EXHIBIT 9

WEBPROS INTERNATIONAL LLC (DBA.CPANEL) DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements and is made an integral part of the Partner NOC Agreement (the "**Agreement**") entered into between WebPros International LLC doing business as cPanel ("**cPanel**") and the "**Partner NOC**" as defined in the Agreement in relation to the transfer and processing of Covered Data in connection with the performance of the Agreement.

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"Adequate Jurisdiction" means the UK, European Economic Area ("EEA") and Switzerland or a country or territory deemed to provide adequate protection for the rights and freedoms of individuals, as set out in: (a) the Data Protection Act 2018 or regulations made by the UK Secretary of State under the Data Protection Act 2018; (b) a decision of the European Commission; and (c) a decision of the Federal Council as listed in Annex 1 of the Swiss Data Protection Ordinance.

"Applicable Data Protection Laws" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time, including (without limitation): the GDPR, Swiss Data Protection Laws and the US Data Protection Laws.

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq*., as amended, including its implementing regulations and the California Privacy Rights Act of 2020.

"Controller Purposes" means: (a) undertaking internal research and development to develop, test, improve and alter the functionality of cPanel’s products and services; (b) creating anonymised datasets for training or evaluation of cPanel’s products and services; and (c) administering Partner NOC's relationship with cPanel under the Agreement.

"Covered Data" means Personal Data that is: (a) provided by or on behalf of Partner NOC to cPanel in connection with the fulfilment of contractual obligations under the Agreement; or (b) obtained, developed, produced or otherwise Processed by cPanel, or its agents or subcontractors, for the purposes of fulfilling such obligations, in each case as further described in Schedule 1.

"Data Subject" means a natural person whose Personal Data is Processed.

"Deidentified Data" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"DPF" means the "DPF", "EU-US Data Privacy Framework", or (where applicable) "Swiss-US Data Privacy Framework" and the "UK Extension to the EU-US Data Privacy Framework", in each case as defined in the relevant US Adequacy Decision.

"DPF List" means the "Data Privacy Framework List" or "DPF List" as defined in the applicable US Adequacy Decision.

"DPF Principles" means the "EU-US Data Privacy Framework Principles" or "Principles" as defined in the applicable US Adequacy Decision.

"GDPR" means Regulation (EU) 2016/679 (the "EU GDPR") or, where applicable, the "UK GDPR", as defined in section 3 of the Data Protection Act 2018.

"Personal Data" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data", "personal information", "personally identifiable information", or similarly defined data or information under Applicable Data Protection Laws.

"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. "Process", "Processes" and "Processed" will be interpreted accordingly.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"Standard Contractual Clauses" or "SCCs" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"Sub-processor" means, with respect to any Processing performed by cPanel as a processor or service provider, an entity engaged by cPanel to Process Covered Data.

"Swiss Data Protection Laws" means the Swiss Federal Act Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force for time to time.

"US Adequacy Decisions" means: (a) the UK Data Protection (Adequacy) (United States of America) Regulations 2023; (b) Commission Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the EU-US Data Privacy Framework; and (c) any adequacy decision adopted by the Swiss government pursuant to the DPF.

"US Data Protection Laws" means all applicable federal and state laws rules, regulations, and governmental requirements relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States, including (without limitation): the CCPA, the Virginia Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 *et seq.*, the Colorado Privacy Act, Colorado Revised Statute Title 6

Article 1 Part 13 § 6-1-1301 *et seq*., the Utah Consumer Privacy Act, Utah Code § 13-6-101 *et seq.*, Connecticut Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring (as such law is chaptered and enrolled).

1.2 The terms "controller", "processor", "business" and "service provider" have the meanings given to them in the Applicable Data Protection Laws.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA is incorporated into and forms an integral part of the Agreement. This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Covered Data and is entered into by cPanel and PartnerNOC together with entering into the Agreement.

3. ROLE OF THE PARTIES

The Parties acknowledge and agree that:

(a) save as set out in paragraph 3(b), cPanel acts as a processor or service provider in Processing Covered Data and Partner NOC acts as a controller or business; and

(b) for the purposes of the GDPR, cPanel acts as a controller with respect to the Processing of Covered Data for the Controller Purposes.

4. DETAILS OF DATA PROCESSING

4.1 The details of the Processing of Personal Data under the Agreement and this DPA (including subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in Schedule 1 to this DPA.

4.2 cPanel shall comply with its obligations under and provide the same level of privacy protection as is required by Applicable Data Protection Laws. Other than in respect of its Processing of Controller Data for the Controller Purposes, cPanel will only Process Covered Data on behalf of and under the instructions of Partner NOC and in accordance with Applicable Data Protection Laws.

4.3 The Agreement and this DPA shall constitute Partner NOC's instructions for the Processing of Covered Data. Partner NOC may issue further written instructions in accordance with this DPA. Without limiting the foregoing, cPanel is prohibited from:

(a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;

(b) sharing Covered Data with any third party for cross-context behavioural advertising without Partner NOC’s express consent;

(c) retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws;

(d) retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and

(e) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that cPanel receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

4.4 cPanel will:

(a) provide Partner NOC with information to enable Partner NOC to conduct and document any data protection impact assessments and prior consultations with supervisory authorities required under Applicable Data Protection Laws; and

(b) promptly inform Partner NOC if, in its opinion, an instruction from Partner NOC infringes the Applicable Data Protection Laws.

5. COMPLIANCE

5.1 Partner NOC shall comply with its obligations as a controller, business or equivalent term under the Applicable Data Protection Laws in relation to the Processing of Covered Data.

5.2 The Parties agree that Partner NOC shall:

(a) provide such information to Data Subjects regarding the Processing of Covered Data by cPanel for Controller Purposes as required under Applicable Data Protection Laws;

(b) to the extent required for the lawful Processing of Covered Data by cPanel for Controller Purposes under Applicable Data Protection Laws obtain valid consents from Data Subjects for such Processing in the form required under Applicable Data Protection Laws; and

(c) notify cPanel promptly of any request received from a Data Subject to exercise their rights under Applicable Data Protection Laws in respect of Covered Data Processed by cPanel for Controller Purposes.

6. CONFIDENTIALITY AND DISCLOSURE

6.1 cPanel shall:

(a) limit access to Covered Data to personnel who have a business need to have access to such Covered Data; and

(b) ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data to which they have access.

7. SUB-PROCESSORS

7.1 cPanel may Process Covered Data at any place, where cPanel or its Sub-processors maintain facilities, subject to the remainder of this clause 7.

7.2 Partner NOC grants cPanel general authorisation to engage Sub-processors. This includes, but is not limited to those Sub-processors listed in Schedule 4, as amended in accordance with clause 7.4 (the "Authorised Sub-processors"), to Process Covered Data.

7.3 cPanel shall:

(a) enter into a written agreement with each Authorised Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than cPanel's obligations under this DPA; and

(b) remain liable for each Authorised Sub-processor’s compliance with the obligations under this DPA.

7.4 cPanel will provide Partner NOC with at least fourteen (14) days’ notice of any proposed changes to the Authorized Sub-processors. Partner NOC shall notify cPanel if it objects to the proposed change to the Authorised Sub-processors (including, where applicable, when exercising its right to object under clause 9(a) of the SCCs) by providing cPanel with written notice of the objection within seven (7) days after cPanel has provided notice to Partner NOC of such proposed change (an "Objection").

7.5 In the event Partner NOC submits an Objection, cPanel and Partner NOC shall work together in good faith to find a mutually acceptable resolution to address such Objection. If cPanel and Partner NOC are unable to reach a mutually acceptable resolution within a reasonable timeframe, which shall not exceed thirty (30) days, cPanel may terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to cPanel.

7.6 cPanel shall remain fully responsible to Partner NOC for the performance of the Authorised Sub-processor’s obligations under its contract with cPanel. cPanel shall notify Partner NOC of any failure by the Authorised Sub-processor to fulfil its obligations under that contract.

8. DATA SUBJECT RIGHTS REQUESTS

8.1 cPanel will notify Partner NOC without undue delay of any request received by cPanel or any Authorised Sub-processor from a Data Subject to assert their rights under Applicable Data Protection Laws in relation to Covered Data Processed by cPanel as a Processor (a "Data Subject Request").

8.2 Partner NOC will have sole discretion in responding to the Data Subject Request in respect of Covered Data, and cPanel shall not respond to the Data Subject Request, save that cPanel may advise the Data Subject that their request has been forwarded to Partner NOC.

8.3 cPanel will provide Partner NOC with reasonable assistance as necessary for Partner NOC to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests in respect of Covered Data.

9. SECURITY

9.1 cPanel will implement and maintain appropriate technical and organisational data protection and security measures designed to ensure security of Covered Data, including, without limitation, protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage of or to Covered Data.

9.2 When assessing the appropriate level of security, cPanel shall take into account the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

9.3 cPanel will implement and maintain as a minimum standard the measures set out in Schedule 2.

10. INFORMATION AND AUDITS

10.1 cPanel shall notify Partner NOC promptly if cPanel determines that it can no longer meet its obligations under Applicable Data Protection Laws.

10.2 Partner NOC may take reasonable and appropriate steps to:

(a) ensure that cPanel uses Covered Data in a manner consistent with Partner NOC's obligations under Applicable Data Protection Laws; and

(b) upon reasonable notice, stop and remediate unauthorized use of Covered Data.

10.3 Partner NOC may audit cPanel's compliance with this DPA in respect of Covered Data that cPanel Processes as processor. The Parties agree that all such audits will be conducted:

(a) not more than annually, unless more frequent audits are required by a supervisory authority with jurisdiction over the Processing of Covered Data or otherwise under Applicable Data Protection Laws;

(b) upon reasonable written notice to cPanel;

(c) only during cPanel's normal business hours; and

(d) in a manner that does not materially disrupt cPanel's business or operations.

10.4 With respect to any audits conducted in accordance with clause 10.3:

(a) Partner NOC may engage a third-party auditor to conduct the audit on its behalf, save that cPanel may reasonably object to the engagement of a third-party auditor if such third-party auditor is a competitor of cPanel; and

(b) cPanel shall not be required to facilitate any such audit unless and until the Parties have agreed in writing the scope and timing of such audit.

10.5 Partner NOC shall promptly notify cPanel of any non-compliance discovered during an audit.

10.6 The results of the audit shall be cPanel's confidential information.

10.7 cPanel shall provide to Partner NOC upon request, or may provide to Partner NOC in response to any audit request submitted by Partner NOC to cPanel, either of the following:

(a) data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company; or

(b) such other documentation reasonably evidencing the implementation of the technical and organisational data security measures in accordance with industry standards.

10.8 If an audit requested by Partner NOC is addressed in the documents or certification provided by cPanel in accordance with paragraph 10.7, and:

(a) the certification or documentation is dated within twelve (12) months of Partner NOC's audit request; and

(b) cPanel confirms that there are no known material changes in the controls audited,

Partner NOC agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

11. SECURITY INCIDENTS

11.1 cPanel shall notify Partner NOC in writing without undue delay after becoming aware of any Security Incident.

11.2 cPanel shall take reasonable steps to contain, investigate, and mitigate any Security Incident, and shall send Partner NOC timely information about the Security Incident, to the extent known to cPanel or as the information becomes available to cPanel, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation.

11.3 cPanel shall provide reasonable assistance with Partner NOC's investigation of any Security Incidents and any of Partner NOC's obligations in relation to the Security Incident under

Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

11.4 cPanel's notification of or response to a Security Incident under this paragraph 11 shall not be construed as an acknowledgement by cPanel of any fault or liability with respect to the Security Incident.

12. TERM

This DPA shall commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, the later of (a) cPanel's deletion of all Covered Data as described in this DPA; or (b) termination of cPanel's Processing of Covered Data for Controller Purposes.

13. INTERNATIONAL TRANSFERS

13.1 With respect to transfers of Covered Data from Partner NOC to cPanel that are subject to a US Adequacy Decision, cPanel shall not transfer Covered Data to a recipient outside the UK, EEA or Switzerland unless:

(a) the recipient is in an Adequate Jurisdiction; or

(b) cPanel, or such recipient, complies with the requirements of the DPF when making such transfer, including taking reasonable and appropriate steps to ensure that the recipient provides the same level of protection as the DPF Principles and notifies Partner NOC or cPanel (in the case of onward transfers) if it makes a determination that it can no longer meet this obligation; or

(c) the transfer is otherwise not prohibited under Chapter V of the GDPR.

13.2 The Standard Contractual Clauses shall, as further set out in Schedule 3, apply to transfers of Covered Data from Partner NOC to cPanel, and form part of this DPA, to the extent that cPanel is not listed or ceases to be listed as a participating organization in the applicable DPF List for the purposes of a US Adequacy Decision, or the relevant US Adequacy Decision is repealed, withdrawn or otherwise ceases to apply to transfers of Covered Data from Partner NOC (as data exporter) to cPanel (as data importer), and one of the following applies:

(a) the GDPR or Swiss Data Protection Law applies to Partner NOC's Processing of such Covered Data when making the transfer; or

(b) the Applicable Data Protection Laws that apply to the Partner NOC when making that transfer (the "Exporter Data Protection Laws") prohibit the transfer of Covered Data to cPanel under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Covered Data, and any one or more of the following applies:

(i) the relevant authority with jurisdiction over the Partner NOC's transfer of Covered Data under this DPA has not formally adopted standard data protection clauses or another transfer mechanism under the Exporter Data Protection Laws; or

(ii) entering into standard contractual clauses approved by the European Commission would reasonably satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(iii) established market practice in relation to transfers subject to the Exporter Data Protection Laws is to enter into standard contractual clauses approved by the European Commission to satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

13.3 The Parties agree that execution of the Agreement shall have the same effect as signing the SCCs.

14. DEIDENTIFIED DATA

If cPanel receives Deidentified Data from or on behalf of Partner NOC, cPanel shall:

(a) take reasonable measures to ensure the information cannot be associated with a Data Subject;

(b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information; and

(c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

15. GENERAL

15.1 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

15.2 The Parties agree that any limitations on either Party's liability under the Agreement shall not apply to any claims, losses or damages arising in respect of a breach of the SCCs.

15.3 The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

SCHEDULE 1
DETAILS OF PROCESSING

A. List of Parties

	Partner NOC	**cPanel**
Role	Data exporter (controller)	Data importer (controller / processor)
Contact persons	Contacts as set out in the underlying Agreement	
Activities relevant to the transfer	The performance of the Agreement	

B. Description of Processing

<table>
<tr><td><b>Categories of Data Subjects</b></td><td colspan="2">• Employees, agents or other individuals authorised by Partner NOC to receive the Services and use the Software pursuant to the terms of the Agreement ("Authorized Users")
• Partner NOC’s clients and customers who it has licenced to use the Software in accordance with the terms of the Agreement ("End Users")</td></tr>
<tr><td><b>Categories of Personal Data</b></td><td colspan="2">• Name, contact information (including email), role at Partner NOC;
• Contents of tickets raised, requests and communications sent to cPanel; and
• Usage data relating to the site for which the Software is deployed, including the device / browser used to connect to the site, IP address, user profile (including age, gender and interests), on-site activities and user interactions</td></tr>
<tr><td><b>Special categories of Personal Data</b></td><td colspan="2">None</td></tr>
<tr><td><b>Frequency of the transfer</b></td><td colspan="2">Continuous</td></tr>
<tr><td><b>Nature of the Processing</b></td><td colspan="2">Collection, storage, deletion, rectification, analysis and aggregation necessary for the performance of the Agreement</td></tr>
<tr><td rowspan="2"><b>Purposes of the data transfer and further Processing</b></td><td><b>Processor Purposes</b></td><td><b>Controller Purposes</b></td></tr>
<tr><td>The delivery of cPanel Software and Services, including:
• Providing the Partner NOC's users with cPanel Software and Services;</td><td>• Undertaking internal research and development to develop, test, improve and alter the functionality of cPanel’s products and services;
• Creating anonymised datasets for training or evaluation of cPanel’s products and services; and</td></tr>
</table>

	• Resolving queries and support requests submitted by the Partner NOC.	• Administering Partner NOC's relationship with cPanel under the Agreement
Retention period	For the duration of the Agreement, unless earlier deletion is requested by the Partner NOC.	For the duration of Processing in accordance with the Controller Purposes.
Subprocessors	As set out in Schedule 4	N/A

C. Competent Supervisory Authority

The competent supervisory authority is: The Texas Attorney General

SCHEDULE 2
TECHNICAL AND ORGANIZATIONAL MEASURES

Operational Security

cPanel maintains a breach response plan that is tested annually. Employee access to information containing personal data is limited in scope and by job functionality. This access limitation is imposed both by policy and by technical limitations on access throughout cPanel.

cPanel maintains dedicated information security teams. One team is responsible for the internal security of our network, the other is responsible for the security of the cPanel software products ("Products"). Our product development team includes employees who monitor our Products and software included in our Products for security issues and responsibly report issues upstream. Both the internal security team, and the product development security team, are responsible for identifying vulnerabilities and responding to security events.

Our security documentation, policies, and processes are frequently reviewed and updated to reflect changes to our processes made in response to newly identified threats. We incorporate "agile" processes into our security processes resulting in continuous updating and revisions necessary to meet ongoing threats. Our security documentation is based on the NIST Cyber Security Framework. This Framework allows us to identify, score, protect, detect, respond and recover from security events.

All staff are subject to locally permissible background checks. Our employees are bound by obligations of confidentiality and non-disclosure that are strictly enforced. Outgoing employees receive detailed debriefings on exit. Portable devices provided by cPanel are monitored. All employees receive security awareness and security training. Additional training is provided based on employee function. Security team members attend security conferences to get outside training each year.

Physical Security

We store data in U.S. based colocation facilities. Our colocation providers are required by contract to meet industry standard security mandates and provide us with notice of a breach. Access to our colocation area is physically and logically controlled.

Access to our facilities is controlled in two or more places. Access is recorded and subject to review. Our facilities are monitored internally and externally by closed circuit video that is archived. Visitors to non-public areas of our facilities are required to be accompanied by an employee at all times. Facilities are patrolled by an independent security company.

The security of our internal network is tested continually. Access to the network is controlled and permissioned. Access to our internal management platform is secured, access is controlled, permissioned and monitored. Remote access is controlled, permissioned and monitored.

Excess equipment is reviewed to determine if data is present. Following inspection, this equipment is disposed of in a manner that meets industry standards for rendering the equipment and residual unusable. Only equipment that did not contain proprietary information is reused.

Product Security

Security is considered at all stages of our Product design and engineering. We use a combination of regularly scheduled security tests of our Product and security review with each major version. We also sponsor a bug bounty program.

We follow a continuous integration methodology for our Product’s code. We consider security needs by undertaking code reviews as part of the code release process. All code is reviewed multiple times prior to being committed to the Product. New Product releases are deployed to a secure staging environment for testing before being deployed to production.

Employee access to the code underlying our Product is access restricted. Employees must undergo specific training related to Product code prior to gaining access. Employees without a specific job function requiring access to the code are prohibited from accessing the code. We maintain logical restrictions on such access, and monitor employee use and access.

cPanel uses strong encryption to secure the transmission of Personal Information across the Public Internet, provided that such a use is supported by the vendor. Use of encryption during transmission, and of the data at rest, is included in cPanel’s contracting process. Our Product facilitates use of encryption in transmission and at rest, to the extent the use of encryption is compatible with the function of the Product. We encrypt information containing personal data at rest when used internally, to the extent encryption is compatible with the use of that data internally.

When we access a customer’s data to provide technical support, this access is logged, and the internal use monitored. When cPanel accesses a customer’s live data, the customer provides express permission to such access and that access is authorized only as related to the customer inquiry and linked to that inquiry.

We use cookies for user authentication. We use session IDs to identify user connections.

SCHEDULE 3
STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

With respect to any transfers referred to in clause **Fehler! Verweisquelle konnte nicht gefunden werden.**, the Standard Contractual Clauses shall be completed as follows:

1.1 Module One (*controller to controller*) of the SCCs will apply with respect to cPanel's Processing of Covered Data for Controller Purposes; otherwise, Module Two (*controller to processor*) of the SCCs will apply to cPanel’s Processing of Covered Data.

1.2 Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

1.3 Option 2 of Clause 9(a) (*General written authorization*) shall apply, and the time period to be specified is determined in clause 7.4 of the DPA.

1.4 The option in Clause 11(a) of the Standard Contractual Clauses *(Independent dispute resolution body*) does not apply.

1.5 With regard to Clause 17 of the Standard Contractual Clauses (*Governing law*), the Parties agree that option 1 will apply and the governing law will be Irish law.

1.6 In Clause 18 of the Standard Contractual Clauses (*Choice of forum and jurisdiction*), the Parties submit themselves to the jurisdiction of the courts of Ireland.

1.7 For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.

1.8 For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organisational measures.

2. UK Addendum

2.1 This paragraph 2 (*UK Addendum*) shall apply to any transfer of Covered Data from Partner NOC (as data exporter) to cPanel (as data importer), to the extent that:

(a) the UK Data Protection Laws apply to Partner NOC when making that transfer; or

(b) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"Approved Addendum" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK

Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"UK Data Protection Laws" means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the "Addendum EU SCCs" shall refer to the SCCs as they are incorporated into this Agreement in accordance with clause **Fehler! Verweisquelle konnte nicht gefunden werden.** and this Schedule 3;

(b) Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

(c) the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

(d) for the purposes of Table 4 of the Approved Addendum, cPanel (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum; and

(e) Section 16 of the Approved Addendum does not apply.

3. Swiss addendum

3.1 This Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR.

3.2 **Interpretation of this Addendum**

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"Addendum" means this addendum to the Clauses;

"Clauses" means the Standard Contractual Clauses as incorporated into this DPA in accordance with clause **Fehler! Verweisquelle konnte nicht gefunden werden.** and as further specified in this Schedule 3; and

"FDPIC" means the Federal Data Protection and Information Commissioner.

(b) This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfils the Parties' obligation to provide appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter’s Processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

3.3 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws

To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.3(a)) the following amendments are made to the Clauses:

(a) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(b) Clause 6 Description of the transfer(s) is replaced with:

"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 those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer."

(c) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(d) References to Regulation (EU) 2018/1725 are removed.

(e) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(f) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(g) Clause 17 is replaced to state: "These Clauses are governed by the laws of Switzerland".

(h) Clause 18 is replaced to state: "Any dispute arising from these Clauses relating to Swiss Data Protection Laws will 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."

3.5 **Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws**

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by paragraph 3.3(c) of this Addendum:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum; and

(B) subject to the provisions of paragraph 2 of this Schedule 3 (UK Addendum), the supervisory authority identified in Schedule 1 shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(b) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses; and

4. Transfers under the laws of other jurisdictions

4.1 With respect to any transfers of Personal Data referred to in clause 13.2(b) (each a "Global Transfer"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

4.2 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the applicable data exporter to the data importer, to the extent the Exporter Data Protection Laws apply to that data exporter's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data Protection Laws.

4.3 The amendments referred to in clause paragraph 4.2 include (without limitation) the following:

(a) references to the "GDPR" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) reference to the "Union", "EU" and "EU Member State" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "Exporter Jurisdiction");

(c) the "competent supervisory authority" shall be the applicable supervisory in the Exporter Jurisdiction; and

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

4.4 Where, at any time during cPanel's Processing of Covered Data under this DPA, a transfer mechanism other than the SCCs is approved under the Exporter Data Protection Laws with respect to transfers of Covered Data by Partner NOC to cPanel, the Parties shall promptly enter into a supplementary agreement that:

(a) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(b) incorporates the details of Processing set out in Schedule 1;

(c) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

4.5 Where required under the Exporter Data Protection Laws, the relevant data exporter shall file a copy of the agreement entered into in accordance with paragraph 4.4 with the relevant national authority.

SCHEDULE 4
AUTHORISED SUB-PROCESSORS

Sub-processor	**Description**
Google Cloud (BigQuery, Looker, Looker Studio, Analytics, Tag Manager, Ads)	Data Warehousing, Reporting, Visualization, and Web Analytics Platform. Tag Distribution Platform. Advertising and Campaign Performance Platform.
Google Fonts	Web Fonts
Fontawesome	Web Fonts
Mixpanel	Analytics & Engagement platform
Reddit Tracking Pixel	Advertisement Campaign Tracking
X, formerly known as Twitter, “Twitter Tracking Pixel”	Advertisement Campaign Tracking
LinkedIN Tracking Pixel	Advertisement Campaign Tracking
Typeform	Online Surveying
AccessiBe	Web Accessibility Solution for ADA and WCAG compliance
BugHerd	Web-based Bug Tracking and Project Management
UserCentrics (CookieBot)	Consent Management and GDPR/CCPA compliance
Hubspot	Inbound Marketing, Sales, and Customer Service
Microsoft (Communication, Clarity, Bing Ads)	Mailing, Calendar, Contact Management, Analytics & Engagement platform. Advertisement campaign tracking.
ZenDesk (Livechat)	Customer Service, Messaging
Hotjar	Analytics, Engagement & Surveying Platform