This **PROCESSOR AGREEMENT** is entered into on the "*Effective Date*", by and between

PARTIES

(1) The Data Controller (Controller)

Your information : Electronically added using the form below this scroll section.

(2) The Data Processor (Processor)
Salon Guru Limited incorporated and registered in England and Wales with company number 09086085 whose registered office is at
Essex House
39-41 High Street,
Dunmow,
Essex, CM6 1AE

BACKGROUND:

(A) The Controller and the Processor enter into a Website Design and Online Marketing agreement **(Service Agreement)** on the "Effective Date" that may require the Processor to process Personal Data on behalf of the Controller.

(B) This Processor Agreement sets out the terms and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS:

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Data Protection Legislation: all applicable data protection laws including GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the Privacy and Electronic Communications Directive (*2002/58/EC*) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).

Data Subject: an individual who is the subject of Personal Data.

GDPR: General Data Protection Regulation (*(EU) 2016/679*).

Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.2 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.3 A reference to writing or written includes email.

2. PROCESSING PURPOSES

2.1 The Controller and the Processor acknowledge that the Controller is the controller and the Processor is the processor and that the Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation.

2.2. Where the Processor appoints a subcontractor pursuant to clause 4 below, the Processor shall be a data controller in relation to such processing.

2.3 The Processor may process the Personal Data categories and Data Subject types set out in Schedule 1 of this Agreement.

3. PROCESSOR'S OBLIGATIONS

- The Processor shall:
    - implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of Data Protection Legislation and ensure the protection of the rights of the Data Subject, as further set out below in this Agreement;
    - only use subcontractors to help with the processing of Personal Data in the circumstances set out in clause 4 below;

    - process the Personal Data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
    - ensure that persons authorised to process the personal data (such as its employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    - take the security measures set out in clause 5 below;
    - taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights as set out in clause 6 below;
    - assist the Controller in ensuring compliance with the obligations set out in clause 7 below (data breach) taking into account the nature of processing and the information available to the Processor;
    - at the choice of the Controller, delete or return all the Personal Data to the Controller after the termination or expiry of the Services Agreement and delete existing copies (unless Union or Member State law requires storage of the Personal Data);
    - make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;
    - assist the Controller in ensuring compliance with the requirement to carry out Data Protection Impact Assessments as set out in Article 35 of GDPR, taking into account the nature of processing and the information available to the Processor;
    - immediately inform the Controller, if in the opinion of the Processor, an instruction from the Controller infringes Data Protection Legislation.
- The Processor will promptly comply with any request by or instruction from the Controller to process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- The Processor will immediately notify the Controller if in its opinion, the Processor carrying out the processing of Personal Data on an instruction from the Controller would infringe any provision of Data Protection Legislation.
- The Processor will keep all Personal Data confidential and not disclose such data to third parties unless specifically authorised in writing by the Controller or as required by law. If the Processor is required by law, court, regulator or supervisory authority to process or disclose any Personal Data, the Processor will first inform the Controller of this and allow the Controller to object or challenge the requirement, unless the law prohibits the Processor from informing the Controller.

4. SUBCONTRACTORS

- The Processor may only authorise a third party ("subcontractor") to process the Personal Data if:
    - the Processor has obtained the consent from the Controller for each appointment of a subcontractor, or the subcontractor's name is set out in Schedule 1, or the subcontractor is working within one of the approved categories; and
    - the Processor has carried out appropriate due diligence on any subcontractor to ensure that the subcontractor can satisfy its contractual obligations; and
    - the Processor and the subcontractor enter into a written contract containing terms the same as those set out in this Agreement, in particular, in relation to data security measures; and
    - the Processor maintains control over all Personal Data it shares with the subcontractor; and
    - the Processor ensures that the subcontractor does not process the Personal Data except on instructions from the Data Controller (unless required to do so by Union or Member State law); and
    - the contract between the Processor and the subcontractor terminates automatically on termination of this Agreement.
- The Processor shall be fully liable for the actions and inactions of the subcontractor and shall be responsible for the subcontractor's performance of obligations.

5. SECURITY

5.1 The Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- the pseudonymisation and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. RESPONSES TO DATA SUBJECTS

6.1 The Processor will put in place such technical and organisational measures as may be appropriate to enable the Controller to comply with the rights of Data Subjects under Data Protection Legislation, including the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object to processing and the right to object to automated individual decision making.

6.2 If the Processor receives any complaint or other communication relating to the processing of the Personal Data or a Subject Access Request from a Data Subject, it must notify the Controller as soon as possible after it receives it and in any event within 5 working days and will provide the Controller with all reasonable assistance in helping the Controller to reply to such communications.

6.3 The Processor will provide to the Controller such information as the Controller may reasonably require in order for the Controller to comply with the rights of Data Subjects under Data Protection Legislation. The Processor may not charge an additional amount for fulfilling its obligations under this clause 6.

6.4 The Processor will provide all appropriate assistance to the Controller to enable it to comply with any information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

6.5 The Processor shall not disclose Personal Data to any third party other than at the Controller's written request or as set out in this agreement or as required by law.

7. PERSONAL DATA BREACH

7.1 If any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable ("Personal Data Loss"), the Processor will notify the Controller without undue delay (and in any event within 2 working days) after learning of such Personal Data Loss and the Processor shall to the extent possible restore any such data at its own expense.

7.2 If the Processor becomes aware of any unauthorised or unlawful processing of the Personal Data or any Personal Data Breach, it will notify the Controller without undue delay (and in any event within 2 working days) including all relevant information such as:

(a) a description of the nature of the Personal Data Breach, the unauthorised or unlawful processing and/or the Personal Data Loss, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken, including measures to

mitigate the impact.

7.3 The parties will co-ordinate and co-operate with each other to investigate any matters arising as contemplated by this clause.

7.4 The Processor shall take all reasonable steps to mitigate the effects and reduce the impact of any Personal Data Breach or unlawful Personal Data processing.

7.5 The Processor agrees that it shall not (and the Controller is solely responsible to):

(a) provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or any other third party, except when the Processor (as opposed to the Controller) is required by law or regulation to provide such notice; and

(b) offer any type of remedy to affected Data Subjects.

7.6 The Processor will cover all reasonable expenses associated with the performance of its obligations under this clause 7.

8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

8.1 The Processor (or any subcontractor of the Processor) shall not transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) without obtaining the Controller's prior written consent (except where the Processor is required to transfer such data by Union or Member State law, in which case the Processor shall inform the Controller of such legal requirement before processing takes place, unless any law prohibits such disclosure on important grounds of public interest).

8.2 If the Controller consents to the transfer or other processing of the Personal Data outside of the EEA and no appropriate safeguards exist (such as an adequacy decision or the Processor being part of the EU-US Privacy Shield), the Processor and the Controller will each execute the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU ("SCCs").

8.2 if the Processor appoints subcontractors that are based outside of the EEA, the Processor shall, prior to any Personal Data being transferred to such countries, (i) ensure that such subcontractor executes the SCCs and (ii) send a copy of such executed SCCs to the Controller.

9. TERM AND TERMINATION

9.1 This Agreement will continue for so long as the Processor processes any Personal Data related to the Services Agreement (**Term**).

9.2 If the Processor breaches this Agreement, such breach shall constitute a material breach of the Services Agreement and the Controller may terminate the Services Agreement immediately on written notice to the Processor without further liability or obligation for the Controller.

10. DATA RETURN AND DESTRUCTION

10.1 The Processor will, on the request of the Controller, provide the Controller with a copy of or access to the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

10.2 On termination or expiry of the Services Agreement, the Processor will at least 7 days prior to the date of expiry or termination ask the Controller whether the Controller wants the Personal Data to be deleted, destroyed, returned or retained and shall follow the Controller's instructions accordingly.

10.3 If the Processor is required by any law, regulation, or government or regulatory body to retain any documents or materials, the Processor will inform the Controller in writing of such requirement, providing details of the legal basis for retention and setting out the timings for deletion when such retention period ends.

10.4 If the Controller requires the Processor to delete or destroy certain documents or materials or anything else containing Personal Data, the Processor shall certify in writing that it has so deleted or destroyed the Personal Data within 3 days of doing so.

11. AUDIT

11.1 The Controller (and any third-party representatives) may audit the Processor's compliance with its obligations under this Agreement and the Processor will give the Controller (and its third-party representatives) all necessary assistance and co-operation to conduct such audits.

11.2 If a Personal Data Breach occurs, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, or if the Controller so requires it, the Processor will:

(a) conduct its own investigation to confirm the cause of such Personal Data Breach or breach of obligations;

(b) provide to the Controller a written report on the investigation including any proposals to remedy any problems identified by the investigation; and

(c) remedy the problems identified within 7 days of the date of the written report.

11.3 On the Controller's written request, the Processor will audit a subcontractor's compliance with its obligations regarding the Controller's Personal Data and provide the Controller with the audit results.

11.4 The Processor will carry out an annual security audit (or at such other periods required by the Controller) identifying any areas of deficiency (when taking into account the scope and nature of the processing of Personal Data and the best practice technologies available at such time) and will provide the written report to the Controller.

12. WARRANTIES

The Processor warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons processing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Services Agreement's contracted services.

13. NOTICE

13.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing.

13.2 Clause 13.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

14. GOVERNING LAW

15.1 This agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with the law of England and Wales.

15.2 Each party irrevocably agrees that the courts of England and Wales shall have non-exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This agreement has been entered into on “Effective Date”.

Signed by the Client (Controller)

Electronically added using the form below this scroll section.

Signed by the Salon Guru (Processor)

Signed by Philip Evans

for and on behalf of Salon Guru Limited Director

SCHEDULE 1

PERSONAL DATA PROCESSING PURPOSES AND SUBCONTRACTORS

Personal account creation and management

Personal data collected during the creation or management of an account on our website through a social media login or in salon.

Newsletter and marketing subscription

Personal data collected when you subscribe to receive our marketing communications either on-line or in-salon.

Purchases management

Personal data collected during the purchase process or when paying for a deal, offer or promotion.

Online browsing

Personal data collected by cookies when users are on our website or on third-party website/apps where cookies are used.

Promotions

Personal data collected during a competition, game, contest, promotional offer, survey etc.

User Generated Content

Personal data collected when users/clients submit images or ratings and reviews on our website or online software tools or accept our re-use content they posted on social media platforms.

Enquiries and Comments

Personal data collected when you ask questions or leave comments on our website.

Approved Subcontractors:

The Data Processor may at times use any of the following named Data Processor subcontractors and share some parts of a client's personal data with them.

NAME OF SUBCONTRACTOR	DATA PROCESSING
Google	Analytics tracking of website visitors via pixel
	Adwords tracking of visitors via pixel
	Google Docs for data storage
	Google enabled logins
Paypal	To process payment data
Go Cardless	To process payment data
Facebook	Tracking via website pixel
	Submission and storage of Client Reviews
	Facebook enabled logins
The in-salon software provider	To store client data and manage communication

The Data Processor may at times use other approved subcontractors that fall into these approved categories…

IT, software and website partners.
Online Data storage facilities.
Email software.
Selected publishing partners and authors.
Selected marketing partners.
Any prospective seller or buyer of businesses or assets, only in the event that we decide to acquire, transfer or sell any business or assets.
Any other third parties (including legal or other advisors, regulatory authorities, courts and government agencies) where necessary to enable us to enforce our legal rights, or to protect the rights, property or safety of our employees or where such disclosure may be permitted or required by law or where we have a legal obligation to do so

SCHEDULE 2

SECURITY MEASURES

Appropriate technical and organisational measures have been taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

We have achieved this in a number of ways:

- Physical Security
    - Our servers are located across three state-of-the-art compounds in Dublin run by Amazon Web Services. Their physical protections include gated/keycard entrances, CCTV and 24 hour security. Full details can be found here: https://aws.amazon.com/compliance/data-center/controls/
- Server administrator security
    - Our servers are only accessible by the technical team within Salon Guru. From time to time we may seek assistance from a third party to help us manage our platform however when access is granted, it is strictly monitored. Access to servers is revoked when no longer required.
- Access Control
    - Users of the system only have access to information required to complete processing for their role. We restrict site access so that users only have access to sites they own and roles IE Administrator or Editor are set based on need.
    - Logins are routinely revoked when no longer required.
    - Our staff are trained to ensure that information is not processed, accessable or viewed by third parties without formal consent.
- Backups & Snapshots
    - All servers within our platform are backed up daily.
    - Server snapshots are stored for a minimum of twenty one days
    - Database backups are stored for ten days however it is possible to go back further than this through Amazons Arora RDS to restore a database or part of a database to a specific point in time.
    - All backups & snapshots are stored within a AWS S3 filesystem which is region replicated so that even if two out of three (Ireland) Data Centers are destroyed Salon Guru will still have access to the data in order to perform a disaster recovery.
- Disaster Recovery
    - Our technical team routinely tests to ensure that snapshots and backups are accessible in order to perform a disaster recover if required.

Salon Guru holds personal data (such as information about sales, contact information and emails). Salon Guru has a range of security measures in place to ensure this data is kept safe from potential online threats.

We achieve this in the following ways:

- SSL (Secure Socket Layer)
    - Our system operates a strict SSL policy and does not allow unencrypted traffic in any form. This includes Administrator access to servers.
    - All websites are HTTPS using TLSv1.3 with a strong cipher (AES 128_GCM)
    - Any non secure requests to visit a website or service are either rejected or redirected.
- Intermediate (between our servers and the visitor)
    - All website traffic is encrypted end-to-end and passes through a security firewall provided by Cloudflare. This is a reverse proxy environment where web traffic is firstly encrypted by our system and is then encrypted for a second time when it passes through the Cloudflare edge network to a visitor.
    - Cloudflare security firewalls are in place to detect traffic that is not genuine and protect systems in the event of a DDOS (Distributed Denial Of Service) attack.
    - Further details of Cloudflare protection systems can be found here: https://www.cloudflare.com/security/
- Server
    - Wordfence is able to detect malicious traffic not detected by Cloudflare and is setup to block unusual activity. Wordfence can also block (without intervention) any known dangerous traffic or IP addresses flagged by the Wordfence security network.
- Database
    - The database(s) is not publicly accessible to the internet and cannot be accessed outside of Amazon Web Services.
- Access Control
    - Users of the system only have access to information required to complete processing for their role. We restrict site access so that users only have access to sites they own and roles IE Administrator or Editor are set based on need.
    - Logins are routinely revoked when no longer required.
    - Our staff are trained to ensure that information is not processed, accessable or viewed by third parties without formal consent.
- Plugins
    - We only install plugins from trusted sources. This reduces the risk of any malicious code or any code designed to steal data being inadvertently added to our system.
    - WordPress plugins are kept up-to-date as required
- Patches

    - Servers are kept up-to-date with the latest security patches and where required, our primary production server is rebuilt every quarter to ensure all server side software contains the very latest security benefits.

As a part of our security measures, our organisation ensures that information is protected as-far-as reasonably possible against a variety of online threats. This list is not exhaustive but does include:

- Brute Force Attacks
    - If a password is typed incorrectly more than three times in a row, the IP address of that user is locked out for up to thirty minutes. This prevents any brute force password attempts to any account or website.
- Password recovery attempts
    - In the event a password reset attempt is requested, this can only be attempted three times before the user is locked out.
    - Password resets can only be completed by verifying an email address
- Web Application Firewall
    - Any IP addresses deemed dangerous by the Wordfence security network are automatically blocked
    - Firewall rules are updated in real time to ensure any security issues detected within any WordPress plugin are patched.
    - Unauthorised Crawlers are blocked. Wordfence only allows crawling of a website from genuine sources IE: Bing/Google Bot etc. This prevents automated and unauthorised crawlers stealing site content/images.
- Server Default Security
    - The public WordPress web directory of our servers is read only to the web server (Nginx & Apache). This prevents unauthorised code / malware & back doors from being able to install on our web servers. Production code can only be updated manually by a Salon Guru Technician.
- Security Scans
    - Wordfence completes daily scans for any files that have been modified and flags anything suspicions
    - Wordfence completes daily scans for any known file based security threats
    - WordPress users are scanned daily for weak passwords
    - Weekly security reports are emailed to Salon Guru’s Technical team.
- Live Traffic
    - Traffic across the system can be monitored in real time. This data includes IP addresses, country of origin and a log of which pages have been accessed.
    - Any threats or unusual activity that is detected can be blocked at any time as required.
- Spam Filters
    - Wordfence monitors site usage for spam which is blocked if any firewall rules or

unusual behaviour is detected.
    - https://akismet.com/ is used to prevent spam to any Comments & Questions page.
    - Any other forms are protected using Google's RECaptcha. Further details can be found here: //www.google.com/recaptcha/intro/v3beta.html
- Rate Limiting & Country Blocking
    - When required, we can limit block access by IP address, country or region as required.

Monitoring is an important part of our security and helps us identify issues that may be arising in real time. Some of the monitoring we have includes:

- Server logs
- Wordfence real time monitoring
- Nagios Server Monitoring
    - This system externally tests all servers and services every two minutes to ensure everything is online and operating as expected. SMS & email notifications are sent to our technical team within four minutes of a fault being detected. Our current system status can be found here: https://nagios.salonguru.net/
- Specific website tests
    - Each website is tested to ensure it is online and responding at least once an hour. You can see the result of our tests in the yoursalon.co dashboard (if used)

Version History

Version 1.1 18/5/2018