UPFIELD - DATA PROCESSING AGREEMENT

DEFINITIONS

- **Agreement** means any agreement between you and us under which you process Upfield Personal Data.
- **Data Protection Legislation** means European Union Directive 2002/58/EC (as amended or updated from time to time) and any legislation and/or binding regulations implementing or made pursuant to them, the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications) and all other worldwide data protection and privacy laws and regulations applicable to Upfield Personal Data.
- **Data Controller** means as defined in the Data Protection Legislation.
- **Data Processor** means as defined in the Data Protection Legislation.
- **Data Processor Information Systems** means any systems, applications and/or computers used by you to process Upfield Personal Data pursuant to the Agreement, which includes laptops and network devices.
- **Data Processor Personnel** means all persons with access to Upfield Personal Data engaged by you in the provision of Services under the Agreement, including employees, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.
- **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as may be amended from time to time.
- **Model Clauses** means the standard contractual clauses approved by the EU Commission (Decision 2010/87/EU as amended by Decision 2016/2297) for the transfer of personal data to processors established in third countries, or any other standard contractual clauses issued by the European Commission which replace such clauses from time to time.
- **Personal Data** means any information relating to an identified or an identifiable natural person (data subject) who can be identified, directly or indirectly (including pseudonymised data).
- **Processing** means accessing, collecting, obtaining, recording, holding, disclosing, using, altering, deleting, erasing or destroying Upfield Personal Data, or carrying out any operation(s) on the Upfield Personal Data or as otherwise defined under applicable Data Protection Legislation. "Process" or "Processed" shall be construed accordingly.
- **Security Incident** means the accidental or deliberate or unlawful or unauthorised acquisition, destruction, loss, alteration, access, use or disclosure of Upfield Personal Data transmitted, stored or otherwise processed or any other breach of paragraph 10.
- **Services** means the services to be provided by you pursuant to this Agreement.
- **Upfield** means Upfield Europe B.V. and / or any of its affiliates with which you have entered into an Agreement involving the processing of Upfield Personal Data and "our", "us" and "we" shall be construed accordingly.
- **Upfield Information Systems** means any systems, applications and/or computers owned/ managed by Upfield, which includes laptops and network devices.
- **Upfield Personal Data** means Personal Data provided or made available by us Upfield to you as a Data Processor under this addendum, including any Personal Data processed in connection with the Agreement.

1 Relationship of the parties

Upfield, as the Data Controller, appoints you as a Data Processor (or sub-processor) to process the Upfield Personal Data described below or as described in the Agreement: a) Types of Personal Data: first name, last name, address, telephone number, email addresses, date of birth; b) Duration of Processing: until the earliest of (i) expiry/termination of this Agreement or (ii) the date upon which Processing is no longer necessary for the purposes of either party performing its obligations under this Agreement (to the extent applicable); c) Nature of Processing: collection, analysis, storage, duplication, deletion, disclosure; d) Purposes of Processing: necessary for the provision of the Services; and e) Categories of data subjects may include employees, customers, end users, contractors, consultants.

2 Data Processing

a. You shall process Upfield Personal Data as a Data Processor only for the purposes described in Clause 1 or as necessary to perform your obligations under the Agreement and strictly in accordance with Upfield's instructions as set out in the Agreement, this addendum or as provided in writing by us from time to time.

b. If you are ever unsure about our instructions, you should contact us to seek clarification or further instructions as soon as possible.

3 Compliance with Data Protection Legislation

You represent and warrant that you shall:

a. Process all Upfield Personal Data in accordance with applicable Data Protection Legislation and notify us promptly, without undue delay, if in the performance of the Services (as an experienced supplier of such services), you identify any potential areas of actual or potential non-compliance with the Data Protection Legislation;

b. not without our prior written consent (a) convert any Upfield Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data; (b) use any Upfield Personal Data for "big data" analysis or purposes; or (c) match any Upfield Personal Data with or against any other Personal Data (whether yours or any third party's);

c. take no action (or omit to take any action) with Upfield Personal Data which would (a) put us in breach of our obligations under Data Protection Legislation or (b) impact the confidentiality, integrity and availability of systems used to Process Upfield Personal Data; and

d. not use Personal Data forming part of the Upfield Personal Data for any purpose which may be inconsistent with those notified to the Data Subjects on or before the time of collection, such notification to be made by you on our behalf (and we will provide you with the wording to be used).

4 Co-operation

You shall co-operate and assist us (at no charge) with any (a) privacy impact assessments and (b) consultations with and/or notifications to relevant regulators that we consider are relevant under Data Protection Legislation. We shall provide reasonable notice to you in advance of any of the above.

5 Your personnel and contractors

a. You shall ensure that your personnel are contractually obligated to maintain the security and confidentiality of any Upfield Personal Data as set out in this addendum, or are otherwise subject to statutory obligations of confidentiality to the same extent.

b. You shall ensure that only your personnel (including contractors) who are required to have access to Upfield Personal Data shall have such access. You will ensure that all such personnel (including contractors) are aware of the Data Protection Legislation, our obligations under it and have received suitable training in the care and handling of any Upfield Personal Data.

6 Data subject rights

You shall promptly forward to us and otherwise co-operate with and assist us (at no charge) including by way of appropriate technical and organisational measures with any requests from data subjects (and other third party requests, including from any national regulator) of any Upfield Personal Data pursuant to Data Protection Legislation (including the ability to correct, delete, block or port Upfield Personal Data and rights of access and disclosure).

7 Deletion or return of Upfield Personal Data

You shall either delete (if permitted by local laws) or return all copies of Upfield Personal Data and cease Processing such Upfield Personal Data the earlier of (a) after the business purposes for which the

Upfield Personal Data was Processed have been completed, (b) the termination of the Agreement or (c) upon our written request.

8 Records

You shall maintain a record of all categories of Processing activities carried out on behalf of Upfield which shall be made available to us upon request.

9 Security

You have implemented and will maintain appropriate technical and organisational measures, internal controls and information security routines intended to protect Upfield Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction to ensure a level of security appropriate to the risk presented by Processing Upfield Personal Data. These shall at all times:

a. be of at least the minimum standard required by Data Protection Legislation and/or those security standards required by us from time to time and no less protective than the measures set out in Annex A; and
b. be of a standard compliant with good industry practice for the protection of Personal Data.

10 Notification of incidents

If you become aware of (or reasonably suspect) that any Security Incident has occurred, you will without undue delay (and in any event within twenty-four (24) hours):

a. notify us of the Security Incident, provide us as much information as possible and regularly update the content of the information without undue delay. Neither you or any Authorised Sub-Processor (as defined below) may (a) delay notifying us on the basis that an investigation is incomplete or ongoing and (b) not make or permit any announcement to any party (other than a national regulator), without our consent (which may be subject to conditions at the our sole discretion);
b. investigate the Security Incident (including interviewing personnel) and provide us with detailed information about the Security Incident including making available a senior, appropriately qualified individual to discuss any concerns or questions we may have;
c. take reasonable steps to (a) mitigate the effects and minimise any damage resulting from the Security Incident and assist us in remediating or mitigating any potential damage (including reputational damage) from a Security Incident to the extent that such remediation or mitigation is within your control and (b) prevent a recurrence of such Security Incident, including interviewing and the possible removal of personnel from the performance of the Services;
d. fully cooperate with us in respect of any Security Incident, including to develop and execute a response plan. You shall at our request co-operate in adequately informing any national regulator or individuals involved as we may direct; and
e. provide us with reasonable co-operation taking measure(s) to record, report and address the Security Incident, including implementing measures to mitigate its possible adverse effects.

11 Sub-Processing

a. You shall not engage, use or permit any third party to Process Upfield Personal Data without our prior written consent (which may be withheld or subject to conditions at our discretion). If we have consented, to the use of such third parties (known as an "Authorised Sub-Processor") for the Processing of Upfield Personal Data, you shall include in any contracts with an Authorised Sub-Processors who will process Personal Data directly or indirectly on our behalf, provisions in our favour which are equivalent to those in this addendum.
b. You shall remain fully liable to us for the performance of each Authorised Sub-Processor, as well as for any acts or omissions of each Authorised Sub-Processor in regard of its Processing of Upfield Personal Data.
c. You shall (a) provide details of any Authorised Sub-Processor upon request and (b) notify us of any proposed sub-contractor, in advance of requesting the consent referred to above. You shall provide copies of documentation to evidence your compliance with above upon our request.

12 Transfer of Data

a. You shall not permit any Processing of Upfield Personal Data outside the European Economic Area without our prior written consent (which may be subject to conditions including requirements to execute Model Clauses or confirmation of certification under the Privacy Shield framework in the USA) unless you or an Authorised Sub-Processors is required to transfer the Upfield Personal Data in compliance with European Union or European Union Member State laws and such laws prohibit notifying us.

13 Audit

a. You shall make available to us, at our request (at no charge), all information necessary to demonstrate compliance with the obligations set out in this addendum.
b. Upon us giving reasonable written advance notice, you shall permit us (or our representatives subject to reasonable confidentiality undertakings) to conduct periodic security scans and audits of your (or an Authorised Sub-Processor(s)) systems and processes in relation to the Processing of Upfield Personal Data. Such audits shall be at our expense and during normal working hours. You shall comply with all our reasonable requests or directions to verify and/or procure that you are in full compliance with your obligations under this addendum. You shall promptly resolve, at your own expense, all security issues discovered by us and reported to you.

14 Liability

Notwithstanding any other right or remedy which we may have in the event of a breach of this addendum under the Agreement (or any other contractual relationship), you agree to i) indemnify us (and keep us indemnified) and ii) defend us at your expense against all costs, claims, damages or expenses for which we may incur or become liable due to any failure by you (or an Authorised Sub-Processor) or your personnel or contractors to comply with any of the obligations under this addendum.

15 General

a. This addendum shall supersede any similar provisions contained in the Agreement unless the existing provisions are more restrictive and in the event of a conflict, shall take precedence in so far as the subject matter relates to the Processing of Personal Data. This addendum is governed by the laws of England and Wales and both we and you agree to the exclusive jurisdiction of the English courts.

Annex A – Security Standards

1. Organizational security controls

1.1 You must have in place a formal information security program with clearly defined information security roles, responsibilities and accountability.

1.2 You shall process Upfield Personal Data, and access and use Upfield Information Systems, only on a need-to know basis.

1.3 You must ensure that the Data Processor Personnel are background check cleared and have participated in appropriate information security awareness training prior to processing any Upfield Personal Data.

1.4 You must ensure any account through which Upfield Personal Data may be accessed is attributable to a single individual with a unique ID (not shared) and each account must require authentication (e.g., password) prior to accessing Upfield Personal Data.

1.5 You must undertake reasonable measures to terminate Data Processor Personnel's physical and logical access to Upfield Personal Data no later than the date of separation or transfer to a role no longer requiring access to Upfield Personal Data. You shall also notify Upfield of any separation or transfer of Data Processor Personnel with Upfield SSO credentials no later than the day of that event.

1.6 Upfield Personal Data shall not be processed on personal accounts or on personally owned computers, devices or media.

2. Technical security controls

2.1 You must use strong passwords, including requirements for minimum password length, lockout, expiration period, complexity, encryption, changing of default passwords, and usage of temporary passwords. User account credentials (e.g., login ID, password) must not be shared.

2.2 You must ensure that:

2.2.1 Your Data Processor Information Systems have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk-based manner, client and server-side antivirus programs that include up-to-date antivirus definitions, and installation into production of all critical patches or security updates within thirty (30) days from the release of any such updates or patches.

2.2.2 Change management process is documented & implemented and includes key controls like segregation of duties.

2.2.3 Any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing Upfield Personal Data must be encrypted at rest. Encryption also must be employed when transferring Upfield Personal Data over public networks/Internet.

2.2.4 Development and testing environments must be physically and/or logically separated from production environments and must not contain Upfield data.

2.2.5 An inactivity lock must be implemented on workstations when left unattended and a password or PIN must be required to enable access.

2.2.6 Mobile devices used to process Upfield Personal Data (including emails) must have centrally-managed security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

3. Physical security controls

3.1 Your locations where Upfield Personal Data is processed must be limited to Data Processor Personnel and authorized visitors. Visitor management process should be in place that requires visitors to wear an ID badge.

3.2 Reception areas must be manned or have other means to control physical access.

3.3 Documents that contain Upfield Personal Data must be kept secured when not in use.

3.4 Any back-up media containing Upfield Personal Data stored at your sites must be kept in a secure location with restricted physical access and be encrypted. If off-site media storage is used, you must have a media check-in/check-out process with locked storage for transportation.

4. Audits

4.1 You must conduct periodic security risk assessments of Data Processor Information Systems that are used to process or store Upfield Personal Data.

4.2 You must use commercially reasonable efforts to remediate within thirty (30) days any items rated as high or critical (or similar rating) in any audits or assessments of Data Processor Information Systems.

5. Disaster Recovery

5.1 You must maintain a Disaster Recovery (DR) program for all Data Processor Information Systems and facilities used to provide services to Upfield. The DR program must be designed to ensure that you have a methodology by which a system can continue to function through an operational interruption or disaster. The DR program shall include controls for backup media management, DR testing and power back-ups.

6. Other

6.1 You must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.

6.2 You must perform or have an independent third party perform vulnerability assessments on Data Processor Information Systems annually and remediate.

6.3 Any Data Processor Personnel accessing your internal or hosted network remotely must be authenticated using two-factor authentication method and such transmissions must be encrypted at a level consistent with industry standards.

6.4 You must implement a device hardening and configuration standard.

6.5 You must implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of Upfield Personal Data from Data Processor Information Systems.

6.6 You must implement processes to support the secure creation, modification, and deletion of HPAs. All HPA access must be established using encrypted mechanisms (e.g., secure shell).

6.7 You must review and update HPA access rights quarterly.

6.8 Data Processor Information Systems consisting of servers and/or network equipment used to store or access Upfield Personal Data must be kept in a secure room with enhanced logical and physical access controls. Physical access must be monitored, recorded and controlled with physical access rights reviewed annually.

6.9 Physical access logs detailing access must be stored for six (6) months unless prohibited by local law.