the processing activity and its ultimate impact on the data subject, considering all sources of possible risk, including the technology used for processing personal data.

Where such DPIA indicate a low or medium residual risk, such residual risks will be documented and managed by the Trust Organization. Where such DPIA indicate that the processing would result in a residual high risk to data subjects, in the absence of measures taken by the Autodesk Company to mitigate the risk, Autodesk Companies will carry out a consultation with the Competent Supervisory Authority prior to the processing.

Autodesk Companies acting as processors on behalf of another Autodesk Company will be required to co-operate as appropriate to assist Autodesk Companies acting as controllers in ensuring compliance with their obligations under this Rule 12.

RULE 13– DATA PROTECTION BY DESIGN AND BY DEFAULT

Autodesk Companies will implement appropriate technical and organisational measures to enable and facilitate compliance with the Policy in practice.

Taking into account the state of the art and cost of implementation and the scope, nature, context and purposes of the processing, Autodesk will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by European Data Protection Law. Autodesk will integrate such measures into the processing when determining the means of the processing, and the time of processing itself to facilitate the protection of Personal Data being processed, and to ensure that, by default, only Personal Data which is necessary for each specific purpose of the processing is processed.

RULE 14 – NATIONAL LAWS AND PRACTICES PREVENTING AUTODESK FROM COMPLYING WITH THE POLICY

Rule 14A – Autodesk Companies will carry out a transfer impact assessment before making transfers to Importing Entities not subject to an adequacy decision under this Policy.

Autodesk Companies will carry out and document a transfer impact assessment to assess if the laws and practices applicable to it prevents it from fulfilling its obligations under this Policy, or has a substantial effect on the guarantees provided under this Policy before making transfers under this Policy or in the event that the relevant legislation is modified. The transfer impact assessment will be based on the understanding that laws and practices that respect fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society will not contradict this Policy.

In carrying out the assessment, the Autodesk Companies will take into account:

a. The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:
- purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support);
- types of entities involved in the processing (the initial data recipient and any further recipient of any onward transfer);
- economic sector in which the transfer or set of transfers occur;
- categories and format of the personal data transferred;
- location of the processing, including storage; and
- transmission channels used.

b. the laws and practices of the third country of destination relevant in light of the circumstances of the transfer including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards; and

c. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under this Policy, including measures applied during the transmission and to the processing of the personal data in the country of destination.

Autodesk Companies will put in place such contractual, technical or organisational safeguards as may be appropriate in the circumstances to supplement the safeguards in this Policy in light of the law and practice in the third country so to ensure an essentially equivalent level of protection for Personal Data. Where a transfer impact determines that additional safeguards to those envisaged under this Policy should be put in place, the Exporting Entity and the Director EMEA Privacy Counsel & DPO will be informed and involved in such an assessment and the selection and implementation of the relevant supplementary measures.

Autodesk Companies will document its transfer impact assessments, as well as any supplementary measures selected and implemented, and will make such documentation available to a Competent Supervisory Authority upon request.

Rule 14B - Autodesk will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on the guarantees provided by the Policy, Autodesk will promptly inform the Director, EMEA Privacy Counsel & DPO unless otherwise prohibited by law or by a law enforcement authority.

The Importing Entity will notify the Exporting Entity and the Director, EMEA Privacy Counsel & DPO if, when making a transfer under this policy, it has reason to believe that it is, or has become,

subject to laws or practices that would prevent it from fulfilling its obligations under this Policy. This will include changes in laws in a third country or a measure (such as a disclosure request) unless prohibited by law or a law enforcement authority (for example, in instances in which Autodesk is subject to a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Upon verification of such notification, the Exporting Entity along with Autodesk Ireland Operations Unlimited Company and the Director, EMEA Privacy Counsel & DPO, will promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by Exporting Entity and/or the Importing Entity to address the situation. The same applies if the Exporting Entity has reasons to believe that the Importing Entity can no longer fulfil its obligations under this Policy.

The Exporting Entity will suspend the data transfer and any transfers for which the same assessment and reasoning would lead to a similar result, if it, along with the Director, EMEA Privacy Counsel & DPO, considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Competent Supervisory Authority to do so. The suspension will last for as long as compliance with this Policy can be achieved or the transfer is ended.

Following such a suspension, the Exporting Entity will end the transfer or set of transfers if this Policy cannot be complied with and compliance with the Policy is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Exporting Entity be returned to it or destroyed in their entirety.

Autodesk Ireland Operations Unlimited Company and the Director, EMEA Privacy Counsel & DPO will inform all other Autodesk Companies of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Autodesk Company or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

The Exporting Entities will monitor, on an ongoing basis, and where appropriate in collaboration with the Importing Entity, developments in the third countries to which Autodesk has transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

Rule 14C – Where an Importing Entities receives a legally binding request from a law enforcement agency or state security body for disclosure of personal data transferred outside Europe under this Policy, the Importing Entity will notify the Exporting Entity, and where required and possible, the data subject

The Importing entity will promptly notify the Exporting Entity, and where required and possible, the data subject (if necessary with the help of the Exporting Entity) if it:

a. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination, or of another third country, for the disclosure of personal data transferred pursuant to this Policy; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

b. becomes aware of any direct access by public authorities to personal data transferred pursuant to this Policy in accordance with the laws of the country of destination; such notification will include all information available to Autodesk.

If the Importing Entity is prohibited from notifying the Exporting Entity and/or the data subject (where required), the Importing Entity 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 Importing Entity will document its best efforts in order to be able to demonstrate them on request of the Exporting Entity.

Where permissible under the laws of the country of destination, the Importing Entity will provide the Exporting Entity, at regular intervals, 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.). If the Importing Entity becomes partially or completely prohibited from providing the Exporting Entity with the aforementioned information, it will, without undue delay, inform the Exporting Entity accordingly. The Importing Entity will preserve this information for as long as the personal data is subject to the safeguards provided by this Policy, and will make it available to the Competent Supervisory Authority upon request.

The Importing Entity will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and may 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 Importing Entity will, under the same conditions, pursue possibilities of appeal. When challenging a request, The Importing Entity will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

The Importing Entity will 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 Exporting Entity. It will also make it available to the Competent Supervisory Authority upon request.

The Importing Entity will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, Autodesk Companies will also ensure that any transfers that it makes to a public authority are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

RULE 15– COMPLAINT HANDLING

Rule 15A – Data subjects will be able to bring complaints against Autodesk

All complaints made under the Policy can be brought in writing or verbally to the attention of the Director, EMEA Privacy Counsel & DPO who is responsible for complaints by emailing privacy.questions@autodesk.com, by telephone to (01) 571 8800, or by writing to the Director, EMEA Privacy Counsel & DPO at 1 Windmill Lane, Dublin Docklands, D02 F206, Dublin Complaints made verbally shall be recorded by Autodesk Companies, and verified with the individual making the complaint before taking any further action. While data subjects are encouraged to use the above points of contact, this is not mandatory.

Rule 15B – Autodesk will appoint a person to handle complaints

The Director, EMEA Privacy Counsel & DPO will ultimately handle complaints arising under this Policy and has an appropriate level of independence in the exercise of their functions. A Data Privacy Manager from the Trust Organization will liaise with relevant business units to investigate the complaint and will coordinate a response.

A Data Privacy Manager from the Trust Organization will acknowledge receipt of a complaint to the data subject concerned within five working days. The Data Privacy Manager will refer the matter to the Data Protection, Use & Ethics team who will investigate and make a substantive response within one month. If, due to the complexity of the complaint and number of requests, a substantive response cannot be given within this period, the Data Privacy Manager will advise the complainant of the reason for the delay within one month of receipt of the complaint, and provide a reasonable estimate (not exceeding two further months from the date on which the individual was notified of the extension) for the timescale within which a response will be provided.

The Data Privacy Manager will also inform the concerned data subjects that they have the right to:

- complain to a competent supervisory authority in the Member State in which the alleged infringement took place, or in which the data subject works or habitually resides; and/or

- bring proceedings against Autodesk Ireland Operations Unlimited Company in the courts of a Member State in which Autodesk has an establishment or in the Member State in which the data subject habitually resides.

If the complainant disputes the response provided, the matter will be referred to the Director, EMEA Privacy Counsel & DPO who will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Director, EMEA Privacy Counsel & DPO will respond to the complainant within one month of the referral. If, due to the complexity of the complaint and number of requests, a substantive response cannot be given within this period, the Data Privacy Manager will advise the complainant of the reason for the delay within one month of receipt of the referral, and provide a reasonable estimate for the timescale (not exceeding two further months) within which a response will be provided. If the complaint is upheld, the Director, EMEA Privacy Counsel & DPO will arrange for any necessary steps to be taken as a consequence.

These rights will apply whether or not they have first made a complaint to the Autodesk Company.

RULE 16– COOPERATION WITH SUPERVISORY AUTHORITIES

Autodesk Companies will cooperate with supervisory authorities by:

- making the necessary personnel available for dialogue with a supervisory authority in relation to this Policy where required;

- actively reviewing and considering:

    - any decisions made by competent supervisory authorities on any data protection law issues that may affect this Policy; and

    - the views of the European Data Protection Board and any successor body as outlined in its published EU guidance on Binding Corporate Rules;

- providing copies of the results of any audit of this Policy upon request to any Competent Supervisory Authority;

- agreeing to be audited (including where necessary, on-site) by the Competent Supervisory Authority for the purpose of reviewing compliance with this Policy in accordance with the applicable law and audit procedures of:

    - the country in which the Autodesk Company being audited is located where the Autodesk Company is based in Europe; and

    - the European country from which Personal Data is transferred, where the Autodesk Company is located outside Europe;

- agreeing to take into account the advice and comply with the formal decisions of a Competent Supervisory Authority relating to the interpretation and application of this Policy, without prejudice to any right to appeal such formal decisions.

Any dispute related to the Competent Supervisory Authorities' exercise of supervision of compliance with this Policy will be resolved by the courts of the Member State of that Competent Supervisory Authority, in accordance with that Member State's procedural law. Autodesk Companies agree to submit themselves to the jurisdiction of these courts.

RULE 17 – NON-COMPLIANCE WITH THE BCRS AND TERMINATION

Rule 17A – Autodesk will take specific actions in the event that an Importing Entity is unable to comply with this Policy.

An Importing Entity will promptly inform the Exporting Entity if it is unable to comply with this Policy, for whatever reason, including the situations described in Rule 16 of this Policy.

When an Importing Entity is in breach of this Policy, or is unable to comply with it, the Exporting Entity will suspend transfers to that Importing Entity.

The Importing Entity will, at the choice of Exporting Entity, immediately return or delete the personal data that has been transferred under this Policy, where:

- the Exporting Entity has suspended the transfer, and compliance with this Policy is not restored within a reasonable time, and in any event within one month of suspension; or
- the Importing Entity is in substantial or persistent breach of this Policy; or
- the Importing Entity fails to comply with a binding decision of a competent court or the Competent Supervisory Authority regarding its obligations under this Policy.

The same commitments should apply to any copies of the data. The Importing Entity will certify the deletion of the data to the Exporting Entity. Until the data is deleted or returned, the Importing Entity will continue to ensure compliance with this Policy.

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 this Policy, and will only process the data to the extent and for as long as required under that local law. For cases were applicable local laws and/or practices affect compliance with this Policy, see Rule 16 above.

Rule 17B – Any personal data received under this policy that is kept by an Importing Entity that ceases to be bound by this Policy will be maintained in compliance with this Policy.

Any Importing Entity which ceases to be bound by this Policy may keep, return, or delete the personal data received under this Policy at the choice of the Exporting Entity.

If the Exporting Entity agrees that the data may be kept by the Importing Entity after that entity ceases to be bound by this Policy, the Importing Entity must continue to ensure compliance with this Policy in respect of the personal data it received under this Policy.

PART 3: THIRD PARTY BENEFICIARY RIGHTS UNDER THIS POLICY

A. European Data Protection Law provides data subjects with third-party beneficiary rights to uphold the level of protection afforded to personal data in Europe when Personal Data is transferred and processed outside Europe. As such, when Personal Data is transferred to and processed by an Importing Entity, this Policy sets forth third-party beneficiary rights to enforce compliance with:

- Part 2 of the Policy;
- Part 3 of the Policy in sections B to D granting third party beneficiary rights and setting the liability and jurisdiction rules under the Policy; and
- the right to access the Policy via Privacy | Autodesk Trust Center, or to obtain a hard copy of the Policy as well as a list of the Autodesk Companies bound by this Policy,

by:

- **making a complaint**: to the competent supervisory authority in the Member State in which the alleged infringement took place, or in which the data subjects works or habitually resides; and/or
- **bringing proceedings**: against Autodesk Ireland Operations Unlimited Company in the courts of a Member State in which Autodesk has an establishment or in the Member State in which the data subject habitually resides.

B. These individuals may in addition seek appropriate redress from Autodesk Ireland Operations Unlimited Company, which accepts responsibility for and agrees to take the necessary action to remedy any breach of the provisions or any of them listed in A by any Importing Entity and, where appropriate, receive compensation from Autodesk Ireland Operations Unlimited Company for any damage whether material or non-material suffered by data subjects as a result of a breach of the provisions or any of them listed in A by an Importing Entity in accordance with the determination of a court or other competent authority

C. For the avoidance of doubt, data subjects shall benefit from the third-party beneficiary rights as described in this Part 3 and the European courts or competent supervisory authorities shall have jurisdiction as if the breach of the provisions described in this Part 3 or any of them was caused by Autodesk Ireland Operations Unlimited Company in the Republic of Ireland. Autodesk accepts that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.[1]

D. In the event of a claim being made in which a data subject has suffered damage where that data subject can demonstrate that it is likely that the damage has occurred because a breach of this Policy, Autodesk has agreed that the burden of proof to show that an Importing Entity is not responsible for the breach, or that no such breach took place, will rest with Autodesk Ireland Operations Unlimited Company. If Autodesk Ireland Operations Unlimited Company can prove that the Importing Entity is not responsible for the event giving rise to the damage, Autodesk Ireland Operations Unlimited Company may discharge itself from any responsibility.

---

[1] Article 80(1) GDPR provides as follows *"The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77 [Right to lodge a complaint with a supervisory authority], 78 [Right to an effective judicial remedy against a supervisory authority] and 79 [Right to an effective judicial remedy against a controller or processor] on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."*

PART 4: PRACTICAL COMPLIANCE

1. COMPLIANCE NETWORK

Autodesk has appointed a Director, EMEA Privacy Counsel & DPO at Autodesk Ireland Operations Unlimited Company, based in Dublin, to oversee data privacy compliance matters in the EEA, including in relation to the BCR Controller Policy. The Director, EMEA Privacy Counsel & DPO is part of the Data Protection Use and Ethics team, and reports directly to the Global Senior Director of Data Privacy & Security (based out of the San Francisco office) and also has access to Autodesk's most senior management data governance stakeholders and the Chief Legal Officer. The Director, EMEA Privacy Counsel & DPO is also an adjunct member of the Privacy Steering Committee ("PSC"), which is an executive body that deals with specific privacy risks escalated to them and helps get the support needed across Autodesk. The PSC may escalate certain decisions and issues to CEO staff, and also facilitates updates to the Board of Directors.

The Director, EMEA Privacy Counsel & DPO is tasked with developing strategies and initiatives to engage with key stakeholders, and to raise awareness of data privacy, security compliance, and governance across Autodesk. The Director, EMEA Privacy Counsel & DPO also works closely with the Trust Organization to implement initiatives necessary for compliance with EU privacy laws and regulations, including in relation to the BCR Controller Policy, and sits on several committees including the PSC and the incident response team.

The Director, EMEA Privacy Counsel & DPO works with Trust Organization and other data governance stakeholders to (i) monitor compliance with the GDPR and other data protection laws, (ii) review internal data protection activities, (iii) advise on data protection impact assessments, (iv) train staff, and (v) support internal audits. The Trust Organization meets with the Director, EMEA Privacy Counsel & DPO on a quarterly basis to provide an update on matters relating to the processing of personal data by Autodesk. In addition, the Director, EMEA Privacy Counsel & DPO obtains legal advice on issues involving the processing of personal data by Autodesk. The Director, EMEA Privacy Counsel & DPO has the support of senior management and, where required, also has access to Autodesk's senior management and can inform the highest management level if any questions or problems arise during the performance of their duties.

The Director, EMEA Privacy Counsel & DPO does not have any tasks that could result in conflict of interests. The Director, EMEA Privacy Counsel & DPO will not be in charge of carrying out data protection impact assessments, nor in charge of carrying out audits if such situations can result in a conflict of interests. However, the Director, EMEA Privacy Counsel & DPO can play a very important and useful role in assisting the BCR members, and the advice of the Director, EMEA Privacy Counsel & DPO should be sought for such tasks.

2. TRAINING

Autodesk will provide appropriate and up to date training to Processing Workers who have permanent or regular access to Personal Data, who are involved in the processing of Personal Data or in the development of tools used to process Personal Data.

All training will be repeated on a regular basis which is envisaged to be approximately once every two years unless a need is identified for more frequent training as a result of any BCR audit, training needs assessment or generally as a result of any issues coming to the attention of the Director, EMEA Privacy Counsel & DPO.

The Trust Organization has overall responsibility for compliance and ethics training within Autodesk including the delivery of Autodesk's formal privacy online training modules. Autodesk has a global Web Based Learning ("**WBL**") that is available to all Workers. The Privacy Program Manager supports the completion of the WBL and is responsible for ensuring that Autodesk Processing Workers are given appropriate time to complete the course.

All Autodesk Processing Workers receive quarterly training on privacy and data protection and on Autodesk's Code of Business Conduct. Training will cover, among others, procedures for managing requests for access to personal data by public authorities and this Policy.

Processing Workers who have permanent or regular access to Personal Data, or who are involved in the processing of Personal Data or in the development of tools to process Personal Data, receive additional tailored training on the Policy and specific data protection issues relevant to their role on a regular basis. Similarly, Autodesk Processing Workers responsible for specific areas of compliance with the Policy, such as responding to data subjects' rights requests or handling complaints, receive specific tailored training in these areas. Training on other specific privacy-related matters such as Records Management, HIPAA Privacy and Security, or country-specific data protection is also provided on a need-to-know basis.

3. AUDIT

Continuing to independently monitor and ensure compliance is an important piece of maintaining trust and sustaining Autodesk's Global Privacy Program, including in relation to the commitments made in this Policy.

Autodesk have established controls to assess compliance with the commitments made in this Policy, and these controls are monitored twice a year through robust self-assessment and internal audit process by the Trust Organization. The Trust Organization decides on the audit programme and is responsible for overseeing the creation of supporting controls, ensuring self-assessments are conducted, as well as managing and mitigating any risks identified.

In addition, an independent audit of Autodesk's Global Privacy Program is conducted by the Autodesk Internal Audit team, a group within the Autodesk Audit & Advisory Services. This group is an independent, objective assurance and consulting organization designed to add value and improve risk areas. Audit of the procedures and controls in place to give effect to the commitments made in the Policy will be undertaken by the Audit & Advisory Services team at least every two years. The Audit & Advisory Services team may also use accredited external auditors. Audits will only be conducted by external auditors where the external auditor enters into a non-disclosure agreement containing sufficient guarantees to implement appropriate technical and organisational measures to protect any personal data entrusted to the external auditor. The Audit & Advisory Services will review all aspects of the scope of the Policy including methods of ensuring corrective actions will take place, taking into account relevant criteria (for example: areas of current regulatory focus or areas of specific or new risk within the products or services provided by Autodesk).

Specific audits (ad hoc audits) may be requested by the Director, EMEA Privacy Counsel & DPO or any other competent function within Autodesk. The Director, EMEA Privacy Counsel & DPO will not be in charge of carrying out audits of this Policy if such a situation could result in a conflict of interests.

The official results of the audits and, in particular, any issues or instances of non-compliance are brought to the attention of the Director, EMEA Privacy Counsel & Autodesk Data Protection Officer and presented to the Autodesk Audit Committee which is a group from Autodesk's ultimate parent company Board of Directors and the Board of Directors of Autodesk Ireland Operations Unlimited Company. The Audit Committee is established to assist the Board in fulfilling its oversight responsibilities by reviewing the financial reporting, the systems of internal controls, and the audit process, and by monitoring compliance with all applicable laws, regulations and policies, including ensuring that corrective actions under the Policy will take place.

Upon request, Autodesk Companies have agreed to provide copies of the results of any audit of this Policy to any Competent Supervisory Authority. The Director, EMEA Privacy Counsel & DPO

will be responsible for liaising with the competent supervisory authorities for the purpose of providing the requested information.

In addition, all Autodesk Companies agree to be audited by competent supervisory authorities in accordance with applicable audit procedures of such competent supervisory authorities.

4. UPDATES OF THE POLICY

Autodesk Companies will keep this Policy up-to-date in order to reflect the current situation (for instance, to take into account modifications of the regulatory environment and changes to the scope of the Policy).

Autodesk Companies will communicate any **material changes** to this Policy which would possibility be detrimental to the level of protection offered by this Policy or significantly affect the Policy (e.g. changes to the binding character) in advance to the Competent Supervisory Authority with a brief explanation of the reasons for the update and, via the Competent Supervisory Authority, to any other supervisory authorities concerned.

Autodesk Companies will communicate all other changes to this Policy (or will confirm that no changes have been made) (including changes in the list of Autodesk Companies) or which have occurred as a result of a change of European Data Protection Law, through any legislative, court or supervisory authority measure, to the Competent Supervisory Authority and via the Competent Supervisory Authority to any other supervisory authorities concerned at least at the annual update. Autodesk Companies will also provide a brief explanation to the Competent Supervisory Authority and via the Competent Supervisory Authorityto any other supervisory authorities concerned of the reasons for any notified changes to the Policy.

Autodesk will communicate all changes to this Policy, whether administrative or material in nature, to the Autodesk Companies bound by this Policy and, systematically, to data subjects who benefit from this Policy, via the Autodesk website when applicable.

The Director, EMEA Privacy Counsel & DPO responsible for the BCR will keep track of and record any updates to this Policy, and will maintain an up-to-date list of the changes made to this Policy, and the list of Autodesk Companies bound by this Policy. The necessary information will be available to and accessible by the data subjects and competent supervisory authorities upon request.

The Director, EMEA Privacy Counsel & DPO will also ensure that all new Autodesk Companies are effectively bound by and can deliver compliance with this Policy before a transfer of Personal Data to them takes place.

Version: 3.0

Date: 23.05.2025

APPENDIX 1

LIST OF AUTODESK COMPANIES IN EUROPE

Name of Entity	Address	Company Registration
Autodesk Ges.mbH	Schottengasse 1 1010 Wien Austria	FN 109096 k
Autodesk spol. s.r.o.	Karolinska 654/2 c/o SPACES Nile House, Prague, 186 00, Czech Republic	49358430
Autodesk ApS	Havnegade 39 1058 Copenhagen K Denmark	34711739
Autodesk France S.A.S.	2-22 Place des Vins de France Hall C – 3rd Floor Paris, France 75012	353 054 299
Autodesk GmbH	Balanstrasse 71a Munich, Germany 81541	HRB 96324
Autodesk Hungary Kft.	H-1136 Budapest, Tátra utca 12/B. 2nd floor 2 Budapest, Hungary	01-09-737549
Autodesk Ireland Operations Unlimited Company	1 Windmill Lane Dublin 2, Ireland D02 F206	614957
Autodesk S.r.l.	76-80 Buzesti Street 1st & 6th floor District 1, Bucharest 011017 Romania	J40/11723/2013
Autodesk B.V.	Poolweg 3, 7991, CP Dwingeloo The Netherlands	24257680
Autodesk Development B.V.	Evert van de beekstraat 1-104 1118 CL Schiphol, Netherlands	24261303
Autodesk Netherlands Holdings B.V.	Poolweg 3, 7991, CP Dwingeloo The Netherlands	66923468
Autodesk Sp. Z o.o.	Ul. Aleksandra Lubomirskiego 24 31-509 Kraków, Poland	KRS 287483
Autodesk, S.A.	calle Josep Plà 2, Torre B2, 6 planta, 08019 Barcelona Spain	A59125229
Autodesk AB	Fabrikstorget 1 412 50 Göteborg Sweden	556239-8189
Autodesk Development S.á.r.l.	Rue des Beaux-Arts 8 c/o LEAX Avocats Sàrl 2000 Neuchâtel, Switzerland	CHE-105.030.227

Name of Entity	Address	Company Registration
Autodesk SA	Worbstrassse 223, 3073 Gümligen Switzerland	CHE-100.274.963
Autodesk S.r.l.	Autodesk S.r.l c/o SPACES Piazza Gae Aulenti 1, Torre B, 5th Floor, 20124 Milano, MI, Italy	05112780159
Spacemaker AS	Edvard Storms gate 2 0166 Oslo, Norway	917 616 159
Spacemaker Sweden AB	Fabrikstorget 1 412 50 Göteborg Sweden	559211-9670
Autodesk Finland OY (previously Spacemaker AEC Software Oy)	Rajatorpantie 8 01600 Vantaa Finland	3131088-8
Autodesk d.o.o. (formerly UPCHAIN d.o.o.)	Autodesk at Regus Hoto Tower, Savska Cesta 32, 10000 Zagreb, Croatia	070098229 (EUID: HRSR.070098229)
ADSK Ireland Limited	1 Windmill Lane Dublin 2, Ireland D02 F206	461412
Autodesk Portugal, Unipessoal Lda	Avenida da Republica 50, 2nd Floor, Lisbon, 1050-196, Portugal	507418921
Autodesk Limited	Talbot Way Small Heath Business Park Birmingham B10 0HJ United Kingdom	01839239

LIST OF AUTODESK COMPANIES IN NON-EUROPEAN COUNTRIES

Name of Entity	Address	Company Registration
Autodesk Australia Pty. Ltd.	11 Talavera Road, Level 5, Building C, North Ryde, NSW Australia, 2113	006 741 340
Autodesk Canada Co.	1471 Lower Water Street, Suite 600 Halifax, Nova Scotia B3J 0J2 Canada	1179451951
Autodesk Colombia, S.A.S.	Carrera 11 No. 79-35 Piso 9, Bogota, Colombia, 110221	02625259
Autodesk de Costa Rica, S.R.L.	San Jose, Santa Ana Cantón, Pozos district, Forum Uno Business Center, Building C, Office Uno C Uno, 12891-1000, Costa Rica	3-102-802054
Autodesk Israel Ltd.	16th Floor, 22 Rothschild Boulevard, Tel Aviv, 6688218, Israel	513996140
Autodesk do Brasil Ltda.	No. 65 Rua James Joule, Rm. 41 4th Floor, Edificio Torre Sul Sao Paulo 04576-080 Brazil	CNPJ 00.015.972/0001-50
Autodesk India Private Limited	Unit A-4 Divyashree Chambers ‘A‘ Wing, Bengaluru 560 025 India	CIN No.: U72200KA1998PTC024308
Autodesk de Mexico, S.A. de C.V.	405 Paseo de Palmas, Piso 8 Mexico City 11000 Mexico D.F.	AME981118611
Autodesk Korea Limited	517 Yeongdong-daero, 17F ASEM Tower, Gangam-gu, Seoul 06164 Republic of South Korea	Company (Corporate) Registration No.: 110111-0890966 Business Registration No.: 220-81-03385 (Tax ID)
Autodesk Ltd. Japan	Toranomon Hills Mori Tower 8F, 23-1 Toranomon 1-chrome, Minato-ku, Tokyo, 105-6308, Japan	0100-01-074615
Autodesk Asia Pte. Ltd.	3 Fusionopolis Way #10-21 Symbiosis 138633 Singapore	199206210K
Autodesk Yazilim Hizmetleri Ticaret Limited Sirketi	Büyükdere Cad. No: 127 Astoria A Kule Kat:9 Esentepe Şişli, Istanbul Turkey	629969
Autodesk Americas LLC	111 McInnis Parkway San Rafael, California 94903 USA	6146172
Autodesk Global, Inc.	111 McInnis Parkway San Rafael, California 94903 USA	6181190
Autodesk, Inc.	111 McInnis Parkway San Rafael, California 94903 USA	2401504
Autodesk Limited (Saudi Arabia)	P.O box 69648 - Riyadh 11557 Saudi Arabia	1010298315
Autodesk Inc., Jordan PSC	King Hussein Business Park Building 6, 4th floor Amman, Jordan PO Box 11181	1329

APPENDIX 2

PROCESSING SCHEDULE

Categories of data subjects	Categories of Personal Data	Purposes of processing	Transfers to Non-European Countries
Customers	**Identifiers**: name, telephone number, physical and/or e-mail addresses, account username, and account password, telephone details, date of birth, facial templates and eyes movement **Professional information**: occupation, industry, professional licenses, work experience and employment history and other qualifications **Commercial information**: details of subscription plans, offerings purchased, used and/or records about interest in Autodesk offerings, events attended and participation in activities **Financial information**: payment information provided when making a purchase of or through an offering **Geolocation information** **Education information**: educational background **Visual, audio and electronic information**: picture or signature, records of interactions and activity engagement, such as correspondence, details of complaints and their resolutions, service records, preferences (including preferred tools, experience, language, and the frequency at which customers wish to receive marketing communications), unique user and device identifiers; operating system; type of device used; product ID; license information; browser information; IP addresses; information about which applications, activities and offerings are used and how they are used, and for how long; posts, discussions, and other types of engagement with Autodesk, including on blogs, discussion forums, or chat rooms; the use of any hyperlinks or downloadable content available through the offerings; information about the use of buttons, tools or content linked to social media services; error data; ; personal data collected through	**Accounts and records**: maintaining customer records and accounts including as required for internal accounting purposes and for preparing statutory filings, audits and financial reviews **Administration of entitlements and membership records**: maintaining records of and managing entitlements such as licenses and subscriptions; providing access to websites and applications; providing services, support or information; distributing application service packs; providing notices about upcoming events like an account or subscription expiration date **Advertising and marketing**: sending communications with information about products and services and special offers or promotions as permitted by local law; sending communications with information about third party products and services and special offers or promotions as permitted by local law; sending questionnaires and surveys; developing customer-tailored marketing communications; conducting public relations activities; running events **Business operations**: delivering goods and rendering services; invoicing, collecting and processing payments; logging customer contact information; providing customer service; determining whether to accept customers; reviewing and forecasting customer activity; managing staff performance and customer interaction; maintaining service levels; addressing customer complaints and enquiries; managing mergers, acquisitions, and re-organizations or disposals **Education and training**: managing enrolments; delivering training classes and online trainings; managing and administering exams and assessments; maintaining records of training and awarded certifications.	Australia Brazil Canada Colombia Costa Rica Israel India Japan Jordan Mexico Saudi Arabia Singapore South Korea Turkey USA

Categories of data subjects	Categories of Personal Data	Purposes of processing	Transfers to Non-European Countries
	the use of cookies and inferences drawn from any of the personal and offering usage information available to Autodesk, such as regarding usage information and preferences, behaviours and other attributes	**Protection of rights**: reducing software piracy and fraud; ensuring that applications and websites are used in compliance with applicable terms and the law; protecting customers and end users **Product development and improvement**: measuring and better understanding how websites and applications are used in order to improve these; tailoring overall customer experience with use of websites and applications	
Workers	**Identifiers**: name, date of birth, address, country of residence, phone number, email address or account password, picture **Professional information**: current and former roles, industry, professional licenses, work experience and employment history, and other qualifications **Protected characteristics**: sex, race, gender, religious, ethnicity, nationality, medical condition, age, and military or veteran status **Medical or health insurance information**: insurance policy number and claims information **Financial account information**: banking details for providing payroll, reimbursing expenses, or administering other benefit **Identifiers of beneficiaries**: name, date of birth, address, country of residence, phone number, and other personal information necessary to administer benefits to beneficiaries, educational backgrounds and continuing education information	**Managing workforce**: managing work activities and personnel generally, including appraisals, promotions and succession planning, administering salary and payments administration and reviews, wages and other awards such as stock options, stock grants and bonuses, health care, pensions and savings plans, training, leave, promotions, transfers, secondments, honouring other contractual benefits, loans, performing workforce analysis and planning, performing background checks, managing disciplinary matters and terminations, making business travel arrangements **Communication and emergencies**: facilitating communication with data subjects, providing references, ensuring business continuity, protecting the health and safety of employees and others, safeguarding it infrastructure, office equipment and other property, facilitating communication in an emergency **Business operations**: managing business operations generally, including operating and managing the it and communications systems, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to manufacturing and other business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, and re-organizations or disposals	Australia Brazil Canada Colombia Costa Rica Israel India Japan Jordan Mexico Saudi Arabia Singapore South Korea Turkey

Categories of data subjects	Categories of Personal Data	Purposes of processing	Transfers to Non-European Countries
		Compliance: complying with legal and other requirements, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, compliance with legal obligations and internal policies relating to diversity and anti-discrimination, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim and complying with internal policies and procedures **Monitoring**: monitoring compliance with internal policies, including the policies with regard to telephone, email, internet and other company resources and the code of business conduct and other monitoring activities as permitted by local law.	USA
Suppliers	**Identifiers**: name, date of birth, professional address, country of residence, phone number, email address or account password, picture **Professional information**: current and former roles, industry, professional licenses, work experience and employment history, and other qualifications	**Accounts and records**: maintaining supplier records and accounts including as required for internal accounting purposes and for preparing statutory filings, audits and financial reviews **Administration of entitlements and membership records**: including maintaining records of and managing entitlements such as licenses and subscriptions; providing access to websites and applications; providing services, support or information; distributing application service packs; providing notices about upcoming events like an account or subscription expiration date **Advertising and marketing**: including sending communications with information about products and services and special offers or promotions as permitted by local law; sending communications with information about third party products and services and special offers or promotions as permitted by local law; sending questionnaires and surveys; developing customer-tailored marketing communications; conducting public relations activities; running events **Business operations**: including invoicing, processing payments; logging supplier contact information; determining whether to engage	Australia Brazil Canada Colombia Costa Rica Israel India Japan Jordan Mexico Saudi Arabia

Categories of data subjects	Categories of Personal Data	Purposes of processing	Transfers to Non-European Countries
		suppliers; reviewing and forecasting supplier activity; managing staff performance and supplier interaction; addressing supplier complaints and enquiries; managing mergers, acquisitions, and re-organizations or disposals. **Protection of rights**: including reducing software piracy and fraud; ensuring that applications and websites are used in compliance with applicable terms and the law; protecting customers and end users	Singapore South Korea Turkey USA

APPENDIX 3

PROCESSING SCHEDULE

The Controller (as defined in Part 1 to this EU Processing Schedule ("**Part 1**")) wishes to appoint the Processor (also as defined in Part 1) to process certain Personal Data on its behalf in accordance with Rule 7B of the Policy. The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of Article 28 of the GDPR.

This Processing Schedule is to be read and interpreted in conjunction with the Policy.

Part 1: Processing Instructions

Description	Details
Name of controller Autodesk Company	[Please add details] (the "**Controller**")
Name of processor Autodesk Company	[Please add details] (the "**Processor**")
Subject-matter of the processing carried out by the Processor	[Please add details - describe services carried out by the Processor on the Controller's behalf in detail]
Nature of the processing carried out by the Processor	[Please add details, e.g. archiving, filming, recording]
Purpose of the processing carried out by the Processor	[Please add details, e.g. detecting unlawful entry]
Categories of Personal Data	• Names • Email addresses • Financial information • Etc.
Categories of data subjects	[Please add details]
Duration of processing carried out by the Processor	[Please add details]

Part 2: Processor's Obligations

2. The Processor shall:

2.1 act only on Controller's instructions when processing Personal Data including with regard to transfers of such Personal Data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller: (a) if it is legally required to process Personal Data otherwise than as instructed by the Controller before such processing occurs, unless the law requiring such processing prohibits the Processor from notifying the Controller, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, in which case it will notify the Controller as soon as that law permits it to do so; and (b) about any instruction from the Controller which, in the Processor's opinion, infringes European Data Protection Laws;

2.2 ensure that personnel/contractors authorised to process Personal Data described in Part 1 have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2.3 implement appropriate technical and organisational security measures in accordance with Rule 7 and set out in Schedule 1 of this Appendix to protect Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage;

2.4 taking into account the nature of the processing and insofar as this is possible, provide such co-operation and assistance by appropriate technical and organisational measures as the Controller reasonably considers to be necessary to enable the Controller to: (a) verify the Processor's compliance with Rules 7A and 7B of the Policy and this Processing Schedule; (b) carry out prior assessments of processing activities which are likely to result in a high risk to the rights and freedoms of data subjects and any related consultations with competent supervisory authorities; (c) fulfil its obligations in respect of any request by a data subjects to exercise their rights under the Policy, including by notifying the Controller without undue delay of any such request; and (d) investigate, mitigate and notify in accordance with Rule 7C of the Policy any personal data breach involving Personal Data, including by notifying the Controller without undue delay of any such personal data breach;

2.5 upon completion of the processing carried out by the Processor on the Controller's behalf and at the choice of the Controller, return all Personal Data processed by the Processor and all copies of such information, or securely destroy Personal Data and certify to Controller that it has done so within an agreed timescale and in an agreed secure manner unless the Processor is prevented from doing so by European or Member State law to which the Processor is subject, in which case the Processor shall inform the Controller as soon as possible and the Personal Data will be kept confidential and will not be actively processed for any purpose;

2.6 make available to the Controller all information necessary to demonstrate compliance with the obligations imposed upon the Processor under this Part 2 and, at the request of the Controller, submit its data processing facilities for audit of the processing activities covered by the Processing Schedule, which shall be carried out by the Controller or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Controller, where applicable, in agreement with the Competent Supervisory Authority; and

2.7 not subcontract any processing of Personal Data or otherwise disclose Personal Data to any Third-Party Entity except as authorised by the Controller in writing. Where sub-contracting is permitted the Processor will: (a) ensure that it has a written contract (the "**Processing Subcontract**") in place with the relevant subcontractor which imposes on the subcontractor the same obligations in respect of processing of Personal Data as are imposed on the Processor under Rule 7B of the Policy and this Part 2 to the Processing Schedule ("**Part 2**"); (b) ensure that there are sufficient guarantees in place to ensure the Processing Subcontract meets the requirements of Article 28 of the GDPR; (c) remain fully liable to the Controller for its obligations under Rule 7B of the Policy and this Part 2; and (d) ensure that Rule 8 of the Policy is complied with in the event that Personal Data is subject to a transfer or onward transfer to a sub-contractor.