PIX4D DATA PROCESSING AGREEMENT

Last modified: October 2021

This Data Processing Agreement and its Annexes (together the "**DPA**") is an agreement between You and Pix4D (Pix4D and You, each a "**Party**" and collectively, the "**Parties**"), which governs the processing of Customer Personal Data by Pix4D on Your behalf in connection with the End-User License Agreement (the "**EULA**"). This DPA is incorporated into, and forms an integral part of, the EULA.

Pix4D may update this DPA from time to time. The version available on our Website pix4d.com/legal is the current version.

All capitalized terms not defined in this DPA shall have the meanings set forth in the EULA. For the avoidance of doubt, all references to the EULA shall include this DPA (including its Exhibits and the EU SCC, as defined herein) and, to the extent applicable, Pix4D's General Terms and Conditions for Customers (the "**General Terms**") and any additional terms annexed thereto that may apply in connection with the Use of a specific Offering (the "**Additional Terms**").

TABLE OF CONTENT

WHEREAS

A. The Parties have entered into the EULA under the General Terms and the Additional Terms, as applicable.

B. In the context of the performance of the EULA, Pix4D and/or any of its Affiliates may have access to Customer Personal Data that is disclosed or otherwise made available via the Licensed Offerings under the EULA by You (or at Your direction) or by the Authorized Users.

C. Insofar as Pix4D will process such Customer Personal Data as Your processor, the Parties wish to ensure that such processing is compliant with applicable Data Protection Laws and agree on certain terms and conditions applicable to such processing as set forth in this DPA.

Now, therefore, the Parties agree as follows:

1. COMMENCEMENT AND DURATION

1.1. **Commencement.** This DPA will be effective and replace any previously applicable data processing agreement from the Terms Effective Date (as defined below).

1.2. **Duration.** Regardless of whether the EULA has terminated or expired, this DPA (including the P-C Clauses as applicable) will remain in effect until, and automatically expire when, Pix4D deletes all Customer Data as described in this DPA.

2. SCOPE OF DATA PROTECTION LAW

2.1. **Application of Data Protection Laws.** The Parties acknowledge that European Data Protection Law and, as the case may be, Non-European Data Protection, will apply to the processing of Customer Personal Data by Pix4D.

2.2. **Application of the Provisions of this DPA.** This DPA has been drafted specifically for the purposes of European Data Protection Law, but also takes into account, to the extent possible, the requirements of Non-European Data Protection, in particular the CCPA as set forth in Section 17, insofar as applicable. Unless otherwise specified in this DPA, the provisions of this DPA shall apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

3. PROCESSSING OF DATA AND PARTIES' ROLES

3.1. **Roles of the Parties.** To the extent European Data Protection Law applies, the Parties acknowledge and agree that with regard to the processing of Customer Personal Data in the context of the performance of the EULA relating to (i) the Authorized Users of the Licensed Offerings for whom You manage their Accounts (and, in particular, decide who has access to an Organization and to what extent) and/or (ii) any other third party appearing on the Content that is disclosed or otherwise made available to Pix4D via the Licensed Offerings under the EULA, You are the controller and Pix4D is the processor acting on Your behalf.

3.2. **Your Compliance and Instructions to Pix4D.** You represent and warrant that (i) You have complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of Your processing of Customer Personal Data, its delegation to Pix4D and any processing instructions You issue to Pix4D, and (ii) You have provided, and will continue to provide, all notices and have obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Pix4D to process Customer Personal Data for the purposes described in the EULA. You shall have sole responsibility for the accuracy, quality, and legality

of Customer Personal Data and the means by which You acquired Customer Personal Data. Without prejudice to the generality of the foregoing, You agree that You shall be responsible for complying with all laws (including Data Protection Laws) applicable to any Content created, sent or managed through the Licensed Offerings under the EULA. The EULA (including this DPA), together with the Use and the manner in which You have configured the Licensed Products in accordance with the EULA, constitute Your complete instructions to Pix4D in relation to the relevant processing of Customer Personal Data, so long as you may provide additional instructions during the Term that are consistent with the EULA, the nature, scope of functionality and lawful use of the Licensed Products, for which you shall bear the resulting costs, unless otherwise provided. Pix4D shall promptly notify You in writing, if it becomes aware or believes that any data processing instruction from You violates European Data Protection Law.

3.3. **Pix4D's Obligations.** Pix4D shall process Customer Personal Data under the EULA in accordance with applicable Data Protection Laws and your documented lawful instructions as described in Section 3.2.

3.4. **Details of the Processing.** The subject-matter of the processing of Customer Personal Data by Pix4D is the performance of the EULA. The types of personal data and categories of data subjects, the frequency of the transfer, the nature of the processing, the purpose of the transfer, the retention period of the data and the sub-processing details are further specified in Exhibit C (*Description of the Transfer*) to this DPA.

4. DATA SUBJECT REQUESTS

During the Term, if Pix4D receives a request from a data subject to exercise their data subjects rights under European Data Protection Law, in relation to Customer Personal Data, Pix4D will: (i) advise the data subject to subject their request to You, (ii) promptly notify You, and (iii) not otherwise respond to that data subject's request directly except as appropriate (for example, to direct the data subject to contact You) or legally required, without Your prior authorization. In addition, Pix4D shall, taking into account the nature of the processing, provide You reasonable additional assistance to the extent possible to enable You to comply with Your data protection obligations with respect to data subject rights under European Data Protection Law. Subject to prior agreement in text between the Parties, You agree to reimburse Pix4D for reasonable costs and expenses incurred by Pix4D in assisting You in accordance with this Section 4.

5. PIX4D PERSONNEL

Pix4D will ensure that any person who is authorized by Pix4D to process Customer Personal Data (including its staff, agents and sub-contractors) are under an appropriate obligation of confidentiality (whether contractual or statutory duty) and have in particular agreed not to disclose any Customer Personal Data to a third party nor to process such data for any other purpose than performing their tasks assigned to them by Pix4D in accordance with the EULA, it being further understood and agreed between the Parties that Pix4D shall remain responsible for the conduct of any of Pix4D personnel as for its own conduct.

6. SUB-PROCESSORS

6.1. **Authorized Sub-Processors.** You agree that Pix4D may engage sub-processors to process Customer Personal Data on Your behalf. The sub-processors currently engaged by Pix4D and authorized by You are (i) Pix4D's Affiliates and (ii) the third parties mentioned in Pix4D's list of sub-processors available at https://www.pix4d.com/legal. In addition, You hereby grant general written

authorization to Pix4D to appoint any other sub-processor in accordance with this Section 6 to perform specific processing activities on behalf of Pix4D.

6.2. **Opportunity to Object to Sub-Processor Changes.** Insofar as European Data Protection Law applies, Pix4D will inform You of any intended changes concerning the addition or replacement of its sub-processors and You will have an opportunity to object to such changes on objectively and reasonably justifiable grounds, within thirty (30) days after having being notified. If You timely object, You will have the opportunity to discuss Your concerns with Pix4D with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Pix4D will, at its sole discretion, either not appoint the new sub-processor, or permit you to terminate the EULA in accordance with the termination provisions of the EULA, without liability to Pix4D (but without prejudice to any fees incurred by You prior to the termination of the EULA).

6.3. **Requirement for Sub-Processor Engagement.** When engaging any sub-processor, Pix4D will ensure that the sub-processor is bound by obligations relating to confidentiality and data protection at least as strict as the provisions of the EULA (including this DPA) to the extent applicable to the nature of the processing activities provided by such sub-processor, it being understood and agreed that Pix4D will remain responsible for the conduct of any of its sub-processors as for its own conduct.

7. DATA SECURITY

Pix4D will implement and maintain appropriate technical and organizational measures that are designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including in particular and at least the measures set forth in Exhibit D (*Security Measures*) to this DPA (the "**Security Measures**"). The Security Measures include measures to encrypt Customer Personal Data, to help ensure ongoing confidentiality, integrity, availability and resilience of Pix4D's systems and services, to help restore timely access to Customer Personal Data following a Data Breach, and for regular testing of effectiveness. You are responsible for reviewing the information made available by Pix4D relating to data security and making an independent determination as to whether the Security Measures meets Your requirements and legal obligations under Data Protection Laws. You acknowledge that the Security Measures are subject to technical progress and development and that Pix4D may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Licensed Offerings provided to You.

8. DATA TRANSFERS TO NON-WHITELISTED COUNTRIES

8.1. **EU SCC.** The Parties agree that Pix4D may transfer Customer Personal Data to non-Whitelisted Countries for the purposes of, or in connection with, the performance of the EULA. Where Pix4D transfers Customer Personal Data subject to European Data Protection Law (back) to You, as the controller, located in a non-Whitelisted Country, the Parties agree to be bound by, and comply with, Module Four (Transfer Processor to Controller) of the EU SCC set forth in Exhibit A (*Module Four (Transfer Processor to Controller) of the EU SCC*) and compiled as follows (the "**P-C Clauses**"), including any applicable country-specific amendments set out in Exhibit B (*Country-Specific Amendments to the EU SCC*) to this DPA, with Pix4D being the "data exporter" and You being the "data importer":

(a) Clauses 1-6;

(b) Clause 7 shall not apply;

(c) Clause 8 with the provisions for "Module Four", including the introductory paragraph;

(d) Clause 10 with the provisions for "Module Four";

(e) Clause 11(a), but without the provisions of the "Option" of Clause 11(a);

(f) Clause 12 with the provisions for "Module Four"; to the extent not in conflict with the EU SCC, the liability between the data importer and the data exporter (but not towards the data subjects) shall be limited/excluded as per Section 14 of this DPA;

(g) Clauses 14-15 with the provisions for "Module Four", insofar as the data exporter combines personal data received from the data importer with personal data collected by the data exporter in a Whitelisted Country;

(h) Clause 16 with the provisions for "Module Four";

(i) Clause 17 with the provisions for "Module Four", with the law of France being the law agreed by the Parties for the purposes of Clause 17;

(j) Clause 18 with the provisions for "Module Four", with the courts of France being the law agreed by the Parties for the purposes of Clause 18.

8.2. **Annexes to the EU SCC.** The Annexes referred to by the P-C Clauses shall be formed as follows:

(a) Annex I.A shall consist of:

i. the information specified in the EULA and provided by You in the relevant Account Registration Form, with Pix4D being the "data exporter" acting as a "processor" and You being the "data importer" acting as a "controller";

ii. the contact information of the data exporter: Contact details for the data exporter are Pix4D SA, Route de Renens 24, 1008 Prilly, Switzerland. The data exporter's data protection team can be contacted at the following email address: data_protection@pix4d.com. The data exporter's data protection officer can be contacted as follows: Parrot Drones, c/o Mr Victor Vuillard, 174 Quai de Jemmapes, 75010 Paris, France;

iii. the contact information of the data importer: Contact details for the data importer, including the contact details of its data protection officer, are available to the data exporter in the relevant Account Registration Form (where such details have been provided by the data importer) and/or may be requested by the data exporter separately thereafter in individual cases;

iv. the activities as described in Exhibit C (*Description of the Transfer*) to this DPA;

v. the Parties agree that the execution of the EULA by the data importer and the data exporter shall constitute execution of these P-C Clauses by both Parties as of the Terms Effective Date.

(b) Annex I.B shall consist of the relevant section of Exhibit C (*Description of the Transfer*);

(c) Annex II shall consist of Exhibit B (*Technical and Organizational Measures*) to this DPA.

(d) Annex III, where applicable, shall consist of Pix4D's list of sub-processors available at https://www.pix4d.com/legal].

8.3. **Transfer Impact Assessment.** The Customer acknowledges that, to the best of

its knowledge, the planned transfers of personal data from Pix4D (back) to the Customer are permitted under applicable law, and the Parties have no reason to believe that the intended transfers are not authorized.

8.4. **Indemnification.** Each Party shall indemnify the other Party in case of claims of third parties due to a breach of its obligations under the P-C Clauses.

9. DATA BREACHES

Upon becoming aware of a Data Breach, Pix4D shall: (i) notify You without undue delay, and where feasible, in any event no later than forty-eight (48) hours from becoming aware of the Data Breach, (ii) provide timely information relating to the Data Breach as it becomes known or as is reasonably requested by You, and (iii) promptly take reasonable steps to contain and investigate any Data Breach. Pix4D's notification of, or response to, a Data Breach under this Section 9 shall not be construed as an acknowledgement by Pix4D of any fault or liability with respect to the Data Breach.

10. GOVERNMENT DATA ACCESS REQUESTS

When processing Customer Personal Data as Your processor under European Data Protection Law, Pix4D does not provide government agencies or authorities, including law enforcement, with access to or information about Pix4D Accounts, including Customer Data, unless it is required to by applicable law. The costs associated with responding to a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority, including law enforcement, for access to or information about a Pix4D Account, including Customer Data, belonging to You and/or the Authorized Users shall be borne by You.

11. REVIEW AND AUDIT OF COMPLIANCE

Pix4D shall provide You with all information reasonably necessary to demonstrate compliance with its obligations under this DPA and allow for and contribute to audits, including inspections, conducted by You or an independent auditor appointed by You to verify Pix4D's compliance with its obligations under this DPA, subject to customary confidentiality covenants. Additionally, Pix4D may provide You, free-of-charge, unsolicited or upon request, with any audit report prepared by Pix4D's auditor confirming Pix4D's compliance with this DPA.

12. IMPACT ASSESSMENTS AND CONSULTATIONS

To the extent required under applicable Data Protection Laws, Pix4D shall, taking into account the nature of the processing and the information available to Pix4D, provide all reasonably requested information regarding the Licensed Offerings to enable You to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Subject to prior agreement in text between the Parties, You will reimburse Pix4D for reasonable costs and expenses incurred by Pix4D in assisting You in accordance with this Section 12.

13. RETURN OR DELETION OF DATA

Upon termination or expiration of the EULA, Pix4D shall (at Your election) delete or return to You all Customer Personal Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Pix4D is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Pix4D shall securely isolate, protect from any further processing

and eventually delete in accordance with Pix4D's deletion policies, except to the extent required by applicable law.

14. LIMITATION OF LIABILITY

Except as provided for under the P-C Clauses set out in Sections 8.1 and 8.2 and except as expressly agreed in this DPA, Pix4D's liability, respectively Your liability, is excluded to the extent permitted under applicable law.

15. MISCELLANEOUS

15.1. **Amendments.** Any amendment to this DPA shall be made in writing and duly signed by authorized representative of the Parties.

15.2. **Conflicts.** In case of any conflict or inconsistency between this DPA and the EULA pertaining to the processing of Customer Personal Data, the provisions of the following documents (in order of precedence) shall prevail: (i) EU SCC, then (ii) this DPA, and then (iii) the EULA

15.3. **Severability**. If any provision of the DPA is held to be unenforceable for any reason, it shall be adjusted rather than voided, if possible, in order to achieve the legal and economic intent of the Parties to the fullest extent possible. In any event, all other provisions of the DPA shall remain valid and enforceable to the fullest extent possible.

15.4. **Notices.** For the purpose of all written communications between the Parties, any notice or other communication made in connection with the EULA shall be in writing (electronic form being deemed as satisfactory) and shall be e-mailed to the addresses below:

If to Pix4D: e-mail: legal@pix4d.com.

If to You: at the e-mail address registered in Your Account. In case of change, it is Your sole responsibility to inform Pix4D of Your new contact details. To this end, You can either contact Pix4D's support team through https://support.pix4d.com or update Your contact details on Your Account.

When and if used, the electronic communication system used by Pix4D will serve as sole proof for the content and the time of delivery and receipt of such electronic communications.

15.5. **Costs.** Each Party shall bear its own costs associated with its compliance with this DPA, including the P-C Clauses, as applicable.

16. GOVERNING LAW – DISPUTE RESOLUTION

16.1. **Governing Law.** Irrespective of the governing law of the EULA, this DPA shall be exclusively governed by and construed in accordance with the substantive law of Switzerland, whereby (i) international conventions, including the United Nations Convention on Contracts for the International Sale of Goods of 11.04.1980 (CISG) and (ii) Swiss conflict of law rules are expressly excluded from application to this DPA.

16.2. **Jurisdiction and Venue.** Irrespective of the place of jurisdiction of the EULA, the ordinary courts of Lausanne, Switzerland, shall have exclusive jurisdiction with regard to any dispute arising between the Parties out of or in connection with this

DPA.

17. ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION

17.1. **Scope and Applicability.** This Section 17 of the DPA applies in addition to the terms of this DPA, insofar as Pix4D processes California Personal Information under the EULA subject to the CCPA. In the event of any conflict or ambiguity between this Section 17 and any other terms of this DPA, this Section 17 will take precedence, but only to the extent of this Section's applicability to Pix4D.

17.2. **Roles of the Parties.** When processing California Personal Information in accordance with Your instructions, the Parties acknowledge and agree that You are a Business and Pix4D is a Service Provider for the purposes of the CCPA.

17.3. **Responsibilities.** The Parties agree that Pix4D will process California Personal Information as a Service Provider strictly for the purpose of licensing the Licensed Offerings under the EULA (the "**Business Purpose**") or as otherwise permitted by the CCPA.

18. DEFINITIONS

Account Registration Form	means the form provided by Pix4D for the registration of Your Account.
Additional Terms	as per meaning in front page.
Authorized Users	means the persons who are permitted by You to use the Licensed Products in accordance with the EULA. For clarity, Authorized Users may include Your employees, Your affiliates and other third parties outside Your entity that have been duly authorized by Your account administrator to become members of an Organization, where You act as a controller of such other third parties.
Business	shall have the meaning given to it in the CCPA.
Business Purpose	as per meaning in Section 17.3.
California Personal Information	means Personal Data that is subject to the protection of the CCPA.
CCPA	means California Civil Code Sec. 1798.100 et seq., also know as the California Consumer Privacy Act of 2018.
CNIL	means the Commission Nationale de l'Informatique et des Libertés as per meaning in Section 8.2**Error! Reference source not found.**.
Consumer	shall have the meaning given to it in the CCPA.
Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Customer Data	means data provided by or on behalf of You or End Users via the Licensed Offerings and under the Account.

Customer Personal Data	means the personal data contained within the Customer Data, including any special categories of personal data.
Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by Pix4D, including, without limitation, any violation of Exhibit D (*Security Measures*).
Data Protection Laws	means all data protection laws and regulations applicable to Pix4D's or Your processing of Customer Personal Data under the EULA, including, as applicable, European Data Protection Law and Non-European Data Protection Law.
Data Subject	shall mean any identified or identifiable natural person to which personal data relates.
Data Subject Request	as per meaning in Section 4.
DPA	as per meaning in front page.
EEA	means the European Economic Area
EULA	as per meaning in front page.
EU SCC	means the standard contractual, as approved by the Decision of the European Commission of June 4, 2021 [C(2021)3972 final] on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and any amendments thereto.
European Data Protection Law	means, as applicable, (a) the GDPR and any local, provincial or national legislation implementing the GDPR, (b) the UK GDPR, and (c) the Swiss DPA, and, in each case, any new or revised version thereof that may become effective during the Term.
FDPIC	means the Swiss Federal Data Protection and Information Commissioner as per meaning in Section 8.2**Error! Reference source not found.**.
GDPR	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, any new or revised version thereof that may become effective during the Term.
General Terms	as per meaning in front page.
Non-European Data Protection Law	means data protection or privacy laws in force outside the EEA, the UK and Switzerland, including, without limitation, the CCPA.

Parties	as per meaning in front page.
P-C Clauses	means Module Four (Transfer Processor to Controller) of the EU SCC as compiled and set forth in Sections 8.1 and 8.2 of this DPA.
Pix4D, Us, Our	Pix4D SA, a Swiss joint-stock company (*société anonyme*), registered in Switzerland under number CHE-207.009.701, having its registered seat at Route de Renens 24, 1008 Prilly, Switzerland.
Security Measures	means the technical and organizational measures of security as described in Exhibit D (*Security Measures*).
Service Provider	shall have the meaning given to it in the CCPA.
Swiss DPA	shall mean the Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance on the Federal Data Protection Act of 14 June 1993, and, in each case, any new or revised version thereof that may become effective during the Term.
Term	means the period from the Terms Effective Date until the end of Pix4D's provision of the Licensed Offerings, including, if applicable, any period during which provision of the Licensed Offerings may be suspended and any post-termination period during which Pix4D may continue providing the Licensed Offerings or transitional purposes.
Terms Effective Data	means the date on which You accepted, or the Parties otherwise agreed to, this DPA.
UK GDPR	means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act, any new or revised version thereof that may become effective during the Term.
Whitelisted Countries	means: - *for Customer Personal Data subject to the GDPR:* the EEA or a country or territory that is the subject of an adequacy decision by the European Commission under Article 45(1) of the GDPR; - *for Customer Personal Data subject to the UK GDPR:* the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or - *for Customer Personal Data subject to the Swiss DPA:* Switzerland or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner or, as the case may be, (ii) is the subject

	of an adequacy decision by the Swiss Federal Council under the Swiss DPA.
You and Your	means the legal entity licensing the Licensed Offerings under the EULA for use by its Authorized Users.

The terms "personal data", "data subject", "processing", "controller" and "processor" as used in this DPA have the meanings given in the GPDR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

Attachments:
Exhibit A: Module Four (Transfer Processor to Controller) of the EU SCC
Exhibit B: Country-Specific Amendments to the EU SCC
Exhibit C: Description of the Transfer
Exhibit D: Security Measures

Exhibit A: Module Four (Transfer Processor to Controller) of the EU SCC

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 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

[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, 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 2021/915.

(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 8.1 (b) and Clause 8.3(b);

(iii) N/A

(iv) N/A

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18.

(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 – Optional

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 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data ([2]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter 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 includes whether the transfer and further processing 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.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([3]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

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.

[3] 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.

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

Clause 13

Supervision

N/A

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(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 ([4]);

(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.

[4] 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.

(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).

(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. 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 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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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.

(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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*)**APPENDIX**

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

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: _____

Address: _____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses: _____

Signature and date: _____

Role (controller/processor): _____

2.

_____

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.

Name: _____

Address: _____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses: _____

Signature and date: _____

Role (controller/processor): _____

2.

_____

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

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

Nature of the processing

Purpose(s) of the data transfer and further processing

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

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

Exhibit B: Country-Specific Amendments to the EU SCC

Switzerland

For the purposes of the Swiss DPA, where transfers of Customer Personal Data under the EULA are subject to the GDPR and the Swiss DPA, the P-C Clauses as applicable according to Sections 8.1 and 8.2 of this DPA shall apply with the following amendments (for the avoidance of doubt, these amendments shall not affect the P-C Clauses as applicable for the purposes of the GDPR):

- References to “Regulation (EU) 2016/679” or “that Regulation” are to be interpreted to as references to the Swiss DPA to the extent applicable.
- References to “Regulation (EU) 2018/1725” are removed.
- References to “Union”, “EU”, and “EU Member State” shall be interpreted to mean Switzerland.
- Clause 17 is replaced to state that “These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by the Swiss DPA.
- Clause 18 is replaced to state:

  "Any dispute arising from these Clauses relating to the Swiss DPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts".
- Until the entry into force of the revised Swiss DPA, the P-C Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the P-C Clauses as natural persons.

For the purposes of the Swiss DPA, where transfers of Customer Personal Data under the EULA are exclusively subject to the Swiss DPA, the P-C Clauses as applicable according to Sections 8.1 and 8.2 of this DPA shall apply with the following amendments:

- References to “Regulation (EU) 2016/679” or “that Regulation” are to be interpreted to as references to the Swiss DPA.
- References to “Regulation (EU) 2018/1725” are removed.
- References to “Union”, “EU”, and “EU Member State” shall be interpreted to mean Switzerland.
- Clause 17 is replaced to state that “These Clauses are governed by the laws of Switzerland”.
- Clause 18 is replaced to state:

  "Any dispute arising from these Clauses relating to the Swiss DPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts".

- Until the entry into force of the revised Swiss DPA, the P-C Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the P-C Clauses as natural persons.

Exhibit C: Description of the Transfer

Categories of data subjects whose personal data is transferred:

Data subjects include the individuals about whom data is provided to Pix4D via the Licensed Offerings by You (or at Your direction) or by Authorized Users, including third parties appearing on the Content.

Categories of personal data transferred:

Data relating to individuals provided to Pix4D via the Services by You (or at Your direction) or by Authorized Users, including personal data of third parties appearing on the Content.

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 parties do not anticipate the transfer of sensitive data.

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

Regular and ongoing.

Nature of the processing:

Pix4D will process Customer Personal Data for the purposes of providing the Licensed Offering for use by You and the Authorized Users in accordance with the EULA.

Purpose(s) of the data transfer and further processing:

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

The Term plus the period from the end of the Term until deletion of all Customer Data by Pix4D in accordance with the EULA and this DPA.

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

See Pix4D's list of sub-processors available at https://www.pix4d.com/legal.

Exhibit D: Security Measures

The following contains the description of the technical and organizational measures implemented by Pix4D (including any relevant certifications) to ensure an appropriate level of security (the "**Security Measures**"), taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of data subjects:

1. Measures of pseudonymisation and encryption of personal data
    a) Pseudonymisation is performed in such a way that no data may be matched to a specific data subject without additional information.
    b) Additional information for attributing personal data to a specific data subject is kept in separate and secure systems which are only accessible by a limited number of individuals.
    c) When encrypting personal data, algorithms and length of keys are kept proportionated to level of sensitivity of the data.
    d) Encryption keys are kept secure and only given to a limited number of individuals.
    e) Internal instruction ensures that anonymization/pseudonymisation is carried out where possible in the event of disclosure or even after the statutory deletion period has expired.
2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
    a) A security officer or a designated member of senior management is appointed to be responsible for the coordination and monitoring of information security rules and procedures.
    b) Data protection aspects are established as an integral part of corporate risk management.
    c) Emergency and contingency plans are maintained for the facilities in which information systems processing personal data are located.
    d) If required, a data protection impact assessment (DPIA) is carried out.
    e) Staff is trained and bound by confidentiality and data secrecy.
    f) Staff is informed about relevant security procedures and their respective roles.
    g) Staff is informed about possible consequences of breaching security rules and procedures.
    h) Work instructions on access control, communication security and operational security are provided to staff.
    i) Work instructions explicitly describe security measures, relevant procedures and responsibilities.
    j) All data protection regulations, instructions and guidelines are documented centrally and accessible to all employees.

k) Components critical to system operation are monitored at all times and protected by protection systems to the extent required to protect them against fire, water, humidity, shocks, heat, cold and unforeseen power outage.

l) Components critical to system operation can be replaced within the required time in the event of their collapse, for example, by backup components, RAID-systems or data mirroring.

m) Where necessary, separate partitions are used for operating systems and data.

3. 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

   a) A backup strategy is defined based on the quantity of data and its frequency of change.

   b) Backup strategy is designed to recover personal data to its last state prior to data loss or data destruction.

   c) Backup systems are physically separated from production systems.

   d) The same security measures are applied to the backup servers as to the production servers.

   e) Individuals entrusted with restoring data are specially trained for this task.

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

   a) TOMS effectiveness is tested at predefined intervals by the "data importer". The nature and frequency of these tests are defined according to the respective measure.

   b) Appropriate measures are defined and taken if tests show that TOMS are not or not sufficiently implemented or do not show the required effectiveness.

   c) New TOMS are introduced if the review of existing TOMS indicate that they are no longer sufficient (e.g., new threats).

   d) One or more individuals are designated to continuously monitor the effectiveness of TOMS and to coordinate testing and any measures to be taken.

5. Measures for user identification and authorisation

   a) Access to information systems is protected by industry-standard identification and authentication procedures.

   b) Data storage devices, workstations, notebooks, smartphones and tablets are encrypted with industry-standard encryption methods.

   c) User accounts and user permissions are managed by designated individuals (administrators).

   d) The restrictive, need-based authorisation concepts of database rights is managed by a minimum number of administrators.

e) Access to personal data is restricted to employees who have a legitimate need to access such personal data within the scope of their individual job function or role.

f) Data that has been collected for different purposes can be processed separately from other data.

g) System activities beyond authorised access are prevented.

h) Guidelines are developed and implemented on the following topics: "secure passwords", "deletion/destruction", "clean desk", "mobile device".

i) Any user accounts that permit authentication are personal and used by one person only.

j) Staff is instructed to disable administrative sessions when leaving premises or when workstations are otherwise left unattended.

k) User passwords consist of at least eight characters, including upper and lower case letters, digits and special characters.

l) Two-factor authentication is used to access critical systems.

m) File shredder and/or external file destruction meet DIN 66399 security standard.

6. Measures for the protection of data during transmission

a) Remote access takes place only over encrypted lines (VPN).

b) Electronic transfer of data and transmission of personal data is carried out with industry-standard encryption methods. For e-mails, at least line encryption (TLS) is used where supported.

c) Signature procedures are implemented where necessary.

d) Data is not transferred to unknown third parties.

7. Measures for the protection of data during storage

a) Access to specific data is restricted to those who need to Process that data. This is controlled via a user authorisation model.

b) Where relevant, different customer data is stored in different databases.

c) External storage media that contain sensitive personal data are encrypted and physically secured

d) Right to enter, change and delete data are assigned on the basis of an authorisation concept.

e) Right to erasure are granted restrictively.

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

a) Systems and services are protected against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access.

b) A burglar alarm system including 24/7 alarm is installed.

c) Exterior and partitioning interior doors are secured with magnetic and closing contacts.

d) Keys and key cards are allocated to individuals.

e) Entrance or reception is staffed at any time during working hours.

f) Buildings and entrances are under constant video surveillance.

g) Visitors are always accompanied by employees.

h) External personnel is carefully selected.

i) For systems that are housed, hosted and maintained by external service providers, corresponding measures to be implemented and maintained by these service providers are arranged.

9. Measures for ensuring event logging

a) Access authorisations and retrieval of data are monitored and logged.

b) Allocation of keys and key cards are logged.

c) Visitors' access is logged.

d) Entry, modification and deletion of data is logged.

e) Data restoration efforts are logged.

f) TOMS' effectiveness test results are logged.

g) Reporting structure test results are logged.

h) Security incidents and data breaches are logged. Records are maintained that include nature of the data breach, categories and approximate number of data subjects concerned, categories and approximate number of personal data records concerned, time period, consequences of the data breach, procedure for recovering data, measures taken to mitigate adverse effects, name(s) of the person(s) who reported the data breach and name(s) of the person(s) to whom the data breach was reported.

i) Logs allow traceability of individual users, not user groups.

10. Measures for ensuring system configuration, including default configuration

a) Technical measures are taken to enable data subjects to easily exercise their right to withdraw consent.

b) Data protection-friendly default settings are used in standard and individual software.

11. Measures for internal IT and IT security governance and management

a) Anti-virus software and a firewall are installed on servers and clients to help avoid malicious software gaining unauthorised access to systems.

b) An intrusion detection system is implemented.

c) A formalized procedure for handling security incidents is in place.

d) Remote access by external parties is monitored.

e) IT hardware and software are checked at predefined intervals to assess whether they need to be updated or replaced for security reasons.

12. Measures for certification/assurance of processes and products

a) The need for certifications for systems and products is regularly assessed.

b) Data security certifications (if any) and audits (including penetration tests, as the case may be) are regularly repeated.

13. Measures for ensuring data minimization

a) Personal data is only collected to the extent necessary to fulfil the intended purposes.

b) Personal data held is reviewed periodically and deleted if not used anymore and if no legal or contractual requirements prohibit the deletion of such personal data.

14. Measures for ensuring data quality

a) Where appropriate, data entry is subject to plausibility tests.

b) Where appropriate, users are presented with the opportunity to verify data entered.

15. Measures for ensuring limited data retention

a) Where appropriate and possible, retention periods are defined.

b) Automated archiving protocols are used for documents and data in productive systems, where possible and appropriate.

16. Measures for ensuring accountability

a) A formal process is defined for following up on security incidents and data breaches.

b) Control mechanisms relating to compliance with data protection principles are based on the requirements of applicable data protection laws.

c) Reporting structures are aligned with the organisation of the Group and the respective unit and allow for reactions within a reasonable and, where such exist, legal timeframe.

d) Reporting structures' effectiveness is tested at predefined intervals.

e) Appropriate measures are defined and taken if the tests show that reporting structures are not or not sufficiently implemented or do not have the required effectiveness.

17. Measures for allowing data portability and ensuring erasure

a) Responsibilities with regard to data portability are clearly defined.

b) Formalised processes for data portability requests from data are in place.

c) Data sets can be identified and separated by the selection functions of the employed system.

d) Data portability requests are sent to the correct units without delay and addressed promptly so that statutory deadlines are met in any case.

e) Appropriate measures are implemented to ensure the removal of personal data from Provider's systems upon termination of the Principal Agreement.

f) Individuals responsible for data portability are trained and competent in how to handle requests regarding data portability. In particular, it is clearly defined which information must be disclosed, transferred or deleted and which requests or parts thereof are not to be complied with.

g) Personal data is transmitted in structured, commonly used and machine readable formats using secure methods.