My Software Group Ltd.

Data Processing Agreement (DPA)

This page is provided for identification and presentation purposes only.

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") shall apply to all agreements entered into by and between the Supplier and its customers for the provision of Software as a Service (SaaS) services. The terms and conditions set forth herein govern the processing of Personal Data by the Supplier on behalf of the Customer in connection with the Supplier's SaaS offerings. This Agreement is integral to ensuring compliance with applicable Data Protection Laws and outlines the responsibilities and obligations of both the Supplier and the Customer with respect to the protection and processing of Personal Data.

Part A
Operative provisions

Definitions

1.1 In this DPA:

applicable law	means applicable law of the United Kingdom (or of a part of the United Kingdom);
Controller	has the meaning given in applicable Data Protection Laws from time to time;
Customer	any user of the Supplier's SaaS services;
Data Protection Laws	means, as binding on either party or the Services: (a) the GDPR; (b) the Data Protection Act 2018; (c) any laws which implement or supplement any such laws; and (d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;
Data Subject	has the meaning given in applicable Data Protection Laws from time to time;

GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);
International Organisation	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data Breach	has the meaning given in applicable Data Protection Laws from time to time;
processing	has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including **process**, **processed** and **processes** shall be construed accordingly);
Processor	has the meaning given in applicable Data Protection Laws from time to time;
Protected Data	means Personal Data received from or on behalf of the Customer in connection with the performance of the Supplier's obligations under any Services Agreement;

Services Agreement	means any agreement entered into between the Supplier and the Customer for the provision of Software as a Service (SaaS) services, including all schedules, annexes, and amendments thereto, under which the Supplier agrees to provide and the Customer agrees to receive such services, and which incorporates the terms of this DPA;
Sub-Processor	means any Processor engaged by the Supplier (or by any other Sub-Processor) for carrying out any processing activities in respect of the Protected Data on behalf of the Customer; and
Supplier	My Software Group Ltd., a company incorporated in England with company registration number 15638670, having is registered office at 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ.

Customer's compliance with Data Protection Laws

The parties agree that the Customer is a Controller and that the Supplier is a Processor for the purposes of processing Protected Data pursuant to any Services Agreement. The Customer shall, at all times, comply with all Data Protection Laws in connection with the processing of Protected Data. The Customer shall ensure all instructions given by it to the Supplier in respect of Protected Data (including the terms of any Services Agreement) shall at all times be in accordance with all Data Protection Laws. Nothing in any Services Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

Supplier's compliance with Data Protection Laws

The Supplier shall process Protected Data in compliance with the obligations placed on it under Data Protection Laws and the terms of any Services Agreement.

Indemnity

The Customer shall indemnify and keep indemnified the Supplier against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data Subjects, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any breach by the Customer of its obligations under this DPA.

Instructions

1.2 The Supplier shall only process (and shall ensure Supplier Personnel only process) the Protected Data in accordance with Section 1 of Part B of this DPA and any Services Agreement (including with regard to any transfer to which paragraph 0 of this Part A relates), except to the extent:

1.2.1 that alternative processing instructions are agreed between the parties in writing; or

1.2.2 otherwise required by applicable law (and shall inform the Customer of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).

1.3 Without prejudice to paragraph 0 of this Part A, if the Supplier believes that any instruction received by it from the Customer is likely to infringe the Data Protection Laws it shall be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing. The Charges payable to the Supplier shall not be discounted or set-off as a result of any delay or non-performance of any obligation in accordance with this paragraph 1.3.

Security

1.4 The Supplier shall implement and maintain the technical and organisational measures set out in Section 2 of Part B of this DPA to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

Sub-processing and personnel

1.5 The Supplier shall:

1.5.1 not permit any processing of Protected Data by any Sub-Processor without the prior specific written authorisation of the Customer;

1.5.2 prior to any Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure such Sub-Processor is appointed under a binding written contract containing materially the same obligations as under this DPA (including those relating to sufficient guarantees to implement appropriate technical and organisational measures) and ensure such Sub-Processor complies with all such obligations;

1.5.3 remain fully liable to the Customer under any Services Agreement for all the acts and omissions of each Sub-Processor as if they were its own; and

1.5.4 ensure that all persons authorised by the Supplier or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.

List of authorised Sub-Processors

The Customer authorises the appointment of the Sub-Processors listed below:

Sub-Processor	**Processing this Sub-Processor is authorised to undertake**
FreeAgent Central Ltd, a company incorporated in **Scotland** under number **SC316774**, whose registered office is at **One Edinburgh Quay, 133 Fountainbridge, Edinburgh, EH3 9QG, United Kingdom**	Accounting and financial management services.
Stripe Payments Europe, Ltd, a company incorporated in **Ireland** under number **513174**, whose registered office is at **The One Building, 1 Grand Canal Street Lower, Dublin 2, Co. Dublin, D02 H210, Ireland**	Payment processing services.
Google LLC, a company incorporated in **Delaware, USA**, whose principal office is at **1600 Amphitheatre Parkway, Mountain View, CA 94043, USA**	Cloud infrastructure, data storage, platform services, collaboration tools, analytics and document management (with data hosted primarily in the UK/EU).

Freshworks Technologies UK Limited, a company incorporated in **England and Wales** under number **09338697**, whose registered office is at **79 Hatton Garden, London, EC1N 8JS, United Kingdom**	Customer support, FAQs and helpdesk services.
Wix.com (UK) Limited, a company incorporated in **England** under number **12576807**, whose registered office is at **30 Old Bailey, London, EC4M 7AU, United Kingdom**	Website hosting, data storage, form submissions and e-commerce transactions
MailerLite Limited, a company incorporated in **Ireland** under number **689826**, whose registered office is at **88 Harcourt St, Saint Kevin's, Dublin 2, D02 DK18, Ireland**	Email sending, list management and campaign analytics.
Cloudflare, Inc., a company incorporated in the **San Francisco, USA,** whose principal office is at **101 Townsend Street, San Francisco, CA 94107, USA**	Content delivery network (CDN), security, tunnelling, and traffic protection services.

Further Sub-Processors

The Customer shall reply to any communication from the Supplier requesting any further prior specific authorisation of a Sub-Processor pursuant to paragraph 1.5.1 of this Part A promptly and in any event within 10 Business Days of request from time to time. The Customer shall not unreasonably withhold, delay or condition any such authorisation.

Assistance

1.6 The Supplier shall (at the Customer's cost and expense) assist the Customer in ensuring compliance with the Customer's obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to the Supplier.

1.7 The Supplier shall (at the Customer's cost and expense) and taking into account the nature of the processing, assist the Customer (by appropriate technical and organisational measures), insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the GDPR in respect of any Protected Data.

1.8 The Supplier shall at the Customer's cost and expense promptly refer to the Customer all requests it receives for exercising any Data Subjects' rights under Chapter III of the GDPR which relate to any Protected Data. It shall be the Customer's responsibility to reply to all such requests as required by applicable law.

International transfers

The Supplier shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to any country or territory outside the United Kingdom or to any International Organisation without the prior written authorisation of the Customer except where required by applicable law (in which case the provisions of paragraph 1.2 of this Part A shall apply).

Audits and processing

The Supplier shall, in accordance with Data Protection Laws, make available to the Customer on request such information that is in its possession or control as is necessary to demonstrate the Supplier's compliance with the obligations placed on it under this DPA and to demonstrate compliance with the obligations on each party imposed by Article 28 of the GDPR, and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose (subject to a maximum of [*one*] audit request in any 12 month period under this paragraph 0). To the extent consistent with the foregoing, the Supplier shall, however, be entitled to withhold information where it is commercially sensitive or confidential to it or its other customers.

Breach

The Supplier shall notify the Customer without undue delay and in writing on becoming aware of any Personal Data Breach in respect of any Protected Data.

Deletion/return

1.9 On the end of the provision of the Services relating to the processing of Protected Data (the **Processing End Date**), at the Customer's cost and expense and the Customer's option, the Supplier shall either return all of the Protected Data to the Customer or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Supplier to store such Protected Data. To the extent the Customer has not notified the Supplier within 30 days of the Processing End Date that it requires the return of any Protected Data the Supplier shall be irrevocably authorised to securely dispose of the Protected Data at the Customer's cost and expense.

1.10 On request from the Customer the Supplier shall confirm in writing whether or not it has complied with its obligations to dispose of the Protected Data under paragraph 1.9 of this Part A.

Survival

1.11 This DPA shall survive termination or expiry of any Services Agreement:

1.11.1 indefinitely in the case of paragraphs 0 and 0 of this Part A; and

1.11.2 in the case of all other paragraphs and provisions of this DPA, until the later of:

(a) the termination or expiry of any Services Agreement; or

(b) return or secure deletion or disposal of the last of the Protected Data in the Supplier's (or any of its Sub-Processor's) possession or control in accordance with any Services Agreement.

Part B
Data processing and security details

Section 1—Data processing details

Processing of the Protected Data by the Supplier under any Services Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Section 1 of this Part B.

Subject-matter of processing:

The processing of Personal Data pertains to the creation, completion, and management of medical patient reports using the Supplier's SaaS platform.

Duration of the processing:

The processing shall continue for the duration of the Services Agreement and any subsequent period required for compliance with legal obligations or as agreed upon in writing by the parties.

Nature and purpose of the processing:

The processing involves collecting, storing, and managing medical data to facilitate the creation, completion, and archiving of patient medical reports for the purpose of healthcare administration and patient care management.

Type of Personal Data:

The Personal Data processed shall include, but not be limited to, patient identification details, medical history, diagnostic information, treatment plans, and other related health data.

Categories of Data Subjects:

Data Subjects include patients whose medical data is processed, as well as healthcare professionals and administrators who interact with the SaaS platform for managing such data.

Specific processing instructions:

The processing of Personal Data shall be conducted in compliance with applicable Data Protection Laws and shall include measures to ensure data accuracy, integrity, and confidentiality. The Supplier must implement access controls to restrict data access to authorised personnel only and ensure that all data transfers are encrypted.

Section 2—Minimum technical and organisational security measures

The Supplier shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

(a) Encryption of data both in transit and at rest to prevent unauthorised access.

(b) Regular security audits and vulnerability assessments to identify and mitigate potential risks.

(c) Comprehensive data breach response and notification procedures.

(d) Role-based access control to ensure only authorised users have access to specific data.

(e) Secure data backup and recovery systems to prevent data loss.

(f) Continuous monitoring of systems for unusual activity or potential security threats.