wordfly

# Data Processing Agreement

**General Data Protection Regulation Data Processing Addendum for Services Agreement**

**(European Economic Area, UK, & Switzerland)**

This Data Processing Addendum (“DPA”) is incorporated into, and is subject to the terms and conditions of, the Agreement between Pop, Inc. (“Pop”, “we” or “us”) and our clients who have contracted with Pop to access and use WordFly, including each of their authorized users (collectively, “Clients”, "users", or "you"). The parties agree that for the purposes of this Addendum, Pop is the Data Processor, and Client is the Data Controller and this Addendum governs Pop’s Processing of Personal Data, as all such capitalized terms are defined in Regulation (EU) 2016/679, referred to as the “General Data Protection Regulation” (“GDPR”). For Clients in the United Kingdom, references to GDPR shall be to the UK GDPR. This Addendum applies solely to the extent Personal Data relates to natural persons in the European Economic Area, the United Kingdom or Switzerland in connection with Pop’s provision of the services for Client as described in the Agreement (“Services”). Except as expressly stated otherwise, in the event of a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum will control. The Addendum will be effective on the last signature date set forth below. Unless otherwise indicated, all capitalized terms used but not defined in this Addendum have the meanings given to them in the GDPR.

1. **Applicable Law.** Client represents and warrants that it has collected Personal Data it provides to Pop in accordance with all applicable law, including the GDPR.
2. **Instructions from the Controller.** Notwithstanding anything in the Agreement to the contrary, Pop will only Process Personal Data on documented instructions from Client, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union, United Kingdom or Member State law to which Pop is subject. Pop will promptly inform Client if following Client instructions would result in a violation of applicable data protection law or where Pop must disclose Personal Data in response to a legal obligation (unless the legal obligation prohibits Pop from making such disclosure).
3. **Confidentiality.** Pop will restrict access to Personal Data to those authorized persons who need such information to provide the Services. Pop will ensure such authorized persons are obligated to maintain the confidentiality of any Personal Data.
4. **Security.** Pop will implement appropriate technical and organizational measures to ensure a level of security appropriate to the Personal Data provided by Client and Processed by Pop.
5. **Sub-processors.** Client agrees that Pop may engage Sub-processors to Process Personal Data in connection with providing the Services consistent with the Agreement. Pop will make a list of such Sub- processors

available to Client upon request, and thereafter will notify Client of any changes to such list. Client may reasonably object to Pop's use of a Sub-processor by notifying Pop promptly in writing within ten (10) business days after receipt of Pop's Sub-processor list or update thereto. Such notice will explain the reasonable grounds for the objection. In the event Client objects to a new Sub-processor, Pop will use commercially reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If Pop is unable to make available such change within thirty (30) days, either party may terminate without penalty the Agreement by providing written notice to the other party. Pop will refund Client any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination, without imposing a penalty for such termination on Client.

6. **Sub-processor Obligations.** Where Pop engages a Sub-processor for carrying out specific 1 Processing activities on behalf of Client, the same data protection obligations as set out in this Addendum will be imposed on that Sub-processor by way of a contract or other legal act under EU or United Kingdom or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the EU or United Kingdom data protection law (as appropriate). Where that Sub-processor fails to fulfill its data protection obligations, Pop will remain fully liable to the Client for the performance of that Sub-processor's obligations.

7. **Access Requests.** Pop has implemented and will maintain appropriate technical and organizational measures needed to enable Client to respond to requests from Data Subjects to access, correct, transmit, limit processing of, or delete any relevant Personal Data held by Pop.

8. **Recordkeeping.** Upon a request issued by a supervisory authority for records regarding Personal Data, Pop will cooperate to provide the supervisory authority with records related to Processing activities performed on Client's behalf, including information on the categories of Personal Data Processed and the purposes of the Processing, the use of service providers with respect to such Processing, any data disclosures or transfers to third parties and a general description of technical and organizational measures to protect the security of such data.

9. **Assistance.** Pop will assist Client: (1) to the extent reasonably necessary in connection with ensuring Client's compliance with Articles 32 to 36 of the GDPR taking into account the nature of Processing and the information available to Pop, and (2) with the fulfillment of Client's obligation to respond to requests for exercising a Data Subject's rights in Chapter III of the GDPR by appropriate technical and organisational measures, insofar as this is possible. Pop reserves the right to charge Client for its reasonable costs in collecting and preparing Personal Data for transfer and for any special arrangements for making the transfer.

10. **International Transfers.** Client authorizes Pop to transfer, store or Process Personal Data in the United States or any other country in which Pop or its Sub-processors maintain servers or other facilities. Client appoints Pop to perform any such transfer of Personal Data to any such country and to store and Process

Personal Data in order to provide the Services. Pop will conduct all such activity in compliance with the Agreement, this Addendum, applicable law and Client instructions.

**Data center locations.** Pop offices and servers are located in the USA. Client acknowledges that Pop may transfer and process Personal Data to and in the United States and anywhere else in the world where Pop, its Affiliates or its Sub-processors maintain data processing operations. Pop shall always ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

**European Data transfers.** To the extent that Pop is a recipient of Personal Data protected by EU or United Kingdom Data Protection Laws ("EU Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable EU Data Protection Law), the parties agree to the following:

- (a) SCCs: Pop agrees to abide by and process EU Data in compliance with the SCCs in the form set out in Annex C. For the purposes of the descriptions in the SCCs, Pop agrees that it is the "data importer" and Client is the "data exporter" (notwithstanding that Client may itself be an entity located outside Europe).
- (b) Privacy Shield: Although Pop does not rely on the EU-US Privacy Shield as a legal basis for transfers of Personal Data in light of the judgement of the Court of Justice of the EU in Case C-311/18, for as long as Pop is self-certified to the Privacy Shield: (i) Pop agrees to process EU Data in compliance with the Privacy Shield Principles and (ii) if Pop is unable to comply with this requirement, Pop shall inform Customer.
- (c) Alternative transfer mechanism. To the extent Pop adopts an alternative data export mechanism (including any new version of or successor to the SCCs or Privacy Shield) for the transfer of EU Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable EU or United Kingdom Data Protection Law and extends to the countries to which EU Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable EU Data Protection Law), Pop may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU Data, including the safeguards set forth below:

    1. Pop undertakes to adopt supplementary measures to protect the EU Data in accordance with the requirements of EU Data Protection Law, including by implementing appropriate technical and organizational safeguards to protect personal data against any interference

that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

2. In the event that Pop receives a legally binding request for access to the EU Data by a public authority, Pop will:

    1. promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless Pop is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If Pop is so prohibited:

        2.1.1 It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

        2.1.2 In the event that, despite having used its reasonable best efforts, Pop is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and/or the competent supervisory authority of the data exporter.

        2.1.3 Oppose any such request for access and contest its legal validity to the extent legally permitted under applicable law.

    2. not make any disclosures of the EU Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

    3. upon request from the data exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to EU Data.

11. **Deletion or Return.** At the choice of the Client, Pop will delete or return to Client all copies of Personal Data in its possession or control after the end of the provision of Services related to Processing, unless applicable law requires retention of the Personal Data. Pop will relay Client's instructions with respect to deleting or returning Personal Data to all Sub-processors.

12. **Breach Notification.** After becoming aware of a Personal Data Breach, Pop will notify Client without undue delay of: (a) the nature of the Personal Data Breach; (b) the number and categories of Data Subjects and data records affected; and (c) the name and contact details for the relevant contact person at Pop.

13. **Audits.** Upon request, Pop will make available to Client all information necessary, and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client, to demonstrate compliance with Article 28 of the GDPR. For clarity, such audits or inspections are limited to

Pop's Processing of Personal Data only, not any other aspect of Pop's business or information systems. If Client requires Pop to contribute to audits or inspections that are necessary to demonstrate compliance, Client will provide Pop with written notice at least 60 days in advance of such audit or inspection. Such written notice will specify the things, people, places or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered Pop's Confidential Information and, notwithstanding anything to the contrary in the Agreement, will remain Confidential Information in perpetuity or the longest time allowable by applicable law after termination of the Agreement. Such materials and derivative work product produced in response to Client's request will not be disclosed to anyone without the prior written permission of Pop unless such disclosure is required by applicable law. If disclosure is required by applicable law, Client will give Pop prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable law or order of a court or governmental agency. Client will make every effort to cooperate with Pop to schedule audits or inspections at times that are convenient to Pop. If, after reviewing Pop's response to Client's audit or inspection request, Client requires additional audits or inspections, Client acknowledges and agrees that it will be solely responsible for all costs incurred in relation to such additional audits or inspections.

**Annex A – Details of Data Processing**

(a) Controller (data exporter): Customer, being a WordFly Client that has engaged Pop to provide the Service under the Agreement.

(b) Processor (data importer): Pop, a Seattle, WA limited liability company, whose legal name is Pop.

(c) Subject matter: The subject matter of the data processing under this DPA is the Personal Data.

(d) Duration of processing: Pop will process Personal Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(e) Purpose of processing: Pop shall only process Personal Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement.

(f) Nature of the processing: Pop provides an email service, automation and marketing platform and other related services, as more particularly described in the Agreement.

(g) Categories of data subjects: (i) Clients and (ii) Client Contacts, each as defined in the Pop Privacy Policy.

(h) Types of Personal Data: Customer may upload, submit or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- Clients: Identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);
- Client Contacts: Identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address); personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

(i) Sensitive Data: Pop does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service.

(j) Processing Operations: Personal Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain and improve the Service provided to Customer pursuant to the Agreement; and/or
- Disclosures in accordance with the Agreement and/or as compelled by applicable law.

**Annex B – Security Measures**

The Security Measures applicable to the Service are described here: https://www.wordfly.com/security/

**Annex C - Standard Contractual Clauses**

Standard Contractual Clauses
2010 Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Pop a Seattle, WA. USA limited liability company whose legal name is Pop (hereinafter the "data importer") and Client (hereinafter the "data exporter") each a “party”; together “the parties”, HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

***Clause 1***

*Definitions*

For the purposes of the Clauses:

- 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- 'the data exporter' means the controller who transfers the personal data;
- 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- 'the Data Protection Law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

***Clause 2***

*Details of the transfer*

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

***Clause 3***

*Third-party beneficiary clause*

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

***Clause 4***

*Obligations of the data exporter*

The data exporter agrees and warrants:

- that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the Data Protection Law and the Clauses;
- that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- that after assessment of the requirements of the Data Protection Law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration,

unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- that it will ensure compliance with the security measures; that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- that it will ensure compliance with Clause 4(a) to (i).

***Clause 5***

*Obligations of the data importer*

The data importer agrees and warrants:

- to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

- that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- that it will promptly notify the data exporter about:
  - any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - any accidental or unauthorised access, and
  - any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

***Clause 6***

*Liability*

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

***Clause 7***

*Mediation and jurisdiction*

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    - to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    - to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

***Clause 8***

*Cooperation with supervisory authorities*

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the Data Protection Law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the Data Protection Law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

***Clause 9***

*Governing Law*

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

***Clause 10***

*Variation of the contract*

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

***Clause 11***

*Subprocessing*

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

***Clause 12***

*Obligation after the termination of personal data processing services*

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

Details of the transfer:

Please see the details set forth in Annex A to the Data Processing Addendum ("DPA") to which these Clauses are appended.

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Annex B – Security Measures

**APPENDIX 3 TO STANDARD CONTRACTUAL CLAUSES**

The parties acknowledge that Clause 10 of the Clauses permits them to include additional business-related terms provided they do not contradict with the Clauses. Accordingly, this Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

**Clauses 4(h) and 8: Disclosure of these Clauses**

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information (as that term is defined in the Agreement) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

**Clause 5(a) and Clause 5(b): Suspension of data transfers and termination**

1. The parties acknowledge that for the purposes of Clause 5(a), data importer may process the personal data only on behalf of the data exporter and in compliance with its documented instructions as set out in the DPA and that pursuant to the DPA, these instructions shall be the data exporter's complete and final instructions.
2. The parties acknowledge that if data importer cannot provide compliance in accordance with Clause 5(a) and/or Clause 5(b), the data importer agrees to promptly inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the affected parts of the Service in accordance with the terms of the Agreement.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Service, it shall first provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. In addition, the data exporter and data importer shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.
5. If, after the Cure Period, the data importer has not or cannot cure the non-compliance in accordance with the paragraphs 3 and 4 above, then the data exporter may suspend and/or terminate the affected part of the Service in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination).

**Clause 5(f): Audit**

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Security Reports and Audits) of the DPA.

**Clause 5(j): Disclosure of subprocessor agreements**

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

**Clause 6: Liability**

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event, shall any party limit its liability with respect to any data subject rights under these Clauses.

**Clause 11: Onward subprocessing**

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer’s compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.

**Annex D - Jurisdiction-Specific Terms**

Europe and the United Kingdom:

1. Objection to Sub-processors. Customer may object in writing to WordFly’s appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with the DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, WordFly will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

2. Government data access requests. As a matter of general practice, WordFly does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about WordFly accounts (including Personal Data Data). If WordFly receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a WordFly account (including Personal Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, WordFly shall: (i) inform the government agency that WordFly is a processor of the data; (ii) attempt to redirect the agency to request the data directly from Customer; and (iii) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy. As part of this effort, WordFly may provide Customer's primary and billing contact information to the agency. WordFly shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or WordFly's property, Sites, or Service.

UK:

1. Until such time as the UK is deemed to provide adequate protection for personal data (within the meaning of applicable EU Data Protection Law) then to the extent WordFly processes (or causes to be processed) any Personal Data protected by EU Data Protection Law applicable to EEA and Switzerland in the United Kingdom, WordFly shall process such Personal Data Data in compliance with the SCCs or any applicable Alternative Transfer Mechanism implemented in accordance with this DPA.

California:

1. Except as described otherwise, the definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.
2. For this "California" section of Annex D only, "WordFly Services" means the suite of marketing tools and insights available for WordFly Customers to use, including without limitation, email campaign management, advertisements, and direct mailings and other related digital communications, analytics and tools made available through the WordFly online marketing platform, as may be further described in the App and/or on the WordFly Site.
3. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Personal Information only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed

in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.

4. WordFly's obligations regarding data subject requests, as described in this DPA, apply to Consumer's rights under the CCPA.
5. Notwithstanding any use restriction contained elsewhere in this DPA, WordFly shall process Personal Information only to perform the WordFly Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law.
6. WordFly may de-identify or aggregate Personal Information as part of performing the Service specified in this DPA and the Agreement.
7. Where Sub-processors process the personal data of Customer contacts, WordFly takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom WordFly has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale". WordFly conducts appropriate due diligence on its Sub-processors.

Canada:

1. WordFly takes steps to ensure that WordFly's Sub-processors, as described in the DPA, are third parties under PIPEDA, with whom WordFly has entered into a written contract that includes terms substantially similar to this DPA. WordFly conducts appropriate due diligence on its Sub-processors.
2. WordFly will implement technical and organizational measures as set forth in the DPA.