Data Processing Addendum

This GDPR Data Processing Addendum ("DPA") forms part of the Terms of Service available at https://pageproofer.com/terms-of-service, entered into by and between _____ ("Customer") and DGrigg Development Inc ("DGrigg"), provider of PageProofer, dated _____, pursuant to which Customer has accessed PageProofer's Application Services as defined in the Terms of Service. The purpose of this DPA is to reflect the parties' agreement with regard to the processing of personal data in accordance with the requirements of Data Protection Legislation as defined below.

In the course of providing PageProofer ("Application Services") to Customer pursuant to the Agreement, DGrigg may process personal data (Annex, A Types of Client Personal Data), on behalf of Customer. DGrigg agrees to comply with the following provisions with respect to any personal data submitted by or for Customer to the Application Services or collected and processed by or for Customer through the Application Services. Any capitalized but undefined terms herein shall have the meaning set forth in the Agreement.

Data Processing Terms

In this DPA, "Data Protection Legislation" means European Directives 95/46/EC and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation (Regulation (EU) 2016/279)), and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction.

"data controller", "data processor", "data subject", "personal data", "processing", and "appropriate technical and organizational measures" shall be interpreted in accordance with applicable Data Protection Legislation.

The parties agree that Customer is the data controller and that DGrigg is its data processor in relation to personal data that is processed in the course of providing the Application Services. Customer shall comply at all times with Data Protection Legislation in respect of all personal data it provided to DGrigg pursuant to the Agreement.

The subject-matter of the data processing covered by this DPA is the Application Services ordered by Customer through PageProofer's website and provided by DGrigg to Customer via https://pageproofer.com. The processing will be carried out until the term of Customer's ordering of the Application Services ceases. Further details of the data processing are set out in Annex A.

In respect of personal data processed in the course of providing the Application Services, DGrigg:

1. Shall process the personal data (Annex A, Details Of Processing) only in accordance with the documented instructions from Customer (as set out in this DPA or as otherwise notified by Customer to DGrigg from time to time) If DGrigg is required to process the personal data for any other purpose provided by applicable law to which it is subject, DGrigg will inform Customer of such requirement prior to the processing unless that law prohibits this on important grounds of public interest;
2. Shall notify Customer without undue delay if, in DGrigg's opinion, an instruction for the processing of personal data given by Customer infringes applicable Data Protection Legislation;
3. Shall implement and maintain appropriate technical and organizational measures designed to protect the personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure (Annex B, Security Measures). These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected;
4. May hire other companies to provide limited services on its behalf, provided that DGrigg complies with the provisions of this Clause. Any such subcontractors will be permitted to process personal data only to deliver the services DGrigg has retained them to provide, and they shall be prohibited from using personal data for any other purpose. DGrigg remains responsible for its subcontractors' compliance with the obligations of this DPA. Any subcontractors to whom DGrigg transfers personal data will have entered into written agreements with DGrigg requiring that the subcontractor abide by terms substantially similar to this DPA.
5. Shall ensure that all DGrigg personnel required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in this Clause (Annex B, Security Measures);
6. At the Customer's request and cost (and insofar as is possible), DGrigg shall assist the Customer by implementing appropriate and reasonable technical and organizational measures to assist with the Customer's obligation to respond to requests from data subjects under Data Protection Legislation (including requests for information relating to the processing, and requests relating to access, rectification, erasure or portability of the personal data) provided that DGrigg reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance;
7. When the General Data Protection Regulation (Regulation (EU) 2016/279) comes into effect, shall take reasonable steps at the Customer's request and cost to assist Customer in meeting Customer's obligations under Article 32 to 36 of that regulation taking into account the nature of the processing under this DPA, provided that DGrigg reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance;
8. At the end of the applicable term of the Application Services, upon Customer's request, shall securely destroy or return such personal data to Customer;
9. May transfer personal data from the EEA to Canada and the US for the purposes of this DPA;

10. Shall allow Customer and its respective auditors or authorized agents to conduct audits or inspections during the term of the Agreement, which shall include providing reasonable access to the resources and personnel used by DGrigg in connection with the provision of the Application Services, and provide all reasonable assistance in order to assist Customer in exercising its audit rights under this Clause. The purposes of an audit pursuant to this Clause include to verify that DGrigg is processing personal data in accordance with its obligations under the DPA and applicable Data Protection Legislation. Notwithstanding the foregoing, such audit shall consist solely of: (i) the provision by DGrigg of written information (including, without limitation, questionnaires and information about security policies) that may include information relating to subcontractors; and (ii) interviews with DGrigg's IT personnel. Such audit may be carried out by Customer or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality. For the avoidance of doubt no access to any part of DGrigg's IT system, data hosting sites or centres, or infrastructure will be permitted;
11. If DGrigg becomes aware of any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data that is processed by DGrigg in the course of providing the Application Services (an "Incident") under the Agreement it shall without undue delay notify Customer and provide Customer (as soon as possible) with a description of the Incident as well as periodic updates to information about the Incident, including its impact on Customer Content (Annex B, Information Security Incident Management). DGrigg shall additionally take action to investigate the Incident and reasonably prevent or mitigate the effects of the Incident;
12. DGrigg shall provide information requested by Customer to demonstrate compliance with the obligations set out in this DPA.

Executed by and on behalf of: **DGrigg**	**Executed** by and on behalf of: **Customer**
_____ Signature	_____ Signature
_____ Name	_____ Name
_____ Role	_____ Role
_____ Date	_____ Date

Annex A: Details Of Processing

Duration of the Processing: The duration of data processing shall be for the term agreed between Customer and DGrigg in the Agreement or an applicable Order Form.

Nature and purpose of the Processing: The scope and purpose of processing of the data subjects' personal data is to facilitate the provision of Application Services.

Types of Personal Data: The personal data transferred includes e-mail, documents and other data in an electronic form provided in the context of Application Services. Types of personal data collected through Application Services:

- Name
- Email
- City
- Region
- Country
- Time zone
- IP Address
- Browser
- Browser Version
- Device
- Operating System
- Screen Height
- Screen Width
- Current URL

Categories of Data Subjects: Data subjects include the Customer’s representatives and end-users including employees, contractors, collaborators, and Customer’s customers. Data subjects may also include individuals attempting to communicate or transfer personal information to users of Application Services. The data subjects exclusively determine the content of data submitted to Application Services.

Annex B: Security Measures

Personnel: Data Processor's personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.

Data Privacy Contact: Derrick Grigg, DGrigg Development Inc., 783 Valley Green Trail, Newmarket, Ontario, Canada, L3X 2V6, derrick@pageproofer.com

Technical and Organization Measures: The Data Processor has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

Organization of Information Security:

1. **Security Roles and Responsibilities:** The Data Processor has appointed Derrick Grigg as the security officer responsible for coordinating and monitoring the security rules and procedures.
2. **Duty of Confidentiality:** The Data Processor's personnel with access to customer data are subject to confidentiality obligations.

Risk Management: The Data Processor conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing. The Data Processor implements measures, as needed, to address vulnerabilities discovered in a timely manner.

Storage: The Data Processor's database servers are hosted in a data center operated by a third party vendor, that has been qualified per the Data Processor's vendor management procedure. The Data Processor maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

Asset Management:

1. **Asset Inventory:** The Data Processor maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.
2. **Asset Handling:** The Data Processor employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access DGrigg Development. networks. The Data Processor imposes restrictions on printing customer data and has procedures for disposing of printed materials that contain customer data. The Data Processor's personnel must obtain authorization prior to storing customer data on portable devices, remotely accessing customer data, or processing customer data outside the Data Processor's facilities.

Software Development and Acquisition: For the software developed by Data Processor, Data Processor follows secure coding standards and procedures set out in its standard operating procedures.

Change Management: Data Processor implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for the Data Processor's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

Third Party Provider Management: In selecting third party providers who may gain access to, store, transmit or use customer data, Data Processor conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

Human Resources Security: The Data Processor informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

Physical and Environmental Security:

1. **Physical Access to Facilities:** The Data Processor limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job function. Data Processor terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.
2. **Physical Access to Components:** The Data Processor maintains records of the incoming and outgoing media containing customer data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of customer data they contain.
3. **Protection from Disruptions:** The Data Processor uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.
4. **Component Disposal:** The Data Processor uses commercially reasonable processes to delete customer data when it is no longer needed.

Communications and Operations Management:

1. **Security Documents:** The Data Processor maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel.
2. **Data Recovery Procedures:** On an ongoing basis, the Data Processor maintains multiple copies of customer data from which it can be recovered. The Data Processor stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located. The Data Processor has procedures in place governing access to copies of customer data. The Data Processor has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.
3. **Encryption/Mobile Media:** The Data Processor uses HTTPS encryption on all data connections. The Data Processor restricts access to customer data in media leaving its facilities. The Data Processor further has a destruction policy for hardware in the data centre that stores customer data.
4. **Event Logging:** The Data Processor logs the use of our data-processing systems. The Data Processor maintains logs for at least 7 days.

Access Control:

1. **Records of Access Rights:** The Data Processor maintains a record of security privileges of individuals having access to customer data.
2. **Access Authorization:** The Data Processor maintains and updates a record of personnel authorized to access systems that contain customer data. The Data Processor deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services as well as such authentication credentials that have not been used for a period of time not to exceed six months. The

Data Processor identifies those personnel who may grant, alter or cancel authorized access to data and resources.

3. **Least Privilege:** Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function. The Data Processor restricts access to customer data to only those individuals who require such access to perform their job function.
4. **Integrity and Confidentiality:** The Data Processor instructs its personnel to disable administrative sessions when leaving the Data Processor's premises or when computers are unattended. The Data Processor stores passwords in a way that makes them unintelligible while they are in force.
5. **Authentication:** The Data Processor uses commercially reasonable practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, the Data Processor requires the password to be at least eight characters long. The Data Processor ensures that de-activated or expired identifiers are not granted to other individuals. The Data Processor maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts. The Data Processor uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
6. **Network Design:** The Data Processor has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

Network Security:

1. **Network Security Controls:** Data Processor's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.
2. **Antivirus:** Data Processor implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Data Processor's server change control procedures.

Information Security Incident Management:

1. **Record of Breaches:** The Data Processor maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.
2. **Record of Disclosure:** The Data Processor tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

Business Continuity Management: The Data Processor employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original state from before the time it was lost or destroyed.