Data Processing Addendum

V082225

This Data Processing Addendum ("DPA") supplements and forms part of the NEOGOV Services Agreement or other written or electronic agreement between NEOGOV and Customer for the purchase of online services from NEOGOV (hereinafter defined as "Services") (the "Services Agreement"). Any references to the Services Agreement will be construed as including this DPA. All capitalized terms not defined herein shall have the meaning given to them in the Services Agreement.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws and Regulations" means, to the extent applicable: (a) the UK Data Protection Act 2018 and UK General Data Protection Regulation 2021 ("UK GDPR"); (b) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or "GDPR"); (c) the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 et seq., including its effective amendments and regulations thereto ("California Consumer Privacy Act" or "CCPA"); (d) the Swiss Federal Act on the Protection of Data ("FAPD") and (e) any other legally-binding data protection laws, rules, regulations, or implementing legislation applicable to NEOGOV's processing of Customer Personal Data, in eachcase, to the extent applicable to NEOGOV's Processing of Personal Data under the Services Agreement.

"Data Subject" means, as applicable the identified or identifiable natural person to whom Personal Data relates as defined by Data Protection Laws and Regulations.

"NEOGOV Group" means NEOGOV and its Affiliates engaged in the Processing of Personal Data under the Services Agreement.

"Personal Data" means any information relating to an identified or identifiable Data Subject where such information is provided to Processor by or on behalf of Controller, and maintained on behalf of, Controller by Processor within its Services environment, and is the type of information protected as "personal data" under Data Protection Laws and Regulations.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the standard contractual clauses for Processors annexed to the European Commission's decision (EU) 2021/914 of June 4 2021, as may be amended, updated, superseded or replaced from time to time for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor directly contracted by NEOGOV or a member of the NEOGOV Group to help NEOGOV provide the Services under the Services Agreement.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. Processing of Personal Data. To the extent NEOGOV Processes Personal Data on behalf of Customerin connection with the Services Agreement, it shall do so in accordance with the requirements of the Data Protection Laws and Regulations directlyapplicable to NEOGOV in the provision of its Services under the Services Agreement. The parties agree thatwith regard to the Processing of Personal Data by NEOGOV on behalf of Customer, Customer is the Controller, NEOGOV is the Processor and that NEOGOV and/or members of the NEOGOV Group will engage Sub-processors.

3. Customer Responsibilities. When using the Services, Customer shall Process Personal Data in accordance with Data Protection Laws and Regulations, including maintaining lawful basis (e.g., consent) and rights to use and provide Personal Data, as part of Customer Data. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations and NEOGOV's Processing of Persona Data shall not cause NEOGOV to violate Data Protection Laws and Regulations. For avoidance of doubt, deidentified data is not considered Personal Data. Customer is solely responsible for the accuracy, quality, and legality of Personal Data. Customer will: (i) maintain a clear and conspicuous privacy policy that discloses the data collection and usage (including third party tracking technologies) resulting from the services and that complies with Data Protection Laws and Regulations, provided that the privacy policy will not need to expressly identify the services unless otherwise required by Data Protection Laws and Regulations; and (ii) honor all individual rights and opt-out requests as required by applicable Data Protection Laws and Regulations.

4. NEOGOV's Responsibilities. NEOGOV shall treat Customer's Personal Data in a confidential manner, and shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Services Agreement and applicable Order Form(s); (ii) Processing initiated by users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Services Agreement. NEOGOV shall not "Sell" Personal Data or "Share" Personal Data for purposes of "Cross-Context Behavioral Advertising" (as such terms are defined in the CCPA). NEOGOV shall not retain, use, or disclose Personal Data (i) for any purpose other than business purposes specified herein (including retaining, using or disclosing the Personal Data for a commercial purpose other than the business purpose specified herein) or as otherwise permitted by the CCPA or (ii) outside of the direct business relationship between Customer and NEOGOV. NEOGOV certifies that it understands the restrictions described in this Section 4 and will comply with them in accordance with the CCPA.

5. Data Protection Impact Assessments. If, pursuant to Data Protection Laws and Regulations, Customer is required to perform a data protection impact assessment (or prior consultation with a regulator having appropriate jurisdiction), upon Customer's request, NEOGOV shall provide such relevant written documentation as is made available by NEOGOV pursuant to this DPA and the Services Agreement. Any additional assistance, should the written documentation specified in this Section be deemed insufficient, shall be subject to written agreement between the parties.

6. Data Subject Requests. If NEOGOV receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making (a "Data Subject Request"), NEOGOV shall notify Customer or direct such Data Subject to Customer. NEOGOV shall assist Customer by appropriate technical and organizational measures, as is technically feasible and commercially reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulation.

7. Security. NEOGOV shall implement and maintain appropriate technical and organizational measures designed for protection of the security, confidentiality and integrity of Customer Data, taking into account the nature, scope, context, purpose of processing, and costs of implementation. NEOGOV regularly monitors compliance with these measures and will not materially decrease the overall security of the Services during a subscription term under the applicable Order Form and the Services Agreement.

8. Sub-Processors; Objection. Customer acknowledges that: (a) NEOGOV's Affiliates may be retained as Sub-processors; and (b) NEOGOV and its Affiliates may engage third-party Sub-processors in connection with theprovision and operation of the Services under the Services Agreement. Sub-processors used as of the date of this DPA are specified in Annex III of Schedule 1 attached to this DPA. Prior to engaging any third-party Sub-processors, NEOGOV or a NEOGOV Affiliate shall carry out appropriate due diligence on each Sub-processor and enter into a written agreement with each Sub-processor containing data protection obligations substantially similar to those in this Services Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor. NEOGOV shall provide notice of any new Sub-processor by posting an updated list of Sub-processors on its website. Such posting shall be deemed to constitute notice to Customer of the new Sub-processor. If Customer objects to a new Sub-processor, Customer may do so by notifying NEOGOV promptly in writing within ten (10) days after the posting of the updated list. Such notice shall explain the Customer's good faith, reasonablegrounds for the objection. In the event Customer objects to a new Sub-processor, NEOGOV will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If the parties are unable to resolve such objection or NEOGOV is otherwise unwilling to resolve or make available such change within a reasonable period of time, Customer may terminate the applicable Order Form(s) with respect to those

Services which cannot be provided by NEOGOV without the use of the objected-to new Sub-processor by providing written notice to NEOGOV.

9. Data Transfers.

   a) EU Data Transfers. Customer acknowledges and agrees that Personal Data may be transferred outside European Union countries to countries recognized by the European Commission as countries where there is an adequate level of protection as updated from time to time ("Authorized Location"). During the term of the Services Agreement, the parties shall comply with the terms and conditions of the Standard Contractual Clauses (Controller to Processor, a current copy is attached hereto as Schedule 1, and the Standard Contractual Clauses are fully incorporated into this DPA. In the event Customer agrees to a transfer of Personal Data outside an Authorized Location, such transfer shall be subject to the execution between the Parties of the EU Standard Contractual Clauses or any other alternative mean validated by GDPR.

   b) UK Data Transfers. In the event of a transfer of Personal Data outside of the UK that is not to an Authorized Location, the parties agree that the EU Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK International Data Transfer Agreement ("IDTA"), and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in this DPA.

   c) Swiss Data Transfers. In the event of a transfer of Personal Data outside of Switzerland that is not to an Authorized Location, the parties agree the EU Standard Contractual Clauses are to be understood as references to the Swiss FDAP insofar as the data transfers are subject exclusively to the Swiss FAPD and not to the GDPR. The term "member state" in the EU Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU Standard Contractual Clauses. Under Annex I(C) of the EU Standard Contractual Clauses (Competent supervisory authority): Where the transfer is subject exclusively to the Swiss FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and Where the transfer is subject to both the Swiss FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the Swiss FADP, and the supervisory authority is as set forth in the EU Standard Contractual Clauses insofar as the transfer is governed by the GDPR.

   d) Other Data Transfer Mechanism. For the avoidance of doubt, should the transfer mechanism specified in this Section 9 be deemed invalid by a regulator or court with applicable authority, the parties shall endeavor in good faith to negotiate an alternative mechanism (if available) to permit the continued transfer of Personal Data.

10. Data Export; Deletion. Upon written request, NEOGOV shall return Customer Data or direct Customer to self-service export, if available and subject to technical feasibility, and/or, to the extent allowed by Data Protection Laws and Regulations or legal obligation, to protect its rights, or copies held in its back up systems solely for disaster recovery systems, delete and make irretrievable Customer Data.

11. Incident Notice. NEOGOV maintains incident management policies and procedures, and shall notify Customer, without undue delay, of any breach of its security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data in connection with NEOGOV's provision of Services under the Services Agreement and of which NEOGOV becomes aware and which requires notification to be made to Customer, a Supervisory Authority and/or Data Subject under Data Protection Laws and Regulations (a "Breach Incident"). "Breach Incident(s)" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, and other network attacks on firewalls or networked systems. NEOGOV shall make reasonable efforts to identify the cause of such Breach Incident and take those steps as NEOGOV deems necessary and reasonable in order to remediate the cause of such a Breach Incident to the extent the remediation is within NEOGOV's reasonable control. Additionally, upon request, NEOGOV shall provide Customer with relevant information about the Breach Incident, as reasonably required to assist the Customer in ensuring Customer's compliance with its own obligations under Data Protection Laws and Regulations to notify any Supervisory Authority or Data Subject in the event of a Breach Incident. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users or any non-NEOGOV products or services.

12. Liability Limits. Each party's and all of its Affiliates' liability, in the aggregate, arising out of or related to this DPA and NEOGOV, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Services Agreement, and any reference to the liability of a party means the total liability of that party and all of its Affiliates under the Services Agreement and all DPAs together.

13. Legal Effect and Conflict. This DPA shall become legally binding between Customer and NEOGOV upon execution of the Services Agreement. Once effective, this DPA shall be incorporated into and form part of the Services Agreement or applicable Order Form. For matters not addressed under this DPA, the terms of the Services Agreement apply. In the event of a conflict between the terms of the Services Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will control.

14. List of Schedules:

Schedule 1: Standard Contractual Clauses

EUROPEAN COMMISSION

Brussels, 4.6.2021

C(2021) 3972 final ANNEX

ANNEX

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)[1] for the transfer of personal data to a third country.
b. The Parties:
    i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
    ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
    iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);
    iv. Clause 12 - Module Two: Clause 12(a), (d) and (f);

v. Clause 13;
vi. Clause 15.1(c), (d) and (e);
vii. Clause 16(e);
viii. Clause 18 - Module Two: 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 - Optional
Docking clause

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE TWO: Transfer controller to processor

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 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[4] (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

MODULE TWO: Transfer controller to processor

a. OPTION 2: GENERAL WRITTEN AUTHORISATION 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 10 days 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.[8] 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

MODULE TWO: Transfer controller to processor

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.

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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 sub-processor) 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

MODULE TWO: Transfer controller to processor

a. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: 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

MODULE TWO: Transfer controller to processor

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[12];
    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). The data exporter shall forward the notification to the controller.
f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller.

g. 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 controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

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

MODULE TWO: Transfer controller to processor

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. The data exporter shall forward the notification to the controller.

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.). The data exporter shall forward the information to the controller.

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. The data exporter shall make the assessment available to the controller.

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    ii. the data importer is in substantial or persistent breach of these Clauses; or
    iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

- In these cases, it shall inform the competent supervisory authority and the controller 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

MODULE TWO: Transfer controller to processor

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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 Ireland (*specify Member State*).
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.

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

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

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

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

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the

purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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

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

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

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): The entity identified as “Customer” in the DPA or Services Agreement

Data importer(s): Governmentjobs.com, Inc. (D/B/A/ NEOGOV), parent company of PowerDMS, Inc., Cuehit, Inc., Ragnasoft LLC (D/B/A/ PlanIT Schedule), and Design PD, LLC (D/B/A Agency360) (collectively, “NEOGOV”)

1. Name: NEOGOV
   2120 Park Place, Suite 100, El Segundo, CA 90245

   Contact Anurag Ojha, CISO and contact details: Tel.: 310-426-6304 Fax: 310-426-6305
   privacy@governmentjobs.com

   Activities relevant to the data transferred under these Clauses: NEOGOV provides cloud-based human resource and public safety software services and support solutions which process Personal Data upon the written instruction of the data exporter in accordance with the terms of the Services Agreement and this DPA.
   Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, prospects, vendors, job applicants, employees, agents, advisors, freelancers, or contact persons of data exporter (who are natural persons), as well as employees or contact persons of all of the foregoing
- Any other users (who are natural persons) authorized by data exporter to use the Services

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data
- Driver’s license, social security number, other government identifiers
- Address
- Work and education history
- Age
- Signature

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

• Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life

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

Transfer is continuous

Nature of the processing

Collecting, storing, deleting, altering, transferring and other processing as set forth in the agreement between the data exporter and data importer or data importer's affiliate for the provision of data importer's cloud-based human resource and public safety software services and support solutions, and related support, maintenance, implementation and training services

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by data importer is in furtherance of servicing the Customer, as well as the performance and operation of the Services pursuant to the Services Agreement.

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

Duration of the processing shall correspond to the duration of the Services Agreement except where otherwise required by applicable law or legal obligation, or for NEOGOV to protect its rights or those of a third party.

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

When sub-processors are involved (see list provided), transfer is limited to transfer necessary for the performance of the agreement, and for its duration.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13, and where possible, select the Irish Data Protection Commission.

…

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

MODULE TWO: Transfer controller to processor

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

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of any Personal Data uploaded to the Services or otherwise maintained on behalf of data exporter (as Data Controller). Data importer reserves the right to update the security controls from time-to-time, provided that at no time shall data importer materially and to the adverse impact of data exporter, decrease the overall security of the Services during a subscription term.

Measures in place:

- Measures of pseudonymisation and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products

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

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

Sub-Processor	Use
Amazon Web Services	Compute, storage, email sending from in app
Google	Customer communications, analytics
Salesforce	Sales process, customer service, analytics
GuideCS	Implementation

Docebo	Implementation, training
Gainsight	Analytics
DataDog	Application health monitoring
AppDynamics	Application health monitoring
MailGun	Outbound email service
Twilio	Outbound email and text messaging
Azure Commercial Cloud	Computer and storage
Blue Jacket Technology, Inc.	Outsourced customer service and contracting support
LingaTech, Inc.	Outsourced customer service and contracting support
One360	Outsourced customer support
OpenAI OpCo, LLC	Generative AI capabilities, including but not limited to, content creation, summarization, and natural language processing
Amazon BedRock	Generative AI capabilities, including but not limited to, content creation, summarization, and natural language processing
Hubspot	Marketing functions
Oracle Eloqua	Marketing email campaigns