|  |  |
| --- | --- |
| **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:** | **AUFTRAGSVERARBEITUNGS-VEREINBARUNG**  **DIESE VEREINBARUNG** wird am [\_\_\_\_\_\_\_\_]  **ZWISCHEN:-**  1. PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], einem Unternehmen mit Sitz in [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] („PPG“); und  2. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], einem Unternehmen mit Sitz in [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] („Lieferant“) geschlossen.  **HINTERGRUND**  (A) Gemäß einem Lieferantenvertrag zwischen PPG und dem Lieferanten (zusammen bezeichnet als „die Parteien“) vom [\_\_\_\_\_\_\_\_\_\_\_] (Liefervertrag), hat der Lieferant zugestimmt, die darin genannten Dienste („Dienste“) auszuführen, die unter Umständen die Übermittlung oder Weitergabe personenbezogener Daten von PPG an den Lieferanten umfassen können.  (B) Die Parteien stimmen zu, dass die Bedingungen dieser Vereinbarung in die Geschäftsbedingungen des Liefervertrags aufgenommen werden und einen Teil davon bilden. Sollten die Bedingungen dieser Vereinbarung in Konflikt mit den Geschäftsbedingungen des Liefervertrags stehen, gelten die Bedingungen dieser Vereinbarung.  **ES WIRD FOLGENDES VEREINBART:** |
| 1. DEFINITIONS AND CLAUSES | 1. Definitionen und Klauseln |
| In this Agreement the following expressions bear the following meanings unless the context otherwise requires: | In dieser Vereinbarung haben die folgenden Ausdrücke folgende Bedeutung, sofern der Kontext nichts anderes erfordert: |
| 1. **"Agreement Personal Data"** 2. Personal Data which is to be Processed under this Agreement, as more particularly described in **SCHEDULE 1** | 1. **„Personenbezogene Daten unter der Vereinbarung“** 2. Die gemäß dieser Vereinbarung zu verarbeitenden personenbezogenen Daten, näher beschrieben in **TABELLE 1.** |
|  |  |
| 1. **"Affiliate"** 2. 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 | **„Verbundenes Unternehmen”**  in Bezug auf jede Person, jedes Unternehmen, welches die betreffende Person kontrolliert, von diesem kontrolliert wird oder sich unter gemeinsamer Kontrolle mit dieser Person befindet, ob direkt oder indirekt oder über einen oder mehrere Vermittler. Im Sinne dieser Definition bedeutet „Kontrolle“ (einschließlich der Begriffe „unter Kontrolle steht“ und „unter gemeinsamer Kontrolle steht mit“), wie sie in Bezug auf jede Person verwendet wird, die direkte oder indirekte Befugnis, die Geschäftsführung und Richtlinien dieser Person zu leiten oder die Leitung zu veranlassen, sei es durch den Besitz an Stimmrechten, als Treuhänder oder Vollstrecker, durch Vertrag oder Kreditvereinbarung oder auf andere Weise. |
| 1. **"Data Protection Laws"** 2. 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; 3. and any legislation and regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them 4. 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 | **„Datenschutzgesetze“**   1. Jedes anwendbare Recht bezüglich des Datenschutzes, der Verarbeitung personenbezogener Daten und Privatsphäre, einschließlich, aber nicht beschränkt auf:    1. die Datenschutz-Grundverordnung (EU) 2016/679;    2. das britische Datenschutzgesetz und die Datenschutz-Grundverordnung, soweit sie im Vereinigten Königreich gemäß dem EU-Austrittsgesetz anwendbar ist; und    3. das Schweizer Bundesgesetz über den Datenschutz (DSG) 2. und alle Gesetze und Verordnungen, die auf deren Grundlage erlassen wurden oder diese umsetzen, abändern, ersetzen, erneuern oder konsolidieren. 3. und Bezugnahmen auf **„Datenverarbeiter“, „betroffene Personen“,**, **„personenbezogene Daten“,**, **„verarbeiten“**, **„verarbeitet“**, **„Verarbeitung“**, **„Auftragsverarbeiter“** und **„Aufsichtsbehörde“** haben die in dem anwendbaren Recht festgelegten Bedeutungen und werden gemäß dem anwendbaren Recht ausgelegt. |
| 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 1, 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 | **„Datensicherheitsvorfall“**   * 1. Ein Sicherheitsverstoß, der zu unbeabsichtigter/m oder unrechtmäßiger/m Vernichtung, Verlust, Veränderung, unbefugter Offenlegung von oder unbefugtem Zugang zu den übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten unter dieser Vereinbarung führt; oder   2. die Entdeckung oder der begründete Verdacht, dass es bei den technologischen Mitteln, mit denen die personenbezogenen Daten unter der Vereinbarung geschützt werden, bei denen es bereits zu einem Sicherheitsverstoß gemäß Nr. 1 gekommen ist, Schwachstellen gibt, was unter Umständen zum Missbrauch oder der Offenlegung dieser personenbezogenen Daten unter der Vereinbarung führen kann; oder   3. alle Mängel und Schwachstellen, welche die durchgängige Widerstandsfähigkeit, Sicherheit und/oder Integrität der Verarbeitungssysteme der personenbezogenen Daten unter der Vereinbarung beeinträchtigen können. |
| 1. **"International Transfer"** 2. 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. **„Internationale Übermittlung“** 2. Eine Übermittlung der personenbezogenen Daten unter der Vereinbarung, welche verarbeitet werden oder nach der Übermittlung verarbeitet werden sollen, in ein Land außerhalb des Vereinigten Königreichs, der Schweiz oder des Europäischen Wirtschaftsraumes. |
| 1. **"Sub-Processor"** 2. any third party Processor appointed by the Supplier to Process Agreement Personal Data | 1. **„Unterauftragsverarbeiter“** 2. Ein vom Lieferanten für die Verarbeitung der personenbezogenen Daten unter der Vereinbarung ernannter Dritter. |
| 1. DATA PROTECTION AND INFORMATION SECURITY | 1. DATENSCHUTZ UND INFORMATIONSSICHERHEIT |
| 1. Authorisation and compliance with laws | 1. Autorisierung und Einhaltung von Gesetzen |
| * 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 Processor solely for the purpose and to the extent described in **SCHEDULE 1**. | * 1. PPG autorisiert den Lieferanten in seinem eigenen Namen und in dem Namen der mit PPG verbundenen Unternehmen, die personenbezogenen Daten unter der Vereinbarung während der Laufzeit dieser Vereinbarung als Auftragsverarbeiter ausschließlich zu dem in **TABELLE 1** beschriebenen Zweck und in dem dort festgelegten Umfang zu verarbeiten |
| * 1. In performing the Services and its other obligations under this Agreement the Supplier will: | * 1. Durch die Erbringung der Dienste und seiner anderen Verpflichtungen gemäß dieser Vereinbarung verpflichtet sich der Lieferant zu folgenden Punkten: |
| * + 1. comply with the Data Protection Laws; and | * + 1. Einhaltung der Datenschutzgesetze; und |
| * + 1. not cause PPG or any PPG Affiliate to breach any obligation under the Data Protection Laws. | * + 1. Keine Veranlassung, PPG oder ein mit PPG verbundenes Unternehmen, eine Verpflichtung gemäß der Datenschutzgesetze zu verletzen. |
| 1. processing of agreement personal data | **2. Verarbeitung der PERSONENBEZOGENEN dAten unter der Vereinbarung** |
| * 1. The Supplier will: | * 1. Der Lieferant wird: |
| 2.1.1 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; | * + 1. die personenbezogenen Daten unter der Vereinbarung nur auf Grundlage dokumentierter Anweisungen von PPG (bei denen es sich um spezifische Anweisungen oder Anweisungen allgemeiner Art handeln kann, wie sie in dieser Vereinbarung dargelegt sind oder wie sie zwischen den Parteien gegebenenfalls anderweitig vereinbart wurden) oder von mit PPG verbundenen Unternehmen verarbeiten, es sei denn, der Lieferant oder der jeweilige Unterauftragsverarbeiter ist verpflichtet, die personenbezogenen Daten unter der Vereinbarung gemäß dem anwendbaren Recht zu verarbeiten, das für den Lieferanten gilt. In diesem Fall wird der Lieferant PPG vor der Verarbeitung über solche rechtlichen Verpflichtungen informieren, es sei denn, das anwendbare Recht verbietet die Benachrichtigung von PPG aus Gründen des öffentlichen Interesses); |
| 2.1.2 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; | * + 1. PPG unverzüglich informieren, wenn nach seinem begründeten Ermessen eine von PPG oder von mit PPG verbundenen Unternehmen erhaltene Anweisung gegen die Datenschutzgesetze verstößt; es wird anerkannt, dass der Lieferant nicht verpflichtet ist, zusätzliche Arbeiten oder Überprüfungen durchzuführen, um festzustellen, ob die Anweisungen von PPG den Datenschutzgesetzen entsprechen; |
| 2.1.3 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; | * + 1. unbeschadet der **Klausel 2.1.1** sicherstellen, dass die personenbezogenen Daten unter der Vereinbarung nur für den in TABELLE 1 beschriebenen Zweck und in dem dort festgelegten Umfang verwendet werden; |
| 2.1.4 without prejudice to clause 2.1.3, not without the prior written consent of PPG or the relevant PPG Affiliate: | * + 1. unbeschadet der **Klausel 2.1.3** ohne vorherige schriftliche Zustimmung von PPG oder eines mit PPG verbundenen Unternehmens folgende Punkte unterlassen: |
| 2.1.4.1 convert any Agreement Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data; | * + - 1. personenbezogene Daten unter der Vereinbarung in anonymisierte, pseudonymisierte, depersonalisierte, aggregierte oder statistische Daten umzuwandeln; |
| 2.1.4.2 use any Agreement Personal Data for “big data” analysis or purposes; or | * + - 1. personenbezogene Daten unter der Vereinbarung zur „Big-Data-Analyse“ oder entsprechenden Zwecken zu verwenden; oder |
| 2.1.4.3 match or compare any Agreement Personal Data with or against any other Personal Data (whether the Supplier’s or any third party’s); | * + - 1. personenbezogene Daten unter der Vereinbarung anderen personenbezogenen Daten (weder denen des Lieferanten noch eines Dritten) anzugleichen oder mit diesen zu vergleichen; |
| * + 1. 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. sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten unter der Vereinbarung autorisierte Person nur in einem Maße Zugang zu den personenbezogenen Daten unter der Vereinbarung hat, wie es für die Ausübung ihrer Rolle bei der Ausführung der Vereinbarung erforderlich ist, und: |
| * + - 1. is subject to binding confidentiality obligations in respect of Agreement Personal Data or is under an appropriate statutory obligation of confidentiality; | * + - 1. verbindlichen Verschwiegenheitspflichten in Bezug auf die personenbezogenen Daten unter der Vereinbarung oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegt; |
| * + - 1. complies with this clause B; and       2. is appropriately reliable, qualified and trained in relation to their responsibilities for Processing of Agreement Personal Data; and | 2.1.5.2 gemäß dieser Klausel B handelt; und   * + - 1. angemessen zuverlässig, qualifiziert und geschult in Bezug auf ihre Verantwortlichkeiten für die Verarbeitung der personenbezogenen Daten unter der Vereinbarung ist; und |
| * + 1. 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. unmittelbar nach dem Ende der Bereitstellung der mit der Verarbeitung verbundenen Dienste oder auf Anforderung zu jeder Zeit alle personenbezogenen Daten unter der Vereinbarung sicher löschen oder sie an PPG (in dem von PPG geforderten Format) zurückgeben und alle verbleibenden Kopien sicher löschen, je nach Wahl von PPG. Die Vornahme dieser Handlung ist unverzüglich anzuzeigen. Dies gilt nicht, wenn das anwendbare Recht die Speicherung der personenbezogenen Daten unter der Vereinbarung durch den Lieferanten erfordert. |
|  |  |
| 1. SECurity measures and incidents | 3. Sicherheitsmaßnahmen und -vorfälle |
| * 1. The Supplier will: | * 1. Der Lieferant wird: |
| 3.1.1 implement, and assist PPG and PPG Affiliates 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; | * + 1. technische und organisatorische Maßnahmen gemäß den Mindestanforderungen in **Tabelle 2** umsetzen und PPG sowie den mit PPG verbundenen Unternehmen bei der Umsetzung dieser Maßnahmen behilflich sein um ein dem Risiko der Verarbeitung der personenbezogenen Daten unter der Vereinbarung angemessenes Sicherheitsniveau zu gewährleisten, insbesondere im Hinblick auf Datensicherheitsvorfälle; |
| 3.1.2 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; | * + 1. PPG ohne unnötige Verzögerung informieren, wenn der begründete Verdacht besteht, dass ein Datensicherheitsvorfall vorliegt, einschließlich, aber nicht beschränkt auf die Art des Datensicherheitsvorfalls, die Kategorien und die ungefähre Anzahl der betroffenen Personen und die betroffenen personenbezogenen Daten unter der Vereinbarung sowie die möglichen Konsequenzen des Datensicherheitsvorfalls, die vorgeschlagenen Maßnahmen zur Behandlung des Datensicherheitsvorfalls und die Eindämmung möglicher nachteiliger Effekte. Wenn die Weitergabe aller maßgeblichen Informationen zur gleichen Zeit nicht möglich ist, können die Informationen ohne unnötige Verzögerung phasenweise weitergegeben werden; jedoch darf der Lieferant (und die Unterauftragsverarbeiter) die Benachrichtigung gemäß der **Klausel 3.1.2** nicht mit der Begründung verzögern, die Ermittlung sei unvollständig oder dauere noch an; |
| 3.1.3 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**; | * + 1. PPG unverzüglich darüber informieren, wenn der Lieferant oder ein Unterauftragsverarbeiter einen Grund kennt oder kennen sollte, aus dem die Erfüllung der **Klausel 3.1.1** nicht möglich ist, unbeschadet seiner Verpflichtung zur Erfüllung, oder der Rechte oder Rechtsbehelfe von PPG bei einem Verstoß gegen **Klausel 3.1.1**; |
| 3.1.4 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 | * + 1. PPG unverzüglich (in jedem Fall innerhalb von 72 Stunden) über eingegangene Anträge zur Ausübung der Rechte einer betroffenen Person gemäß der Datenschutzgesetze sowie über die von einer betroffenen Person, einer Auftsichtsbehörde oder einem Dritten in Bezug auf die personenbezogenen Daten unter der Vereinbarung erhaltene Kommunikation oder Beschwerden in Kenntnis setzen; und |
| 3.1.5 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). | * + 1. nicht ohne zuvorige schriftliche Zustimmung von PPG eine Ankündigung bezüglich eines Datensicherheitsvorfalls machen oder genehmigen oder auf einen Antrag auf Ausübung der Rechte einer betroffenen Person gemäß der Datenschutzgesetze oder auf Kommunikation oder eine Beschwerde einer betroffenen Person oder einer Aufsichtsbehörde im Bezug auf personenbezogene Daten unter der Vereinbarung antworten (es sei denn, dies ist nach anwendbarem Recht erforderlich). |
| 1. supplier assistance | 4. Unterstützung durch den Lieferanten |
| 4.1 Supplier will assist/provide reasonable assistance to PPG and PPG's Affiliates in: | * 1. Der Lieferant muss PPG und mit PPG verbundene Unternehmen bei Folgendem unterstützen/angemessene Hilfestellung leisten: |
| 4.1.1 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; | * + 1. Antwort auf Anträge auf Ausübung der Rechte einer betroffenen Person gemäß der Datenschutzgesetze sowie auf Kommunikation und Beschwerden einer betroffenen Person und einer Aufsichtsbehörde und anderen Dritten in Bezug auf die personenbezogenen Daten unter der Vereinbarung, einschließlich, aber nicht beschränkt auf geeignete technische und organisatorische Maßnahmen, sofern dies möglich ist; |
| 4.1.2 documenting any Data Security Incidents and reporting any Data Security Incidents to any Supervisory Authority and/or Data Subjects; | * + 1. Dokumentierung von Datensicherheitsvorfällen und Melden von Datensicherheitsvorfällen an Aufsichtsbehörden und/oder betroffene Personen; |
| 4.1.3 conducting privacy impact assessments of any Processing operations and consulting with Supervisory Authorities, Data Subjects and their representatives accordingly; and | * + 1. Durchführung einer Datenschutz-Folgenabschätzung auf die Privatsphäre von Verarbeitungsverfahren sowie Beratung mit Aufsichtsbehörden, betroffenen Personen und ihren jeweiligen Vertretern; und |
| 4.1.4 taking measures to address Data Security Incidents, including without limitation, where appropriate, measures to mitigate their possible adverse effects. | * + 1. Ergreifen von Maßnahmen zum Umgang mit Datensicherheitsvorfällen, einschließlich, aber nicht beschränkt auf erforderliche Maßnahmen zur Eindämmung möglicher nachteiliger Effekte; und |
| 1. appointment of subprocessors | 5. ERnennung von Unterauftragsverarbeitern |
| * 1. PPG agrees that the Supplier may engage Sub-Processors for the purposes of Processing Agreement Personal Data, provided that: | * 1. PPG erklärt sich damit einverstanden, dass der Lieferant Unterauftragsverarbeiter zum Zwecke der Verarbeitung der personenbezogenen Daten unter der Vereinbarung beauftragen kann, vorausgesetzt, dass: |
| * + 1. the Supplier shall only engage Sub-Processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that the Processing is done in accordance with this Agreement and PPG's, and Sub-Processor's, obligations under Data Protection Laws; and | * + 1. der Lieferant nur Unterauftragsverarbeiter verpflichtet, die ausreichende Garantien bieten, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit dieser Vereinbarung und den datenschutzrechtlichen Verpflichtungen von PPG und den Unterauftragsverarbeitern erfolgt, und |
| 5.1.2 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 use of the objected-to Sub-Processor. | * + 1. der Lieferant jederzeit einen neuen Unterauftragsverarbeiter benennen kann, sofern PPG 15 Werktage im Voraus informiert wird und PPG diesen Änderungen nicht innerhalb dieser Frist widerspricht. Widerspricht PPG der Bestellung eines neuen Unterauftragsverarbeiters innerhalb dieser Frist, kann PPG durch schriftliche Mitteilung an den Lieferanten die Leistung, die der Lieferant nicht ohne den Einsatz des beanstandeten Unterauftragsverarbeiters erbringen kann, kündigen. |
| * 1. 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 for all acts and omissions of Sub-Processors as if they were its own. | 5.2 Sollte der Lieferant einen Unterauftragsverarbeiter beauftragen, einen Teil der Leistungen im Zusammenhang mit der Verarbeitung der personenbezogenen Daten unter der Vereinbarung zu erbringen, muss der Lieferant sicherstellen, dass vor der Verarbeitung ein schriftlicher Vertrag zwischen dem Lieferanten und dem Unterauftragsverarbeiter besteht, in dem die Verarbeitungshandlungen des Unterauftragsverarbeiters geregelt sind und der dem Unterauftragsverarbeiter gleichwertige Konditionen auferlegt, die für den Lieferanten gemäß dieser **Klausel B** gelten. Der Lieferant hat dafür zu sorgen, dass der Unterauftragsverarbeiter alle Verpflichtungen dieser **Klausel B** erfüllt. Der Lieferant bleibt verantwortlich und haftbar für alle Handlungen und Unterlassungen des Unterauftragsverarbeiters als wären sie seine eigenen. |
| * 1. The Supplier shall maintain a list of Sub-Processors and shall promptly provide this to PPG on request. | 5.3 Der Lieferant führt eine Liste der Unterauftragsverarbeiter und stellt diese PPG auf Anfrage unverzüglich zur Verfügung. |
| 1. international transfers | 6. Internationale Übermittlungen |
| * 1. The Supplier will not make an International Transfer without PPG's prior written consent. If the 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. Der Lieferant darf ohne vorige schriftliche Zustimmung von PPG keine internationale Übermittlung durchführen. Sollte PPG vorab eine schriftliche Zustimmung zur internationalen Übermittlung erteilt haben, muss der Lieferant vor dem Durchführen der internationalen Übermittlung zur Zufriedenheit von PPG angemessene Sicherheitsvorkehrungen aufzeigen oder umsetzen, die sicherstellen, dass die internationale Übermittlung gemäß den Datenschutzgesetzen erfolgt, und dafür sorgen, dass den betroffenen Personen durchsetzbares Recht und wirksame Rechtsbehelfe zur Verfügung stehen. Solche angemessenen Sicherheitsvorkehrungen können unter anderem folgende Punkte umfassen: |
| * + 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; | * + 1. das Zielland oder Zielgebiet, in das die internationale Übermittlung erfolgen soll, unterliegt einem gültigen Angemessenheitsbeschluss der Europäischen Kommission oder die Angemessenheit wird durch eine andere anerkannte Maßnahme nach den geltenden Datenschutzgesetzen bestimmt; |
| * + 1. 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 Affiliate's identified by PPG will be a data exporter. In particular, and without limiting the above obligation: | 6.1.2 der Lieferant erklärt sich damit einverstanden, die Verpflichtungen eines Datenimporteurs gemäß den Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern einzuhalten, die durch die Entscheidung der Europäischen Kommission vom 5. Februar 2010, veröffentlicht unter der Dokumentennummer K(2010) 593 2010/87/EU (die „Standardvertragsklauseln“), festgelegt wurden. Der Lieferant erkennt an, dass PPG und von PPG bestimmte mit PPG verbundene Unternehmen Datenexporteur im Sinne der Standardvertragsklauseln sind. Insbesondere, und ohne dabei die oben genannten Verpflichtungen einzuschränken: |
| * + - 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; | 6.1.2.1 erklärt sich der Lieferant damit einverstanden, den betroffenen Personen Drittbegünstigten Rechte gemäß Klausel 3 der Standardvertragsklauseln einzuräumen, sofern die Haftung des Lieferanten auf die eigenen Verarbeitungstätigkeiten des Lieferanten beschränkt ist; |
| * + - 1. 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; | 6.1.2.2 erklärt sich der Lieferant damit einverstanden, dass die Verpflichtungen des Lieferanten aus den Standardvertragsklauseln dem/den Recht(en) des/der Mitgliedstaat(en) unterliegen, in dem/denen PPG oder die mit PPG verbundenen Unternehmen als Datenexporteur, niedergelassen sind; |
| * + - 1. 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; | 6.1.2.3 erklären die Parteien sich bereit, dass PPG für die Zwecke von Klausel 5(h) und 11 der Standardvertragsklausen dem Lieferanten die Unterauftragsvergabe gemäß den Bestimmungen in **Klausel 2** dieser Vereinbarung gestattet; |
| * + - 1. 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 | 6.1.2.4 erklären sich die Parteien damit einverstanden, dass alle Prüfungsrechte gemäß den Klauseln 5(f) und 12(2) der Standardvertragsklauseln in Übereinstimmung mit Klausel 7 dieser Vereinbarung ausgeübt werden. Die Parteien erklären sich bereit, dass im Falle eines etwaigen Widerspruchs zwischen dieser Vereinbarung und den Standardvertragsklauseln, dass die Standardvertragsklauseln Vorrang haben sollen; und |
| * + - 1. 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**; | 6.1.2.5 die Einzelheiten der Anhänge zu den Standardvertragsklauseln in **TABELLE 1** und die erforderlichen Sicherheitsmaßnahmen in **TABELLE 2** festgelegt sind; |
| * + 1. 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 | 6.1.3 die internationale Übermittlung erfolgt in die Vereinigten Staaten von Amerika und der Lieferant oder, sofern relevant, der Unterauftragsverarbeiter hat und unterhält für die Dauer der Verarbeitung eine aktuelle Registrierung unter dem US-EU Privacy Shield. Sofern diese Klausel 6.1.3 anwendbar ist, wird der Lieferant PPG unverzüglich schriftlich benachrichtigen, wenn der Lieferant oder, sofern relevant, der Unterauftragsverarbeiter die Registrierung beendet, die Aufhebung oder den Widerruf der Registrierung voraussieht oder eine Aufsichtsbehörde die Einhaltung der Vorschriften in Frage stellt oder er selbst feststellt, dass der Lieferant oder, sofern relevant, der Unterauftragsverarbeiter die Verpflichtungen unter dem Privacy Shield nicht mehr erfüllen kann; oder |
| * + 1. 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. | 6.1.4 der Lieferant oder, sofern relevant, der Unterauftragsverarbeiter bestätigt, dass die gesamte Verarbeitung der personenbezogenen Daten unter der Vereinbarung durch die verbindlichen Unternehmensrichtlinien (BCRs) des Lieferanten oder Unterauftragsverarbeiters abgedeckt ist, deren Inhalte in diese Vertragsbedingungen aufgenommen werden. Der Lieferant erklärt sich damit einverstanden, dass PPG als Verantwortlicher das Recht hat, diese verbindlichen Unternehmensrichtlinien gegenüber dem Lieferanten oder, sofern relevant, dem Unterauftragsverarbeiter durchzusetzen, einschließlich des Anspruchs auf Schadensersatz bei Verletzung der Richtlinien. |
| * 1. If the appropriate safeguards demonstrated or implemented by the Supplier (or the relevant Data Processor/Processor) 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 such applicable law prohibits notice to PPG on public interest grounds. | * 1. Sollten die vom Lieferanten (oder maßgeblichen Datenverarbeiter/Auftragsverarbeiter) aufgezeigten oder umgesetzten angemessenen Sicherheitsvorkehrungen gemäß dieser **Klausel 6** zu einem Zeitpunkt kein angemessenes Schutzniveau in Bezug auf die personenbezogenen Daten unter der Vereinbarung bieten, muss der Lieferant alternative Maßnahmen umsetzen, die von PPG oder einem mit PPG verbundenen Unternehmen gefordert werden, um sicherzustellen, dass die maßgebliche internationale Übermittlung und die daraus resultierende Verarbeitung den Datenschutzgesetzen entspricht. Der Lieferant oder maßgebliche Unterauftragsverarbeiter muss die in dieser **Klausel 6** festgelegten Bedingungen nicht einhalten, wenn die internationale Übermittlung gemäß dem anwendbaren Recht des Vereinigten Königreichs, der Schweiz oder der Europäischen Union oder den Mitgliedstaaten der Europäischen Union stattfindet, vorausgesetzt, dass der Lieferant PPG vor der internationalen Übermittlung über diese rechtlichen Verpflichtungen informiert, es sei denn, das anwendbare Recht verbietet die Benachrichtigung des Kunden aus Gründen des öffentlichen Interesses. |
| 1. audit rights | 7. Prüfungsrechte |
| * 1. The Supplier will:   7.1.1 make available to PPG and PPG Affiliates all information necessary to demonstrate compliance applicable Data Protection Laws and with the obligations set out in this **clause B**; and | * 1. Der Lieferant muss:      1. PPG und mit PPG verbundene Unternehmen alle Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der geltenden Datenschutzgesetze und der in dieser **Klausel B** festgelegten Verpflichtungen erforderlich sind; und |
| 7.1.2 allow for and contribute to audits, including without limitation inspections, conducted by PPG or another auditor mandated by PPG. | * + 1. Prüfungen erlauben und zu ihnen beitragen, einschließlich aber nicht beschränkt auf von PPG oder einem anderen von PPG ernannten Prüfer durchgeführte Kontrollen. |
| 1. indemnification | 8. Entschädigung |
| * 1. The Supplier will indemnify PPG and PPG Affiliates against any damages of and/or fines imposed against PPG and any PPG Affiliate, 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). | * 1. Der Lieferant muss PPG und mit PPG verbundenen Unternehmen für Schäden und/oder Strafzahlungen, die dem Kunden und anderen Mitgliedern des Unternehmens des Kunden auferlegt werden, entschädigen, wenn diese durch oder in Verbindung mit einem Verstoß seitens des Lieferanten oder eines Unterauftragsverarbeiters gegen die in dieser **Klausel B** enthaltenen Verpflichtungen entstanden sind (einschließlich aber nicht beschränkt auf Nichterbringen oder Verzögerung in der Ausführung oder mangelhaften Ausführung oder Nichtausführung dieser Verpflichtungen). |
| * 1. 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. | 8.2 Jeder Verstoß gegen diese **Klausel B** durch den Lieferanten oder Unterauftragsverarbeiter gilt als wesentlicher Verstoß gegen diese Vereinbarung und kann nicht behoben werden, unabhängig von dem aus einem solchen Verstoß resultierenden finanziellen Verlust oder Rufschaden unabhängig vom Umfangs eines finanziellen Schadens oder des Entzugs eines Vorteils, der als Folge einer solchen Verletzung entsteht. |
| **9.** This Agreement is executed in two versions, in German and English. In case of conflict, the English version will prevail. | **9.** Diese Vereinbarung wird in zwei Versionen, d.h. in deutscher und englischer Sprache, abgeschlossen. Im Falle von Widersprüchen genießt die englische Version Vorrang. |
| Signed by PPG [ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  ………………………………………….. Signature  ………………………………………….. Name Director | Unterzeichnet von [PPG \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  ………………………………………….. Unterschrift  ………………………………………….. Name Unternehmensleiter |
| Signed by Supplier [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  …………………………………………. Signature  ………………………………………….. Name Director | Unterzeichnet vom Lieferanten [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  …………………………………………. Unterschrift  ………………………………………….. Name Unternehmensleite |
| |  |  | | --- | --- | | 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. TABELLE 1 | | | 1. **Verarbeitungs-gegenstand** | [DETAILS] | | 1. **Verarbeitungs-dauer** | [DETAILS] | | 1. **Verarbeitungsart** | [DETAILS] | | 1. **Verarbeitungs-zweck** | [DETAILS] | | 1. **Art von personen-bezogenen Daten** | [DETAILS] | | 1. **Kategorien betroffener Personen** | [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 an 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. | | |  | | --- | | 1. TABELLE 2 2. Sicherheitsmaßnahmen | | **1. Physische Zugangskontrolle:**  Unbefugte Personen werden daran gehindert, physischen Zugang zu Räumlichkeiten, Gebäuden oder Räumen zu erhalten, in denen sich Datenverarbeitungssysteme befinden, die personenbezogene Daten nach dieser der Vereinbarung verarbeiten („**Datenzentren**“).  Maßnahmen:  Die **Datenzentren** gewährleisten strenge Sicherheitsverfahren, die von Wachpersonal, Überwachungskameras, Bewegungsmeldern, Zugangskontrollmechanismen und anderen Maßnahmen durchgesetzt werden, um zu verhindern, dass Geräte und Einrichtungen der **Datenzentren** beeinträchtigt werden. Nur autorisierte Personen haben Zugang zu Systemen und Infrastrukturen innerhalb der Einrichtungen der **Datenzentren**. Um die ordnungsgemäße Funktionalität zu gewährleisten, werden physische Sicherheitseinrichtungen (z.B. Bewegungssensoren, Kameras usw.) regelmäßig gewartet. Im Einzelnen werden in den **Datenzentren** die folgenden physischen Sicherheitsmaßnahmen umgesetzt:   * Der Lieferant schützt seine Vermögenswerte und Einrichtungen mit geeigneten Mitteln auf der Grundlage einer internen Sicherheitsklassifizierung. * Im Allgemeinen werden Gebäude durch Zugangskontrollsysteme (Smart Card Access System) gesichert. * Als Mindestanforderung muss die äußerste Gebäudebegrenzung mit einer zertifizierten Schlüsselanlage einschließlich einer modernen, aktiven Schlüsselverwaltung ausgestattet sein. * Abhängig von der Sicherheitsklassifizierung werden Gebäude, einzelne Bereiche und das umliegende Gelände durch zusätzliche Maßnahmen geschützt. Dazu gehören spezifische Zugangsprofile, Videoüberwachung und Einbruchmeldeanlagen. * Die Zugangsberechtigungen werden den berechtigten Personen individuell nach den Maßnahmen der System- und Datenzugangskontrolle erteilt (siehe Abschnitt 2 und 3 unten). Dies gilt auch für den Zugang von Besuchern. Gäste und Besucher des Gebäudes des Lieferanten müssen sich an der Rezeption anmelden und von autorisiertem Personal begleitet werden. * Die Mitarbeiter des Lieferanten und das externe Personal müssen ihre ID-Karten an allen PPG- und Lieferantenstandorten tragen.   **2. System-Zugangskontrolle:**  Es muss verhindert werden, dass Datenverarbeitungssysteme unbefugt verwendet werden.  Maßnahmen:   * Mehrere Berechtigungsstufen werden verwendet, um den Zugriff auf sensible Systeme zu ermöglichen, einschließlich der Speicherung und Verarbeitung der personenbezogenen Daten unter dieser Vereinbarung. Es gibt Prozesse, die sicherstellen, dass autorisierte Benutzer die entsprechende Berechtigung zum Hinzufügen, Löschen oder Ändern von Benutzern haben. * Alle Benutzer greifen mit einer eindeutigen Kennung (Benutzer-ID) auf die Lieferantensysteme zu. * Der Lieferant verfügt über Verfahren, die sicherstellen, dass die geforderten Berechtigungsänderungen nur richtlinienkonform durchgeführt werden (z.B. werden keine Rechte ohne Berechtigung gewährt). Verlässt ein Nutzer den Lieferanten, werden seine Zugriffsrechte entzogen. * Der Lieferant hat eine Passwortrichtlinie festgelegt, die die gemeinsame Nutzung von Passwörtern verbietet, regelt, was zu tun ist, wenn ein Passwort offengelegt wird, verlangt, dass Passwörter regelmäßig gewechselt werden und Standardpasswörter geändert werden. * Das Unternehmensnetzwerk des Lieferanten ist durch Firewalls vor dem öffentlichen Netzwerk geschützt. * Der Lieferant setzt an den Zugangspunkten zum Firmennetzwerk (für E-Mail-Konten) sowie auf allen Dateiservern und allen Arbeitsplätzen aktuelle Antivirensoftware ein. * Ein Security Patch Management ist implementiert, um die Bereitstellung relevanter Sicherheitsupdates sicherzustellen. * Der vollständige Fernzugriff auf das Unternehmensnetzwerk und die wichtige Infrastruktur des Lieferanten ist durch eine starke Authentifizierung geschützt.   **3. Kontrolle des Datenzugriffs:**  Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugang zu den personenbezogenen Daten unter dieser Vereinbarung, sofern sie ein Zugriffsrecht haben; und die personenbezogenen Daten unter dieser Vereinbarung dürfen bei der Verarbeitung, Nutzung und Speicherung nicht ohne Autorisierung gelesen, kopiert, geändert oder entfernt werden.  Maßnahmen:   * Der Zugang zu persönlichen, vertraulichen oder sensiblen Informationen wird nur dann gewährt, sofern die Kenntnis notwendig ist. Das heißt, Mitarbeiter oder externe Dritte haben Zugang zu den Informationen, die sie zur Erfüllung ihrer Arbeit benötigen. Der Lieferant verwendet Berechtigungskonzepte, die dokumentieren, wie Berechtigungen vergeben werden und welche Berechtigungen vergeben werden. Alle persönlichen, vertraulichen oder anderweitig sensiblen Daten werden in Übereinstimmung mit den Sicherheitsrichtlinien und -standards des Lieferanten geschützt. * Alle Produktionsserver eines Lieferantendienstes werden in den jeweiligen Datenzentren betrieben. Sicherheitsmaßnahmen zum Schutz von Anwendungen, die persönliche, vertrauliche oder andere sensible Informationen verarbeiten, werden regelmäßig überprüft. Zu diesem Zweck führt der Lieferant interne und externe Sicherheitskontrollen und Penetrationstests an den IT-Systemen durch. * Der Lieferant verbietet die Installation von fremder bzw. persönlicher Software oder anderer Software, die nicht vom Lieferanten genehmigt wurde, auf Systemen, die für einen IT-Service verwendet werden. * Ein Sicherheitsstandard des Lieferanten regelt, wie Daten und Datenträger gelöscht oder vernichtet werden.   **4. Steuerung der Datenübermittlung:**  Personenbezogene Daten unter dieser Vereinbarung dürfen während der Übermittlung nicht ohne Genehmigung gelesen, kopiert, geändert oder entfernt werden.  Maßnahmen:   * Beim physischen Transport von Datenträgern werden beim Lieferanten angemessene Maßnahmen zur Sicherstellung der vereinbarten Service-Levels (z.B. Verschlüsselung) ergriffen. * Personenbezogene Daten unter dieser Vereinbarung, die über die internen Netzwerke des Lieferanten übermittelt werden, sind wie alle anderen vertraulichen Daten gemäß der Sicherheitsrichtlinie des Lieferanten geschützt. * Bei der Übermittlung der Daten zwischen dem Lieferanten und PPG werden alle Daten verschlüsselt.   **5. Steuerung der Dateneingabe:**   * Es wird gewährleistet, rückwirkend zu prüfen und festzustellen, ob und durch wen personenbezogene Daten unter dieser Vereinbarung eingegeben, geändert oder aus den Datenverarbeitungssystemen entfernt wurden. * Der Auftragnehmer gestattet autorisierten Personen nur den Zugriff auf die personenbezogenen Daten unter dieser Vereinbarung, die für die Durchführung ihrer Arbeit erforderlich sind. * Der Lieferant hat ein Protokollierungssystem zur Eingabe, Änderung und Löschung implementiert.   **6. Auftragssteuerung:**  Personenbezogene Daten unter dieser Vereinbarung, die im Auftrag verarbeitet werden, werden ausschließlich in Übereinstimmung mit dieser Vereinbarung und den entsprechenden Anweisungen von PPG verarbeitet.  Maßnahmen:   * Der Lieferant verwendet Kontrollen und Prozesse, um die Einhaltung der Verträge zwischen dem Lieferanten und seinen Kunden, Unterauftragsverarbeitern oder anderen Dienstleistern sicherzustellen. * Im Rahmen der Sicherheitspolitik des Lieferanten erfordern die personenbezogenen Daten unter dieser Vereinbarung mindestens das gleiche Schutzniveau wie "vertrauliche" Informationen gemäß dem Klassifizierungsstandard des Lieferanten.   **7. Verfügbarkeitskontrolle:**  Personenbezogene Daten unter dieser Vereinbarung werden vor einem Datensicherheitsvorfall geschützt.  Maßnahmen:   * Der Lieferant setzt Backup-Prozesse und andere Maßnahmen ein, die eine schnelle Wiederherstellung geschäftskritischer Systeme bei Bedarf gewährleisten. * Der Lieferant verwendet unterbrechungsfreie Stromversorgungen (z.B. UPS, Batterien, Generatoren usw.), um die Stromversorgung des Rechenzentrums sicherzustellen. * Der Lieferant hat Notfallpläne sowie Geschäfts- und Notfallstrategien für Cloud Services definiert. * Notfallprozesse und -systeme werden regelmäßig getestet.   **8. Kontrolle der Datentrennung:**  Personenbezogene Daten unter dieser Vereinbarung werden nicht mit personenbezogenen Daten eines anderen Kunden des Lieferanten verarbeitet oder gespeichert.  Maßnahmen:   * Der Lieferant nutzt die technischen Möglichkeiten der eingesetzten Software (z.B. Mandantenfähigkeit oder separate Systeme), um eine Datentrennung zwischen den personenbezogenen Daten unter dieser Vereinbarung und anderen Daten zu erreichen. * Der Lieferant unterhält, wenn möglich, für jede Datenverarbeitung eigene Vorkehrungen.   **9. Kontrolle der Datenintegrität:**  Sicherstellung, dass die personenbezogenen Daten unter dieser Vereinbarung während der Verarbeitung intakt, vollständig und aktuell bleiben:  Maßnahmen:  Der Lieferant hat zum Schutz vor unbefugten Änderungen eine mehrstufige Abwehrstrategie implementiert. Dies bezieht sich auf die Kontrollen, wie sie in den Abschnitten Kontrolle und Maßnahmen oben beschrieben sind. Insbesondere sind dies:   * Firewalls; * Sicherheitsüberwachungsstelle; * Antivirensoftware; * Backup und Wiederherstellung; * Externe und interne Penetrationstests; * Regelmäßige externe Prüfungen zum Nachweis von Sicherheitsmaßnahmen. | |
|  |  |