**DATA PROCESSING AGREEMENT**

**THIS AGREEMENT** is made the day of [\_\_\_\_\_\_\_\_]

**BETWEEN:-**

1. PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], a company with registered office at [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ("PPG"); and

2. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], a company with registered office at [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ("Supplier").

**BACKGROUND**

(A) Pursuant to a supplier contract between PPG and the Supplier (together “the Parties”) dated [\_\_\_\_\_\_\_\_\_\_\_] (Supply Contract), the Supplier has agreed to provide the services detailed therein (“Services”) which may involve the transfer or sharing of personal data by PPG to the Supplier.

(B) The Parties agree that the terms of this agreement shall be incorporated into and form part of the terms and conditions of the Supply Contract. To the extent that any of the terms of this agreement conflict with any of the terms and conditions of the Supply Contract, the terms of this Agreement shall prevail.

**IT IS AGREED THAT:**

1. Definitions and clauses

In this agreement the following expressions bear the following meanings unless the context otherwise requires:

|  |  |
| --- | --- |
| 1. **“Agreement Personal Data”**
 | 1. Personal Data which is to be Processed under this Agreement, as more particularly described in **SCHEDULE 1**
 |
| 1. **"Affiliate"**
 | 1. in relation to any person, any entity that controls, is controlled by or is under common control with, that person, whether directly or indirectly, through one or more intermediaries. For the purposes of this definition, “control’ (including the terms “controlled by” and “under common control with”), as used with respect to any person, means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of said person, whether through the ownership of voting securities, as trustee or executor, by contract or credit arrangement or otherwise
 |
| 1. **“Data Protection Laws”**
 | 1. all applicable laws relating to data protection, the processing of personal data and privacy, including without limitation:
	1. the General Data Protection Regulation (EU) 2016/679;
	2. the UK Data Protection Act and the General Data Protection Regulation as made applicable in the UK by the UK European Union (Withdrawal) Act; and
	3. the Swiss Federal Data Protection Act;
2. and any legislation and regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them
3. and references to **“Data Processor”, “Data Subjects”**, **“Personal Data”**, **“Process”**, **“Processed”**, **“Processing”**, **“Processor”** and **“Supervisory Authority”** have the meanings set out in, and will be interpreted in accordance with, such applicable laws
 |
| 1. **“Data Security Incident”**
 | * 1. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed; or
	2. a discovery or reasonable suspicion that there is a vulnerability in any technological measure used to protect any Agreement Personal Data that has previously been subject to a breach within the scope of (a), which may result in exploitation or exposure of that Agreement Personal Data; or
	3. any defect or vulnerability with the potential to impact the ongoing resilience, security and/or integrity of systems Processing Agreement Personal Data
 |
| 1. **“International Transfer”**
 | 1. a transfer to a country outside the United Kingdom, Switzerland or the European Economic Area of Agreement Personal Data which is undergoing Processing or which is intended to be Processed after transfer
 |
| 1. **“Sub-Processor”**
 | 1. any third party Processor appointed by the Supplier to Process Agreement Personal Data
 |

1. DATA PROTECTION AND INFORMATION SECURITY
2. **AUTHORISATION AND COMPLIANCE WITH LAWS**
	1. PPG authorises the Supplier, on its own behalf and on behalf of PPG's Affiliates, to Process the Agreement Personal Data during the term of this Agreement as a Data Processor solely for the purpose and to the extent described in **SCHEDULE 1**.
	2. In performing the Services and its other obligations under this Agreement the Supplier will:
		1. comply with the Data Protection Laws; and
		2. not cause PPG or any PPG Affiliate to breach any obligation under the Data Protection Laws.
3. **PROCESSING OF AGREEMENT PERSONAL DATA**

The Supplier will:

* + 1. Process the Agreement Personal Data only on documented instructions from PPG (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise agreed between the parties from time to time) or the relevant PPG Affiliate unless the Supplier or the relevant Sub-Processor is required to Process Agreement Personal Data to comply with applicable laws to which the Supplier is subject, in which case the Supplier will notify PPG of such legal requirement prior to such Processing unless such applicable laws prohibit notice to PPG on public interest grounds;
		2. immediately inform PPG if, in its reasonable opinion, any instruction received from PPG or PPG Affiliate infringes any Data Protection Laws, it being acknowledged that the Supplier shall not be obliged to undertake additional work or screening to determine if PPG's instructions are compliant;
		3. without prejudice to clause **2.1.1,** ensure that Agreement Personal Data will only be used for the purpose and to the extent described in **SCHEDULE 1**;
		4. without prejudice to clause 2.1.3, not without the prior written consent of PPG or the relevant member of its Group:
			1. convert any Agreement Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data;
			2. use any Agreement Personal Data for “big data” analysis or purposes; or
			3. match or compare any Agreement Personal Data with or against any other Personal Data (whether the Supplier’s or any third party’s);
		5. ensure that any individual authorised to Process Agreement Personal Data accesses such Agreement Personal Data strictly on a need to know basis as necessary to perform their role in the performance of this Agreement, and:
			1. is subject to binding confidentiality obligations in respect of Agreement Personal Data or is under an appropriate statutory obligation of confidentiality;
			2. complies with this clause B; and
			3. is appropriately reliable, qualified and trained in relation to their responsibilities for Processing of Agreement Personal Data; and
		6. at the option of PPG, securely delete or return to PPG (in the format required by PPG) all Agreement Personal Data promptly after the end of the provision of Services relating to Processing or at any time upon request, and securely delete any remaining copies and promptly certify when this exercise has been completed, unless applicable laws require storage by the Supplier of Agreement Personal Data.
1. **SECURITY MEASURES AND INCIDENTS**
	1. The Supplier will:
		1. implement, and assist PPG and the other members of its Group to implement, appropriate technical and organisational measures at a minimum to the standard set out in Schedule 2 to ensure a level of security appropriate to the risk presented by Processing the Agreement Personal Data, in particular from a Data Security Incident;
		2. notify PPG without undue delay after becoming aware of a reasonably suspected or actual Data Security Incident, including without limitation the nature of the Data Security Incident, the categories and approximate number of Data Subjects and Agreement Personal Data records concerned, the likely consequences of the Data Security Incident and any measure proposed to be taken to address the Data Security Incident and to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue delay, but the Supplier (and Sub-Processors) may not delay notification under this clause 3.1.2 on the basis that an investigation is incomplete or ongoing;
		3. notify PPG immediately if at any time the Supplier or a Sub-Processor is, or ought to be, aware of any reason why it is unable to comply with **clause 3.1.1,** without prejudice to its obligation to comply with,or to any rights or remedies which PPG may have for breach of **clause** **3.1.1**;
		4. promptly (and in any event within 72 hours) notify PPG of any request that it receives for exercise of a Data Subject’s rights under the Data Protection Laws or communication or complaint that it receives from a Data Subject or Supervisory Authority or other third party in connection with Agreement Personal Data; and
		5. not, without PPG’s prior written consent, make or permit any announcement in respect of a Data Security Incident or respond to any request for exercise of a Data Subject’s rights under the Data Protection Laws or communication or complaint from a Data Subject or Supervisory Authority in connection with Agreement Personal Data (except where required to do so by applicable law).
2. **SUPPLIER ASSISTANCE**
	1. Supplier will assist/provide reasonable assistance to PPG and PPG’s Affiliates in:
		1. responding to requests for exercising Data Subjects’ rights under the Data Protection Laws and communications and complaints from Data Subjects and Supervisory Authorities and other third parties in connection with Agreement Personal Data, including without limitation by appropriate technical and organisational measures, insofar as this is possible;
		2. documenting any Data Security Incidents and reporting any Data Security Incidents to any Supervisory Authority and/or Data Subjects;
		3. conducting privacy impact assessments of any Processing operations and consulting with Supervisory Authorities, Data Subjects and their representatives accordingly; and
		4. taking measures to address Data Security Incidents, including without limitation, where appropriate, measures to mitigate their possible adverse effects.
3. **APPOINTMENT OF SUB-PROCESSORS**
	1. PPG agrees that the Supplier may engage Sub-Processors for the purposes of Processing Agreement Personal Data, provided that:
		1. the Supplier shall only engage Sub-Processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that Processing is done in accordance with this Agreement and PPG's, and Sub-Processor's, obligations under Data Protection Laws; and
		2. the Supplier may at any time appoint a new Sub-Processor provided that PPG is given 15 working days prior notice and PPG does not object to such changes within that timeframe. If PPG objects to the appointment of a new Sub-Processor within such period, PPG may, by providing written notice to Supplier, terminate the Service which cannot be provided by Supplier without the use of the objected-to Sub-Processor.
	2. If the Supplier engages a Sub-Processor to perform any part of the Services involving the Processing of Agreement Personal Data, the Supplier will ensure that, prior to the Processing taking place, there is a written contract in place between the Supplier and the Sub-Processor that specifies the Sub-Processor’s Processing activities and imposes on the Sub-Processor the equivalent terms as those imposed on the Supplier in this clause **B**. The Supplier will procure that Sub-Processors will perform all obligations set out in this clause **B** and the Supplier will remain responsible and liable to PPG and PPG Affiliates for all acts and omissions of Sub-Processors as if they were its own.
	3. The Supplier shall maintain a list of Sub-Processors and shall promptly provide this to PPG on request.
4. **INTERNATIONAL TRANSFERS**
	1. The Supplier will not make an International Transfer without PPG’s prior written consent. If PPG gives its prior written consent to an International Transfer, before making that International Transfer the Supplier will demonstrate or implement, to PPG’s satisfaction, appropriate safeguards for that International Transfer in accordance with Data Protection Laws and will ensure that enforceable rights and effective legal remedies for Data Subjects are available. Such appropriate safeguards may include without limitation:
		1. the country or territory to which the International Transfer is to be made is subject to a valid adequacy decision issued by the European Commission or adequacy is determined by another valid method under applicable Data Protection Laws;
		2. the Supplier agrees to comply with the obligations of a data importer as set out in the Standard Contractual Clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU (the "**Standard Contractual Clauses**"). The Supplier acknowledges that PPG and PPG Affiliates identified by PPG will be a data exporter. In particular, and without limiting the above obligation:
			1. the Supplier agrees to grant third party beneficiary rights to Data Subjects as set out in clause 3 of the Standard Contractual Clauses, provided that the Supplier's liability shall be limited to the Supplier's own processing operations;
			2. the Supplier agrees that the Supplier's obligations under the Standard Contractual Clauses shall be governed by the law(s) of the Member State(s) in which PPG or PPG Affiliate that is the data exporter is established;
			3. the parties agree that for the purposes of clause 5(h) and 11 of the Standard Contractual Clauses, PPG consents to the Supplier subcontracting operations in accordance with the provisions set out in **clause 2** of this Agreement;
			4. the parties agree that any rights to audit, pursuant to clauses 5(f) and 12(2) of the Standard Contractual Clauses, will be exercised in accordance with **clause 7** of this Agreement. The parties agree that in the event of any conflict between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail; and
			5. the details of the appendices applicable to the Standard Contractual Clauses are as set out in **SCHEDULE 1** and the security measures required are as set out in **SCHEDULE 2**;
		3. the International Transfer is to the United States of America and the Supplier or Sub-Processor, as relevant, has and maintains for the duration of the Processing a current registration under the US-EU Privacy Shield. Where this **clause 6.1.3** applies, the Supplier will promptly notify PPG in writing it the Supplier or the Sub-Processor, as relevant, ceases to maintain, or anticipates the revocation or withdrawal, or is otherwise challenged by any regulatory authority as to the status of, or makes a determination itself that the Supplier or Sub-Processor, as relevant, can no longer meet the obligations under the Privacy Shield; or
		4. the Supplier or Sub-Processor, as relevant, confirms that all of the Processing of Agreement Personal Data is covered by the Supplier's or Sub-Processor's binding corporate rules, the terms of which are incorporated into these terms. The Supplier agrees that PPG, as data controller, has the right to enforce these binding corporate rules against the Supplier or Sub-Processor, as relevant, including a right to compensation in the event that the rules are breached.
	2. If the appropriate safeguards demonstrated or implemented by the Supplier in accordance with this clause 6 are deemed at any time not to provide an adequate level of protection in relation to Agreement Personal Data, the Supplier will implement such alternative measures as may be required by PPG or by the PPG Affiliate to ensure that the relevant International Transfer and all resulting Processing are compliant with Data Protection Laws. The Supplier or the relevant Sub-Processor will not need to comply with the conditions set out in this clause 6 if it is required to make an International Transfer to comply with United Kingdom, Swiss or European Union or European Union member state applicable laws, provided however that the Supplier will notify PPG of such legal requirement prior to such International Transfer unless applicable law prohibits notice to PPG on public interest grounds.
5. **AUDIT RIGHTS**
	1. The Supplier will:
		1. make available to PPG and PPG Affiliates all information necessary to demonstrate compliance with applicable Data Protection Laws and the obligations set out in this **clause** B; and
		2. allow for and contribute to audits, including without limitation inspections, conducted by PPG or another auditor mandated by PPG.
6. **INDEMNIFICATION**
	1. The Supplier will indemnify PPG and PPG Affiliates against any damages of and/or fines imposed against PPG and PPG Affiliates, in each case arising out of or in connection with any breach by the Supplier or any Sub-Processor of any of its obligations under this clause B (including without limitation any failure or delay in performing, or negligent performance or non-performance of, any of those obligations).
	2. Any breach of this clause B by the Supplier or any Sub-Processor will be a material breach of this Agreement which is not capable of being remedied, irrespective of whether any financial loss or reputational damage arises, and irrespective of the level of any financial loss or deprivation of benefit arising, as a consequence of such breach.

|  |  |
| --- | --- |
| Signed by PPG [ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] …………………………………………..Signature…………………………………………..NameDirector | Signed by [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ………………………………………Signature ………………………………………NameDirector |

|  |
| --- |
| 1. SCHEDULE 1
 |
| 1. **Subject matter of Processing**
 | [DETAILS] |
| 1. **Duration of Processing**
 | [DETAILS] |
| 1. **Nature of Processing**
 | [DETAILS] |
| 1. **Purpose of Processing**
 | [DETAILS] |
| 1. **Type of Personal Data**
 | [DETAILS] |
| 1. **Categories of Data Subject**
 | [DETAILS] |

|  |
| --- |
| 1. SCHEDULE 2
2. SECURITY MEASURES
 |
| 1. **Physical Access Control:**

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which Process Agreement Personal Data ("**Data Centres**").Measures:**Data Centres** shall adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and **Data Centre** facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the **Data Centre** facilities. To ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at the **Data Centres**:* The Supplier protects its assets and facilities using the appropriate means based on a internal security classification.
* In general, buildings are secured through access control systems (smart card access system).
* As a minimum requirement, the outermost shell of the building must be fitted with a certified key system including modern, active key management.
* Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance and intruder alarm systems.
* Access rights will be granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 2 and 3 below). This also applies to visitor access. Guests and visitors to the Supplier's building must register their names at reception and must be accompanied by authorized personnel.
* The Supplier's employees and external personnel must wear their ID cards at all PPG and Supplier locations.
 |
| 1. **System Access Control:**

Data processing systems must be prevented from being used without authorization.Measures:* Multiple authorization levels are used to grant access to sensitive systems including those storing and processing Agreement Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
* All users access the Supplier systems with a unique identifier (user ID).
* The Supplier has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the Supplier, its access rights are revoked.
* The Supplier has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every six months complying with the requirements for complex passwords. Each computer has a password-protected screensaver.
* The Supplier corporate network is protected from the public network by firewalls.
* The Supplier uses up–to-date antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.
* A security patch management is implemented to ensure deployment of relevant security updates.
* Full remote access to the Supplier's corporate network and critical infrastructure is protected by strong authentication.
 |
| 1. **Data Access Control:**

Persons entitled to use data processing systems shall gain access only to the Agreement Personal Data that they have a right to access, and Agreement Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.Measures:* Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. The Supplier uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the Supplier security policies and standards.
* All production servers of any Supplier service are operated in the relevant Data Centres. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, the Supplier conducts internal and external security checks and penetration tests on the IT systems.#
* The Supplier does not allow the installation of personal software or other software not approved by the Supplier to systems being used for any IT Service.
* A Supplier security standard governs how data and data carriers are deleted or destroyed.
 |
| 1. **Data Transmission Control:**

Agreement Personal Data must not be read, copied, modified or removed without authorization during transfer.Measures:* Where data carriers are physically transported, adequate measures are implemented at the Supplier to ensure the agreed service levels (for example, encryption).
* Agreement Personal Data transferred over the Supplier internal networks are protected as any other confidential data according to the Supplier's security policy.
* When the data is being transferred between the Supplier and PPG, all data are encrypted.
 |
| 1. **Data Input Control:**
* It shall be possible to retrospectively examine and establish whether and by whom at the Supplier Agreement Personal Data have been entered, modified or removed from data processing systems.
* The Supplier only allows authorized persons to access Agreement Personal Data as required in the course of their work.
* The Supplier has implemented a logging system for input, modification and deletion.
 |
| 1. **Job Control:**

Agreement Personal Data being Processed on commission shall be processed solely in accordance with the Agreement and related instructions of PPG.Measures:* The Supplier uses controls and processes to ensure compliance with contracts between the Supplier and its customers, Sub-Processors or other service providers.
* As part of the Supplier's security policy, Agreement Personal Data requires at least the same protection level as “confidential” information according to the Supplier's information classification standard.
 |
| 1. **Availability Control:**

Agreement Personal Data shall be protected against a Data Security Incident.Measures:* The Supplier employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
* The Supplier uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centre.
* The Supplier has defined contingency plans as well as business and disaster recovery strategies for cloud services.
* Emergency processes and systems are regularly tested.
 |
| 1. **Data Separation Control:**

Agreement Personal Data is not Processed or stored with Personal Data belonging to another Supplier client.Measures:* The Supplier uses the technical capabilities of the deployed software (for example: multi-tenancy or separate systems) to achieve data separation between Agreement Personal Data from other data.
* The Supplier maintains, when possible dedicated instances for each data processing.
 |
| 1. **Data Integrity Control:**

Ensures that Agreement Personal Data will remain intact, complete and current during processing activities:Measures:The Supplier has implemented a defence strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above. In particular:* Firewalls;
* Security Monitoring Centre;
* Antivirus software;
* Backup and recovery;
* External and internal penetration testing;
* Regular external audits to prove security measures.
 |