**PERSONAL DATA PROCESSING EXHIBIT**

**THIS EXHIBIT** is made the day of [\_\_\_\_\_\_\_\_] between PPG [\_\_\_\_\_\_], a company with registered office at [\_\_\_\_\_\_] ("PPG"); and [\_\_\_\_\_\_\_\_], a company with registered office at [\_\_\_\_\_\_] ("Supplier").

**BACKGROUND**

(A) Pursuant to a supplier contract between PPG and the Supplier (together “the Parties”) (‘Agreement’), 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 exhibit shall be incorporated into and form part of the terms and conditions of the Agreement. To the extent that any of the terms of this agreement conflict with any of the terms and conditions of the Agreement, the terms of this exhibit shall prevail.

**IT IS AGREED THAT:**

1. **DEFINITIONS**

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

**“Agreement Personal Data”** means personal data listed in **SCHEDULE 1.**

1. **“Data Privacy Laws”** all applicable laws relating to data privacy or data security, the processing of personal data, including without limitation (i) the General Data Protection Regulation (EU) 2016/679 (GDPR), (ii) the UK GDPR and Data Protection Act 2018, (iii) state and federal US privacy laws; (iv) China Personal Information Protection Law (PIPL); (v) the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA); (vi) the General Data Protection Law (LGPD); and any legislation and regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them. References to **“Data Processor”, “Data Subjects”**, **“Personal Data”**, **“Process”**, **“Processed”**, **“Processing”**, **“Processor”** and **“Supervisory Authority”, “Sell” or “Sale”** have the meanings set out in and will be interpreted in accordance with such applicable laws.

**“Data Incident”** means (i) any breach of security and/or confidentiality leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data or any indication that of such breach having taken place or being about to take place (ii), a complaint or a request with respect to the exercise of a data subject’s rights or (iii) an investigation into or seizure of the Agreement Personal Data by government officials; or (iv) any defect or vulnerability with the potential to impact the ongoing resilience, security and/or integrity of systems Processing Agreement Personal Data; or (v) where, in the opinion of the Supplier, implementing an instruction received from PPG would violate Data Privacy Laws.

1. **“International Transfer”** means a transfer of Agreement Personal Data from one country or territory to another country or territory to which such transfer is prohibited or subject to any requirement to take additional steps to adequately protect personal data.
2. **“Sub-Processor”** means any third-party Processor appointed by the Supplier to Process Agreement Personal Data.
3. **AUTHORISATION AND COMPLIANCE WITH LAWS**
	1. **Authorisation and purpose limitation.** 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 the Agreement. Without prejudice to clause **3,** Agreement Personal Data will only be used for the purpose and to the extent described in **SCHEDULE 1**.
	2. **Compliance with laws.** In performing the Services and its other obligations under this Agreement the Supplier, Supplier’s affiliates and any Sub-Processors will comply with the Data Privacy Laws, including additional privacy provisions as set forth in **SCHEDULE 3**, if applicable,and not cause PPG or any PPG affiliate to breach any obligation under the Data Privacy Laws**.** To the extent there is any conflict between the provisions in SCHEDULE 3 and any other terms in this exhibit, the provisions of SCHEDULE 3 will prevail.
4. **DATA PROCESSING**
	1. **Instructions.** Supplier will 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 EU/UK Data Privacy 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. **Sale.** Supplier, Supplier affiliates or any Sub-Processors will not Sell Agreement Personal Data.
	3. **Confidentiality.** Supplier will 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 the Agreement and subject to binding confidentiality obligations in respect of Agreement Personal Data or is under an appropriate statutory obligation of confidentiality. Supplier guarantees that all of its and its affiliates’ staff are qualified and trained in relation to their responsibilities for Processing of Agreement Personal Data.
	4. **Retention.** At the option of PPG or PPG’s affiliates, Supplier shall securely delete or return to PPG or to PPG’s affiliates all Agreement Personal Data promptly after the end of the provision of Services relating to Processing and securely delete any remaining copies and promptly certify when this exercise has been completed, unless EU/UK applicable laws require storage by the Supplier of Agreement Personal Data.
5. **SECURITY MEASURES AND INCIDENTS**
	1. **Appropriate Security.** Supplier will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by Processing the Agreement Personal Data. These measures shall include at a minimum the measures set out in **SCHEDULE 2**.
	2. **Data Incident Notification.** Supplier will notify PPG without undue delay after becoming aware of a suspected or actual Data Incident. Such notification shall include, without limitation, the nature of the Data Incident, the categories and approximate number of Data Subjects and Agreement Personal Data records concerned, the likely consequences of the Data Incident and any measure proposed to be taken to address the Data Incident and to mitigate its possible adverse effects. Where 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 on the basis that an investigation is incomplete or ongoing.
	3. **Third Party Communication.** Supplier will not, without PPG’s prior written consent, make or permit any announcement in respect of a Data Incident or respond to any request for exercise of a Data Subject’s rights 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).
6. **SUPPLIER ASSISTANCE**
	1. **Data Incidents.** Supplier, Supplier’s affiliates and any Sub-Processors shall assist PPG and PPG’s affiliates taking measures to address any Data Incidents, including mitigation of their adverse effects, and assist in reporting any such incidents to a supervisory authority and/or Data Subjects.
	2. **Requests.** Supplier shall inform without undue delay and provide assistance to PPG and PPG affiliates in responding to requests for exercising Data Subjects’ rights, supervisory authorities and third parties in connection with Agreement Personal Data.
7. **APPOINTMENT OF SUB-PROCESSORS**
	1. **Authorisation to use sub-processors.** Subject to Clause 1.3 of Schedule 3 in case appointment of a sub-processor means international transfer of Agreement Personal Data, PPG agrees that the Supplier may engage the Sub-Processors for the purposes of Processing Agreement Personal.
	2. **Sufficient Guarantees.** 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 exhibit and PPG's obligations under Data Privacy Laws.
	3. **Sub-processor contract.** 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 same terms as those imposed on the Supplier in this exhibit. The Supplier will procure that Sub-Processors will perform all obligations set out in this exhibit 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.
8. **INTERNATIONAL TRANSFERS**
	1. **Authorisation to transfer.** Subject to additional privacy provisions in Schedule 3, PPG hereby authorises Supplier and its Sub-Processors to realize International Transfer of Agreement Personal Data, provided that the Supplier ensures such transfers comply with Applicable Data Privacy Laws. Without prejudice to the general authorization to transfer, the Supplier will inform and keep PPG updated of the countries to which the International Transfer is to be made.
	2. **Legal obligation to transfer.** The Supplier or the relevant Sub-Processor will not need to comply with the conditions set out in this exhibit, if it is required to make an International Transfer to comply with the Supplier’s legal obligations, provided however that the Supplier will notify PPG of such legal requirement prior to such International Transfer unless EU/UK applicable law prohibits notice to PPG on public interest grounds.
9. **AUDIT RIGHTS**
	1. **Provision of information.** The Supplier will make available to PPG and PPG affiliates all information necessary to demonstrate compliance with applicable Data Privacy Laws and the obligations set out in this exhibit.
	2. **Cooperation.** The Supplier will allow for and contribute to audits, including without limitation inspections, conducted by PPG or another auditor mandated by PPG.
10. **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, the Supplier’s affiliates or any Sub-Processor of any of its obligations under this exhibit.
	2. Any breach of this exhibit by the Supplier or any Sub-Processor will be a material breach of the 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 Supplier ………………………………………….Signature …………………………………………..NameDirector |

|  |
| --- |
| 1. SCHEDULE 1
 |
| 1. **Subject matter of Processing**
 | The subject matter of the processing under the Agreement is Agreement Personal Data. |
| 1. **Nature of Processing**
 | Supplier and its Sub-Processors are providing Services or fulfilling contractual obligations to PPG as set out in the Agreement. These Services may include the processing of Agreement Personal Data by the Supplier and/or its Sub-Processors. |
| 1. **Purpose of Processing**
 | The Agreement Personal Data will be processed only for the purposes of performance of the Services under the Agreement. |
| 1. **Duration of Processing**
 | Duration of the Processing equals the duration of the Agreement. |
| 1. **Type of Personal Data**
 | [DETAILS TO BE COMPLETED BY THE BUSINESS] |
| 1. **Categories of Data Subjects**
 | The categories of Data Subjects whose personal data are Processed are as thoseset out in the Agreement. |
| 1. **Frequency of the transfer**
 | [DETAILS TO BE COMPLETED BY THE BUSINESS] |

|  |
| --- |
| 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 breach of security and/or confidentiality leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data.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.
 |

1. SCHEDULE 3
2. additional privacy provisions
3. **EEA.** To the extent Agreement Personal Data originates in the EEA, the following additional provisions shall apply:
	1. **International Transfers:** If Supplier transfers Agreement Personal Data outside of EEA, the Supplier will take appropriate safeguards before any such transfer is made including ensuring that 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 Privacy Laws.
	2. **2021 Standard Contractual Clauses**. The parties agree that the 2021 Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area, either directly or via onward transfer, to any country or recipient outside the European Economic Area that is not recognized by the European Commission as providing an adequate level of protection for personal data. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this exhibit by this reference) and completed as follows:

|  |
| --- |
| Module Two (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where PPG is a controller and the Supplier is acting as a data processor |
| Clause 7 | The optional docking clause will not apply. |
| Clause 9 | Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 5 (APPOINTMENT OF SUB-PROCESSORS) of this exhibit. |
| Clause 11 | The optional language will not apply |
| Clause 17(Option 1) | French law |
| Clause 18(b) | Disputes will be resolved before the courts of France |
| Annex I, Part A | Data Exporter: PPG.Contact details: PPG privacy team - privacy@ppg.com.Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.Data Importer: The supplier.Contact details: \_\_\_\_\_\_\_\_\_\_\_\_ - \_\_\_\_\_\_\_@\_\_\_\_\_\_  |
| Annex I, Part B | The categories of data subjects are described in Schedule 1 of this exhibit.The Sensitive Data transferred is described in Schedule 1 of this exhibit.The frequency of the transfer is a continuous basis for the duration of the Agreement.The nature of the processing is described in Schedule 1 of this exhibit.The purpose of the processing is described in Section 1 of this exhibit.The period for which the personal data will be retained is described in Schedule 1 (Details of Processing) of this exhibit.For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth at Schedule 1. |
| Annex I, Part C | The Commission Nationale de l'Informatique et des Libertés (CNIL) will be the competent supervisory authority. |
| Annex II | Schedule 2 (Security Measures) of this exhibit serves as Annex II |
| Annex III | Schedule 3 Clause 1.3 (Authorised Sub-processors) of this exhibit serves as Annex III |

* 1. **Authorised Sub-processors.**

|  |  |  |
| --- | --- | --- |
| **Sub-Processor Entity (name and address)** | **Brief Description of Processing and Services to be provided** | **Location of Processing** |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. **Conflict.** To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this exhibit, the provisions of the Standard Contractual Clauses will prevail.
	2. **Binding corporate rules.** In casethe Supplier or Sub-Processor, as relevant, has in place binding corporate rules, it 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.
	3. **Impact Assessments.** Supplier shall assist PPG in conducting privacy impact assessments of any Processing operations and consulting with supervisory authorities, Data Subjects and their representatives accordingly.
1. **UNITED KINGDOM:** To the extent Agreement Personal Data originates in the UK, the following additional provisions shall apply:
	1. **UK Standard Contractual Clauses.** The parties agree that template Addendum B.1.0 issued by the United Kingdom Information Commissioner’s Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it may be revised under Section 18 thereof (the “**UK Addendum**”) will apply to personal data that is transferred from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK Addendum, the UK Addendum will be deemed entered into and appended to the EU Standard Contractual Clauses (and incorporated into this exhibit by this reference) and completed as indicated in Clause 2.2 of this **Schedule 3**.
	2. As permitted by clause 17 of the UK Addendum, the Parties agree to change the format of the information set out in Part 1 of the UK Addendum so that:
		1. the details of the parties in table 1 and table 2 shall be as set out in Schedule 1 (with no requirement for signature);
		2. for the purposes of table 2, the UK Addendum shall be appended to the EU Standard Contractual Clauses (including the selection of modules and options and the disapplication of optional clauses as noted above in clause 1.2 of this Schedule 3);
		3. the appendix information listed in table 3 is set out in Schedules 1 and 2 of this Agreement; and
		4. neither the data exporter or data importer party can terminate the UK Addendum as per table 4 of the UK Addendum.
2. **CHINA:** To the extent Agreement Personal Data originates in the People’s Republic of China (“China” or “PRC”), the following additional provisions apply:
	1. **Definitions.** For the purposes of this exhibit, any references to “Personal Data”, “Control/Controller”, “Processor” and “Data Subject” shall have the same meaning as “Personal Information”, “Process/Personal Information Processor”, “Entrusted Party”, and “Personal Information Subject” as defined in the PIPL and other PRC laws as applicable.
	2. **Authorisation to use Entrusted Parties.** PPG agrees that the Supplier may engage Entrusted Parties for the purposes of Processing Agreement Personal Data, subject to PPG’s prior specific written consent. Supplier may not engage any other Entrusted Parties or transfer or disclose any Agreement Personal Data to any Entrusted Party or other party (including Supplier affiliates) without the prior specific written consent of PPG.
	3. **International transfers.** If applicable to the Services, and if a Chinese Supervisory Authority adopts Chinese Standard Contract Clauses (“Chinese SCCs”) in accordance with Article 38 of the PIPL or other applicable PRC laws, and PPG notifies Supplier that it wishes to incorporate such Chinese SCCs into this exhibit, Supplier shall agree to the changes as reasonably required by PPG in order to achieve this. Supplier shall regularly review its internal policies for the international transfer of Agreement Personal Data to assess the suitability of the implemented supplementary measures and identify and implement additional or alternative solutions as necessary to ensure that an adequate level of data protection is maintained.
	4. **Conflict.** To the extent there is any conflict between the Chinese SCCs and any other terms in this exhibit, the provisions of the Chinese SCCs will prevail.
	5. **Personal Information protection/security impact assessments.** Supplier shall assist PPG with data protection and/or security assessments (including the Personal Information Protection Impact Assessment under Article 55 of the PIPL and Security Assessment in relation to international transfers pursuant to Article 38 of the PIPL), in accordance with the PIPL and applicable PRC laws.