



Data Processing Agreement

Between **Plesk International GmbH, Vordergasse 59, 8200 Schaffhausen / Switzerland**, acting for itself and on behalf of all its worldwide affiliates of the Particle group of companies, namely Plesk GmbH (Germany), Plesk Technologies S.L.U. (Spain), Plesk RU L.L.C. (Russia), Plesk K.K. (Japan) and Plesk CA Software Ltd. (Canada) (collectively hereinafter referred to as (“Plesk” or the “Data Processor”)), and

Partner Company Name: (for Entrepreneurs: Full Name)	Schüle Maschinenbau
Street / Nr.: Böisinger Str. 5	ZIP Code: 72285
City: Pfalzgrafenweiler	Country: Deutschland
Data Privacy Officer Name: Peter Schüle	
Contact Email: kontakt@schuele-maschinenbau.de	
Company Phone: +4974451059	

(“Partner” or the “Data Controller”),
each a “Party”, collectively the “Parties” hereto.

Instructions: This Data Processing Agreement (the “Agreement”), including all exhibits hereto has been pre-signed on behalf of Plesk. To enter into this Agreement, Partner must

- **complete all required form fields throughout the document by providing Partner’s full legal entity name, address, contact- and signatory information;**
- **submit the completed and signed Agreement (incl. Exhibits) to Plesk via the associated DocuSign process.**

This Agreement specifies the Parties’ data protection obligations in regards to the Processing of data by the Data Processor on behalf of the Data Controller, as stipulated or established in the existing Plesk Partnership Agreement, an assigned Parallels Hosting Partner Program Agreement or any other contractual understanding between the Parties, which involves the processing of personal data on behalf of the Data Controller (collectively the “**Base Agreement**”). It applies to all activities performed in connection with the Base Agreement in the course of which the Data Processor, or a 3rd party acting on its behalf (the “Sub-Processor”), may come into contact with or process personal data belonging to the Data Controller or its’ customers on behalf of the Data Controller.

This Data Processing Agreement will come into force and effect on **the date of the last dated signature hereunder** (the “**Effective Date**”) and will be bound to the term of the Base Agreement, unless terminated by either Party giving the other at least 3 months prior written notice of its intention to terminate. This Agreement will terminate automatically at the termination or expiry of the Base Agreement. All Exhibits hereto place integral parts of this Data Processing Agreement upon signature hereof.

§1 Definitions

(1) “Personal Data”

Personal Data means any information relating to an identified or identifiable natural person (the “Data Subject”).

2) “Processing”

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) "Instruction"

Instruction means any written instruction, issued by the Data Controller to the Data Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, de-personalizing, blocking, deletion, making available). Instructions will initially be specified in the Base Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (individual instructions).

(4) "Data Controller"

Data 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.

(5) "Data Processor"

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

(6) "GDPR"

GDPR means the EU General Data Protection Regulation 2016/679.

(7) "EU Standard Contractual Clauses" or "EUSCC" means a set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA, as issued by the European Commission (Decision C (2021) 3972).

(8) This Agreement applies to the Processing of Personal Data by Plesk on behalf of Partner in the course of providing Services under the Base Agreement. For the purposes of this Data Processing Agreement:

Partner may in some cases be considered as a Data Processor for a third-party Data Controller, and Plesk may in such situations be a Sub-Processor to Process Personal Data on Partner's behalf. For simplification purposes, Plesk is hereinafter referred to as a Data Processor and Partner is hereinafter referred to as a Data Controller. Any notifications given by the third -party Data Controller to Partner will in such cases be conveyed to Plesk insofar as the notifications relate to the Services provided by Plesk. In addition, any instructions given by Partner to Plesk relating to the Processing of Personal Data should not in such cases contradict or conflict with the instructions given by the third-party Data Controller.

§ 2 Scope and Responsibility

(1) The Data Processor will process Personal Data on behalf of the Data Controller. Processing will include such actions as may be specified in the Base Agreement, any statement of work, Work Order or any other written statement signed by both Parties or provided in another written form, involving the Processing of Personal Data or the possibility of such.

Within the scope of the Base Agreement, either Party will be responsible for complying with the statutory requirements relating to data protection and applicable to its Processing of Personal Data pursuant to the Base Agreement and this Agreement.

(2) Based on this responsibility, the Data Controller will be entitled to require from the Data Processor the rectification, deletion, blocking and making available of Personal Data during and after the term of the Base Agreement.

(3) The regulations of this Agreement will equally apply if technical maintenance or services are performed on behalf of the Data Controller and access to Personal Data in such context cannot be excluded.

(4) Any Personal Data Processed by the Data Processor under this Agreement or the Base Agreement will remain the property of the Data Controller.

(5) Together with this Agreement, the Parties will enter into EU Standard Contractual Clauses in the official format as issued by the European Commission (Decision C(2010)593). The EUSCC are attached hereto as Exhibit 3 and made an integral part of this Agreement.

§ 3 Obligations of Processor

(1) The Data Processor will collect, process and use Personal Data only in compliance with and within the scope of the Data Controller's Instructions or as specified and agreed in the Base Agreement.

(2) Within the Data Processor's area of responsibility, the Data Processor will structure its internal corporate organization for compliance with the specific requirements of the protection of Personal Data, established by GDPR, local data protection laws or any other applicable privacy and data protection laws and regulations currently in effect (the "Data Protection Laws"). The Data Processor will take the appropriate technical and organizational measures to ensure a level of security appropriate to the risk to the Data Controller's Personal Data in accordance with the requirements of Article 32 GDPR. Such measures hereunder will include, but not be limited to:

- a) the pseudonymization and encryption of personal data where possible;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services (logical, physical access control, transfer control);
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (availability control);
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Data security measures referred to in this section above will be supported by the use of state-of-the-art encryption technology. An overview of the technical and organizational measures implemented by the Data Processor will be attached to this Agreement as an Exhibit.

(3) Upon the Data Controller's request, the Data Processor will provide all information concerning the protection of Personal Data within the Data Processor's organization in the sense of Article 32 of GDPR and will provide reasonable assistance to the Data Controller in order to allow it to comply with its obligations under the Data Protection Laws.

(4) The Data Processor will ensure that any personnel, entrusted with Processing the Data Controller's Personal Data have undertaken in writing to comply with the principle of data secrecy in accordance with Article 5(f) GDPR and have committed themselves to confidentiality. The undertaking to secrecy will continue after the termination of the above-entitled activities.

(5) The Data Processor will notify to the Data Controller the contact details of the Data Processor's data protection Officer (if appointed) or the responsible associate, respectively.

(6) The Data Processor will, without undue delay, inform the Data Controller in case of a Personal Data Breach (as defined under Article 4 (12) GDPR) and will investigate and provide the Data Controller with sufficient information related to the Personal Data Breach and will ensure reasonable cooperation in order to enable Data Controller to comply with any legal obligation to report the Personal Data Breach and to inform Data Subjects and the supervisory authority within the time frame provided in the Data Protection Laws.

(7) Where applicable, the Data Controller will retain title as to any carrier media provided to the Data Processor as well as any copies or reproductions thereof. The Data Processor will store such media safely and protect them against unauthorized access by third parties. The Data Processor will, upon the Data Controller's request, provide to the Data Controller all information on the Data Controller's Personal Data and information. The Data Processor will be obliged to securely delete any test and scrap material, based on an Instruction issued by the Data Controller on a case-by-case basis. Where the Data Controller so decides, the Data Processor will hand over such material to the Data Controller or store it on the Data Controller's behalf.

(8) The Data Processor will be obliged to self-audit and verify the fulfilment of the above-entitled obligations and will maintain an adequate documentation of such verification which will be provided to the Data Controller upon request.

(9) The Data Processor will inform the Data Controller without undue delay of any Personal Data Breach of Processing of Personal Data it becomes aware of.

§ 4 Obligations of Controller

(1) The Data Controller and Data Processor each will be responsible for conforming with such statutory data protection regulations as are applicable to them.

(2) The Data Controller and Processor will be responsible for fulfilling their duties to inform resulting from Article 33 GDPR.

(3) The Data Controller will, upon termination or expiration of the Base Agreement, and, by way of issuing an Instruction, stipulate, within a period of time set by the Data Controller, the measures to return Personal Data on carrier media or to delete stored Personal Data.

(4) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Base Agreement or arising out of Instructions outside the Base Agreement's scope shall be borne by the Data Controller.

(5) If applicable, the Data Controller will at all times make sure to have a sufficient legal basis for handing over his own customers' data to the Data Processor in the event, the processing activities of the Data Processor relate to customers' data. Such legal basis has to be set forth in writing between the Data Controller and his customer and must be provided to the Data Processor upon request.

§ 5 Enquiries by Data Subjects or Supervisory Authorities

The Data Processor will, without undue delay, inform the Data Controller in case of any request, claim or notice from a Data Subject or any third party and assist and cooperate with Data Controller in order ensure compliance with the Data Protection Laws. Where the Data Controller, based upon GDPR or other applicable data protection law, is obliged to provide information to an individual about the collection, Processing or use of its Personal Data, the Data Processor will assist the Data Controller in making this information available, provided that the Data Controller has instructed Processor in writing to do so.

§ 6 Audit Obligations

The Data Controller may, prior to the commencement of Processing, and in regular intervals thereafter, audit the technical and organizational measures taken by the Data Processor, and will document the resulting findings. For such purpose, the Data Controller will collect voluntary disclosures from the Data Processor.

The Data Controller will: (i) ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to Data Processor's and/or its Sub-Processors' businesses, and acknowledging that such information request, audit or inspection: (a) will not oblige Data Processor to provide or permit access to information concerning Data Processor's internal business information or relating to other recipients of services from the Data Processor; and (b) shall be subject to any reasonable policies, procedures or instructions of Data Processor or its Sub-Processors for the purposes of preserving security and confidentiality; and (ii) provide Data Processor at least 30 days' prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides Data Controller with less than 30 days' notice, in which case Data Controller shall provide Data Processor with as much notice as possible).

If any information request, audit or inspection relates to systems provided by or on the premises of Data Processor's Sub-Processors, the scope of such information request, audit and/or inspection will be as permitted under the relevant agreement in place between Data Processor and the Sub-Processor.

A maximum of one information request, audit and/or inspection may be requested by Data Controller in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing.

The Data Processor will cooperate with the Controller in the sense of Art. 28 III h GDPR in the facilitation of any audit or inspection or other work undertaken pursuant to Data Processor's obligations under this Agreement.

§ 7 Sub-Processors, Subcontractors

(1) The Data Controller generally agrees that the Data Processor may subcontract parts of its contractual obligations hereunder to the Data Processor's affiliated companies and/or third parties (Sub-Processors) within or outside the EEA. Sub-Processors will only act on the Data Processor's Instructions when Processing Personal Data and will abide by any applicable data protection laws in effect.

The Data Processor agrees and warrants to remain liable to the Data Controller for any acts or omissions of its Sub-Processors related to the subcontracted Processing by them under this Agreement.

(2) Where the Data Processor engages Sub-Processors, the Data Processor will be obliged to pass on the Data Processor's contractual obligations hereunder as required by the GDPR to such Sub-Processors and will restrict the Sub-Processor's access to data only to what is necessary to maintain the subcontracted services. Sentence 1 of this paragraph 2 will apply in particular, but will not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the Base Agreement. Furthermore, the Data Processor is responsible for setting-up and maintaining appropriate safeguards between it and the Sub-Processors as stipulated in Article 46 GDPR.

(3) The Plesk website <https://www.plesk.com/legal> lists all Sub-Processors that are currently authorized by Plesk to access or process data on behalf of the Data Processor, only for specific purposes.

Plesk will periodically update the applicable list of Sub-Processors on that website. The Data Controller may subscribe to the update service available on <https://www.plesk.com/legal> in order to remain informed about any changes to this list. Alternatively, the Data Controller hereby commits to periodically check such website for changes in the list of Plesk Sub-Processors and acknowledges that satisfies its needs in regards to Sub-Processor information by the Data Processor. If the Data Controller does not approve a newly added Sub-Processor, then without prejudice to any termination rights under the Base Agreement and subject to the applicable terms and conditions, either Party shall have the right to either terminate this Agreement, its Instruction to Process data in writing or reject a specific form of data Processing in writing towards the Data Processor in order to avoid processing by such new Sub-Processor.

§ 8 International Data Transfers

The Data Controller acknowledges that the Data Processor's Sub-Processors may maintain data processing operations in countries outside the EEA or in countries without an adequate level of data protection, if it is required for the fulfillment of the Data Controller's Instructions or the underlying agreement. In such case, the Data Processor warrants that such Processing outside the EEA is protected by appropriate safeguards as requested by article 46 of GDPR. Specifically, the Data Processor will only transfer of Personal Data to entities outside the EEA if such entities are bound by EU Standard Contractual Clauses adopted by the EU Commission, Binding Corporate Rules or such other appropriate safeguard to make sure that the foreign entity will have established an adequate level of data protection within its organization by taking the appropriate technical and organizational measures in accordance to GDPR and local data protection laws in effect.

§ 9 Duties to Inform

Where the Data Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties, public authority or government body, while being Processed, the Data Processor will inform the Data Controller without undue delay. The Data Processor will, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in the Data Controller's sole property and area of responsibility, that Personal Data is at the Data Controller's sole disposition, and that the Data Controller is the responsible body in the sense of the GDPR and if possible, the Data Processor will not disclose any Personal Data of Partner to the extent allowed by the applicable laws.

§10 Indemnity and Limitation of Liability

Unless expressly stipulated differently in this Agreement, the Base Agreement or the applicable law, the Data Processor is solely liable and responsible for its' gross negligence and willful misconduct. This limitation of liability also applies to its assigned agents and proxies. In cases of simple negligence, the Data Processor shall only be liable for typical and foreseeable damages, caused by a violation of a cardinal contractual obligation. In this case, however, the Data Processor's, its affiliates', officers', directors', employees', agents', service providers', suppliers' or licensors' liability for indirect damages, business interruption, loss of goodwill or for any type of incidental, special, exemplary, consequential or punitive loss or damages is excluded, regardless of whether such Party has been advised of the possibility of such damages.

Notwithstanding the foregoing, in the event the Data Controller forwards his own customers' data to the Data Processor for further processing under this Agreement, the Data Controller will indemnify and hold harmless the Data Processor against all claims made by third parties, cost (including legal costs) and fines relating to the legal basis of such data forwarding. In this respect, the Data Controller has the sole and exclusive responsibility of making sure to have a sufficient permission by the Data Subject or his customers and a legal basis to forward data to Plesk for processing. Plesk strictly disclaims all associated liability towards Data Subjects or Data Controller customers, respectively.

Notwithstanding anything to the contrary in this Agreement or the Base Agreement, the Data Processor's aggregate liability to the Data Controller or any 3rd party arising out of this Agreement or any data Processing services performed hereunder, shall in no event exceed to the limitations set forth in the Base Agreement. For the avoidance of doubt, this section shall not be construed as limiting the liability of either party with respect to claims brought by Data Subjects. The Data Controller and the Data Processor act as joint debtors in respect to such claims.

§11 General, Choice of Law

(1) No change of or amendment to this Agreement and all of its components, including any commitment issued by the Data Processor, will be valid and binding unless made in writing and signed by either Party and unless they make express reference to being a change or amendment to these regulations. The foregoing will also apply to the waiver of this mandatory written form.

(2) If any provision (or part thereof) of this Agreement is held invalid by a court with jurisdiction over the Parties, such provision (or part thereof) will be deemed to be restated to reflect as far as possible the Parties' original intentions in accordance with applicable law, and the remainder of the Agreement or provision will remain in full force and effect as if the Agreement had been entered into without the invalid provision (or part thereof).

(3) This Agreement is governed by the laws of Switzerland. The courts located in Zürich / Switzerland will have the exclusive jurisdiction over the parties in regards to this Agreement.

(4) Name of the Plesk Data Protection Officer: Kai Bollmann (privacy@plesk.com)

[Signature Page Follows]




Signature Date: 21. Februar 2022	
For the Data Processor	For the Data Controller
Plesk International GmbH	Schüle Maschinenbau
  Plesk International GmbH Vordergasse 59 8200 Schaffhausen / CH CHE-278.733.710	 DocuSigned by: Peter Schüle <small>Maschinenbau u. Maschinenbau Büdingen-Strasse 9 Tel. 07145/1029 Fax 8371 72285 Plätzgrabenweiler</small> 23DBA8B92A80412...
Signature	Signature
Name: Sascha Konzack, CFO	Name: Peter Schüle

Exhibit 1

A description of Personal Data elements and the purpose of their Processing by the Data Processor on behalf of the Data Controller. The description will state the extent, the nature and purpose of contemplated collection, Processing and use of data, the type of data, and the circle of data subjects.

- The Data Controller may store names and email addresses of certain of its key employees or end - customers in the Data Processor's closed licensing system for purposes of account creation or maintenance in order to gain access to use such system for the purpose of license creation and customer license management. Only authorized employees with validated separate access rights have access to such information in the course of the provision of licensing services to the Data Controller.
- In the event the Data Controller is a SaaS / Hosting customer of the Data Processor (e.g. for the product "Sitejet"), the Data Processor may be instructed by the Data Controller to store the names, email addresses, phone numbers and the IP of the Data Controller's customers, users and visitors of hosted websites for purposes of authentication, service provision as well as user behavior analysis.
- In the course of the provision of requested technical support services via remote login to the Data Controller's servers, the Data Processor may have the general ability to access end customer data stored on such servers, although the services performed do not involve any access or actual processing of such data by the Data Processor.
- The possibility that such data may contain personal data of EU customers cannot be entirely excluded.
- Processing of such data in accordance with data privacy laws is limited to possible visibility only, unless the nature of the requested services involve direct access and actual processing of such data by the Data Processor by the Data Controller's request.
In such cases, processing may involve copying, transferring and adding the data from the former system to a new system or any other professional services requested by the Data Controller. The data is only stored and/or transferred to the destination server(s) specified by the Data Controller in such cases and not retained to the Data Processor's systems, unless specifically requested by the Data Controller.
- Data Subjects may be Data Controller's end-customers or employees and the data may contain personal data like names, addresses, email addresses, IP addresses, contact information and other information stored on the supported servers by the Data Subjects.
- Access to such data is limited to the timeframe during which a Data Processor's support engineer is remotely logged into a Data Controller's server. For licensing data, the Processing of data is limited to the timeframe of the underlying licensing relationship.
- In cases of remote support services, no data is stored, transferred or in any other way processed by the Data Processor, unless the nature of the support issue requires a download of data to an external resource and/or to the Data Processor's test environment, in which case a specific instruction by the Data Controller is mandatorily required.
- Every Data Processor employee or subcontractor is bound by a comprehensive Plesk Data Protection Policy. Where access to data is required to be granted from outside the EEA, such access is protected by the appropriate safeguards and guarantees (e.g. by EU Standard Contractual Clauses), required under the applicable Data privacy laws like GDPR or local data protection laws.

Exhibit 2**List of technical and organizational measures taken by Plesk as the Data Processor****1. Organization of Information Security**

The Plesk group employs a group-wide Chief Information Officer, responsible for the entire IT system of all group entities. The CIO has sufficient authority to handle any operational and tactical level security initiatives, issues, as well as a group wide IT security framework.

Where required, the CIO appoints additional Security Managers in different departments, responsible for the day-to-day handling of operational security issues, as well as reporting.

2. Entry Control

Plesk maintains physical security standards designed to restrict unauthorized physical access to office resources. Plesk does not host any security critical server infrastructure for the provision of services which may involve the processing of personal data. Only limited access points exist into offices, which are controlled by access readers. Access is allowed only for authorized staff that have approved access. Visitors will only be granted access to premises for approved purposes and after being checked upon entry. Employees upon termination are removed from the access list and, if they have a badge, they must surrender it. Non-Plesk operations and security staff are registered upon entering the premises and are escorted when they are on the premises.

3. Access Control

Access to servers/tools which may involve the processing of or contain personal data is regulated by means of user IDs and passwords, including two factor authentication for each authorized person. Additionally, systems which may allow the processing of personal data are only accessible via a closed VPN system with access documentation and additional user access restriction. Any passwords have to meet special security requirements (e.g. minimum length, numbers and capital letters, regular password change) set for Plesk network. Access credentials to processing systems are withdrawn immediately upon cessation of processing privileges or upon termination of employment. All client stations are required to be locked when inactive (with automatic log-off) and mandatorily need to be protected by up-to-date anti-virus software. A group-wide firewall solution is protecting the internal systems against unauthorized access. Plesk will not access or in other wise process client personal data on supported server infrastructure, unless specifically requested to do so by the exporter and unless the nature of the support issue requires such processing in order to solve the reported issue.

4. Intervention Control

Specific security measures are in place for remote access to Plesk's internal systems from outside the logical firewall, including a Plesk approved remote access (VPN) solution. Firewalls are used to prevent access from external networks. External guest-only Wi-Fi in the Plesk offices is separated from internal network with a firewall with same restrictive security settings that are appropriate for separation from public internet. Internal network access reviews are in place. Access to client personal data is allowed only by authorized Plesk support representatives according to principles of segregation of duties. No access is granted, unless a business need is evident and approved.

5. Transfer Control

Transfer of data within Plesk's network takes place behind Plesk's firewall. Backup data intended for off - site storage is encrypted prior to transport. Client sensitive personal data is handled as Plesk Confidential Information. Client sensitive personal data is not allowed to be stored at workstations, mobile devices, or portable storage media without a valid business need to do so or without written approval by the data subject. All approved Plesk workstations, mobile devices, or portable storage media (such as a removable HDD, a USB storage device etc., have to be encrypted.

Plesk services support a variety of information delivery protocols for transmission of data over public networks such as HTTPS, SFTP, and FTPS, SSH etc. Security configuration and patch management activities are performed and reviewed.

6. Input Control

Where technically available, Plesk maintains logs of activities in systems, applications, and network infrastructure devices. According documentation includes data down to the specific user and not a user group. Data input, alteration and deletion is handled by role management and is logged in internal system. Deletion routines are implemented in consultation with the Data Protection Officer into any process involving the storage of personal data by the importer.

7. Order Control

Processing of data on behalf of the exporter is primarily given in case of remote support services. The provision of such services mandatorily requires signature of a separate Data Processing Agreement, defining the processing activities, the data processed as well as the terms of processing in accordance to the GDPR and other privacy laws. The provision of support adheres to the following principles:

- To trace different orders Plesk uses a ticket control system which shows at any time the status of the respective order from order entry until end of the order.
- Plesk uses GDPR-complaint ticketing system Zendesk (GDPR regulations: <https://www.zendesk.com/company/customers-partners/eu-data-protection/#gdpr-sub>). Appropriate guarantees have been put in place between Plesk and Zendesk in order to effectively safeguard any data transfer.
- The concept of data minimization and reduction has been implemented into the support process with the effect that the amount of personal data (if any), which is to be transferred to Plesk systems in order to solve the reported issue, is reduced to the absolute minimum.
- All Plesk employees are bound by a comprehensive internal Data Protection Policy and are trained on fundamental privacy principles on a revolving basis. Any data processing activity is jointly evaluated between the respective team, the Data Protection Officer and the legal team for compliance with privacy laws prior to processing.

8. Change Control

Modifications to operating system resources and application software are governed by Plesk's change management process and supervised by the IT Department, led by the group CIO. Changes to firewall rules are also governed by the change management process and are separately reviewed by the Plesk security staff before implementation. Plesk does not perform any modifications on customer systems without authorization.

9. Security Control

Internal and external vulnerability scanning is regularly conducted by authorized administrators as well as external specialists to help detect and resolve potential system security exposures. Anti-virus detection systems are in place throughout all Plesk servers, client devices and offices.

10. Separation Control

The architecture of the used IT system is designed to maintain logical separation of client data for different processing purposes, supporting user roles per system component in order to prevent an exchange of data across systems and access to data by unauthorized individuals. Due to the fact that in most cases, the processing activity by the importer is limited to the general possibility of access, no data is stored and requires separation in most cases. Wherever data is moved to exporter systems, access to such data is limited to the responsible support engineer and his defined team.

11. Security Policies

Plesk maintains privacy and security policies that are communicated to Plesk's employees. Plesk requires and conducts privacy and security education training to individuals worldwide who support Plesk customers and maintains a security team that is focused on information security, led by the CIO. Plesk security policies and

standards are reviewed and re-evaluated annually. Plesk security incidents are handled in accordance with a comprehensive incident response procedure.

Exhibit 3

2021 EUSCC (only applicable for non-EEA customers)

STANDARD CONTRACTUAL CLAUSES

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) 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

- (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), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least two weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.

- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) 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.
- (f) The Parties agree that if one Party is held liable under paragraph (e), 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.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (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

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 that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Switzerland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

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 be 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: **Schüle Maschinenbau**

Address: Böisinger Str. 5 72285
Pfalzgrafenweiler Deutschland

Contact person's name, position and contact details:

Peter Schüle owner kontakt@schuele-maschinenbau.de

Activities relevant to the data transferred under these Clauses: none

Signature and date:  21. Februar 2022
Role (controller/processor): Controller

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

1. Name: Plesk International GmbH

Address: Vordergasse 59, 8200 Schaffhausen / Switzerland

Contact person's name, position and contact details: Kai Bollmann, Data Protection Officer

Activities relevant to the data transferred under these Clauses: The provision of technical support services by Plesk and its group companies.

Signature  

Date:

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Possibility of access to controller employee and customer names, email addresses, server login data, IP addresses, data stored on supported server or hosted website (e.g. Sitejet product).

Categories of personal data transferred

General temporary access to data stored on supported server or hosted website. No sensitive data involved.

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

In cases of the provision of technical support services, the possibility of transfer / processing is limited to cases in which remote access is granted by the exporter to the importer in order to perform technical support on server administration software, licensed by the importer. Frequency is one-off, upon request.

In the event the exporter is a SaaS / hosting customer of the importer (e.g. Sitejet product), the frequency of the transfer is ongoing for the duration of the hosting subscription.

Nature of the processing

In the course of the provision of requested technical support services via remote login to the exporter's servers, the importer (and possible sub-processors) may have the general ability to access end customer data stored on such servers, although the services performed do not involve any access or actual processing of such data by the importer.

In the course of the provision of SaaS / hosting services (e.g. Sitejet product), the nature of processing is the storage of data of website owners (names, addresses) and website visitors (IP) on behalf of the exporter as part of the importer's website hosting offering on server infrastructure, controlled by the importer.

Purpose(s) of the data transfer and further processing

In cases of the provision of technical support, no specific purpose of transfer or processing is given, as transfer or processing are limited to a general possibility of access to data only. The services requiring such access do not involve a direct handling, storing, transferring or processing of such data.

In the course of the provision of SaaS / hosting services (e.g. Sitejet product), the purpose of data processing is the performance of a contract for SaaS / website hosting services to the exporter and / or the exporter's customers.

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

No data retaining in cases of technical support. The possibility of access to server data is limited to the timeframe during which access to the server is granted by the exporter.

Data collected for the provision of SaaS / hosting services (e.g. Sitejet product) to the exporter and/or the exporter's customers is retained until the underlying hosting subscription ends. Thereafter, data is deleted in accordance to the importer's data retention policy.

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

The importer uses its affiliated companies worldwide to deliver 24/7/364 support. These act as sub-processors and are bound by comprehensive privacy compliance requirements and contracts (DPAs / EUSCCs), comparable to the ones, contained in these EUSCC.

Further sub-processors are in place in order to provide the ordered services for as long as their involvement is required for this purpose. These additional sub-processors provide storage, hosting, communication and payment services to enable the importer to deliver the services to the exporter.

C.COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) / Schweiz

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

1. Organization of Information Security

The Plesk group employs a group-wide Chief Information Officer, responsible for the entire IT system of all group entities. The CIO has sufficient authority to handle any operational and tactical level security initiatives, issues, as well as a group wide IT security framework.

Where required, the CIO appoints additional Security Managers in different departments, responsible for the day-to-day handling of operational security issues, as well as reporting.

2. Entry Control

Plesk maintains physical security standards designed to restrict unauthorized physical access to office resources. Plesk does not host any security critical server infrastructure for the provision of services which may involve the processing of personal data. Only limited access points exist into offices, which are controlled by access readers. Access is allowed only for authorized staff that have approved access. Visitors will only be granted access to premises for approved purposes and after being checked upon entry. Employees upon termination are removed from the access list and, if they have a badge, they must surrender it. Non-Plesk operations and security staff are registered upon entering the premises and are escorted when they are on the premises.

3. Access Control

Access to servers/tools which may involve the processing of or contain personal data is regulated by means of user IDs and passwords, including two factor authentication for each authorized person. Additionally, systems which may allow the processing of personal data are only accessible via a closed VPN system with access documentation and additional user access restriction. Any passwords have to meet special security requirements (e.g. minimum length, numbers and capital letters, regular password change) set for Plesk network. Access credentials to processing systems are withdrawn immediately upon cessation of processing privileges or upon termination of employment. All client stations are required to be locked when inactive (with automatic log-off) and mandatorily need to be protected by up-to-date anti-virus software. A group-wide firewall solution is protecting the internal systems against unauthorized access. Plesk will not access or in other wise process client personal data on supported server infrastructure, unless specifically requested to do so by the exporter and unless the nature of the support issue requires such processing in order to solve the reported issue.

4. Intervention Control

Specific security measures are in place for remote access to Plesk's internal systems from outside the logical firewall, including a Plesk approved remote access (VPN) solution. Firewalls are used to prevent access from external networks. External guest-only Wi-Fi in the Plesk offices is separated from internal network with a firewall with same restrictive security settings that are appropriate for separation from public internet. Internal network access reviews are in place. Access to client personal data is allowed only by authorized Plesk support representatives according to principles of segregation of duties. No access is granted, unless a business need is evident and approved.

5. Transfer Control

Transfer of data within Plesk's network takes place behind Plesk's firewall. Backup data intended for off - site storage is encrypted prior to transport. Client sensitive personal data is handled as Plesk Confidential Information. Client sensitive personal data is not allowed to be stored at workstations, mobile devices, or portable storage media without a valid business need to do so or without written approval by the data subject. All approved Plesk workstations, mobile devices, or portable storage media (such as a removable HDD, a USB storage device etc., have to be encrypted.

Plesk services support a variety of information delivery protocols for transmission of data over public networks such as HTTPS, SFTP, and FTPS, SSH etc. Security configuration and patch management activities are performed and reviewed.

6. Input Control

Where technically available, Plesk maintains logs of activities in systems, applications, and network infrastructure devices. According documentation includes data down to the specific user and not a user group. Data input, alteration and deletion is handled by role management and is logged in internal system. Deletion routines are implemented in consultation with the Data Protection Officer into any process involving the storage of personal data by the importer.

7. Order Control

Processing of data on behalf of the exporter is primarily given in case of remote support services. The provision of such services mandatorily requires signature of a separate Data Processing Agreement, defining the processing activities, the data processed as well as the terms of processing in accordance to the GDPR and other privacy laws. The provision of support adheres to the following principles:

- To trace different orders Plesk uses a ticket control system which shows at any time the status of the respective order from order entry until end of the order.
- Plesk uses GDPR-complaint ticketing system Zendesk (GDPR regulations: <https://www.zendesk.com/company/customers-partners/eu-data-protection/#gdpr-sub>). Appropriate guarantees have been put in place between Plesk and Zendesk in order to effectively safeguard any data transfer.
- The concept of data minimization and reduction has been implemented into the support process with the effect that the amount of personal data (if any), which is to be transferred to Plesk systems in order to solve the reported issue, is reduced to the absolute minimum.
- All Plesk employees are bound by a comprehensive internal Data Protection Policy and are trained on fundamental privacy principles on a revolving basis. Any data processing activity is jointly evaluated between the respective team, the Data Protection Officer and the legal team for compliance with privacy laws prior to processing.

8. Change Control

Modifications to operating system resources and application software are governed by Plesk's change management process and supervised by the IT Department, led by the group CIO. Changes to firewall rules are also governed by the change management process and are separately reviewed by the Plesk security staff before implementation. Plesk does not perform any modifications on customer systems without authorization.

9. Security Control

Internal and external vulnerability scanning is regularly conducted by authorized administrators as well as external specialists to help detect and resolve potential system security exposures. Anti-virus detection systems are in place throughout all Plesk servers, client devices and offices.

10. Separation Control

The architecture of the used IT system is designed to maintain logical separation of client data for different processing purposes, supporting user roles per system component in order to prevent an exchange of data across systems and access to data by unauthorized individuals. Due to the fact that in most cases, the processing activity by the importer is limited to the general possibility of access, no data is stored and requires separation in most cases. Wherever data is moved to exporter systems, access to such data is limited to the responsible support engineer and his defined team.

11. Security Policies

Plesk maintains privacy and security policies that are communicated to Plesk's employees. Plesk requires and conducts privacy and security education training to individuals worldwide who support Plesk customers and maintains a security team that is focused on information security, led by the CIO. Plesk security policies and standards are reviewed and re-evaluated annually. Plesk security incidents are handled in accordance with a comprehensive incident response procedure.

2021 EUSCC Controller to Processor

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. all sub-processors listed on www.plesk.com/legal (automatic update subscription available)