|  |  |
| --- | --- |
| **DATA PROCESSING AGREEMENT****THIS AGREEMENT** is made the day of [\_\_\_\_\_\_\_\_]**BETWEEN:-**1. PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], a company with registered office at [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ("PPG"); and2. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], 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:** | **GEGEVENSVERWERKINGSOVEREENKOMST****DEZE OVEREENKOMST** is opgesteld op [\_\_\_\_\_\_\_\_]**TUSSEN:-**1. PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], een bedrijf met maatschappelijke zetel op [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ('PPG'); en2. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], een bedrijf met maatschappelijke zetel op [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ('Leverancier').**ACHTERGROND** (A) Conform een leveranciersovereenkomst tussen PPG en de Leverancier (samen 'de Partijen') van [\_\_\_\_\_\_\_\_\_\_\_] (Leveranciersovereenkomst) is de Leverancier akkoord gegaan om de daarin vermelde diensten ('Diensten') te leveren, die het delen van persoonsgegevens door PPG aan de Leverancier kunnen omvatten.(B) De Partijen gaan akkoord dat de voorwaarden van deze Overeenkomst opgenomen zijn en deel uitmaken van de algemene voorwaarden van de Leveranciersovereenkomst. Als de voorwaarden van deze Overeenkomst strijdig zijn met de algemene voorwaarden van de Leveranciersovereenkomst, dan hebben de voorwaarden van deze Overeenkomst voorrang.**ER WORDT OVEREENGEKOMEN DAT:** |
| 1. DEFINITIONS AND CLAUSES
 | 1. Definities en clausules
 |
| In this Agreement the following expressions bear the following meanings unless the context otherwise requires: | In deze Overeenkomst hebben de volgende uitdrukkingen de volgende betekenissen, tenzij de context anders aangeeft: |
| 1. **"Agreement Personal Data"**
2. Personal Data which is to be Processed under this Agreement, as more particularly described in **SCHEDULE 1**
 | 1. **'Persoonsgegevens uit de Overeenkomst'**

Persoonsgegevens die volgens deze Overeenkomst worden verwerkt, zoals uitvoeriger beschreven in **SCHEDULE 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
 | **"Affiliate"**met betrekking tot enige entiteit, een entiteit die zeggenschap heeft over een entiteit, een entiteit die onder de zeggenschap staat van of onder gezamenlijke zeggenschap staat met die entiteit, direct of indirect, via een of meer tussenpersonen. Voor de toepassing van deze definitie wordt "onder zeggenschap" (met inbegrip van de termen "onder zeggenschap van" en "onder gezamenlijke zeggenschap"), zoals deze met betrekking tot enige entiteit worden gebruikt, verstaan het bezit, direct of indirect, van de bevoegdheid om het bestuur en het beleid van deze entiteit te leiden of te doen leiden, hetzij door middel van het bezit van stemgerechtigde effecten, als trustee of uitvoerder, door middel van een contract of een kredietregeling of anderszins. |
| 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
 | 1. **'Wetten voor Gegevensbescherming'**
2. alle toepasselijke wetten betreffende gegevensbescherming, de verwerking van persoonsgegevens en privacy, inclusief zonder beperking:
	1. de algemene verordening gegevensbescherming (EU) 2016/679;
	2. De UK Data Protection Act en de Algemene Verordening Gegevensbescherming zoals beschikbaar gemaakt in de UK via de UK European Union (Withdrawal) Act; en
	3. De Zwitserse Federale Gegevensbeschermingswetgeving;

En enige wet- of regelgeving die de bovenstaande wetgeving implementeert, opvolgt, vervangt, aanpast of consolideert.1. en verwijzingen naar **'gegevensverwerker', 'betrokkenen'**, **'persoonsgegevens'**, **'verwerking'**, **'verwerkt'**, **'verwerken'**, **'verwerker'** en **'toezichthoudende instantie'** hebben de betekenis zoals vermeld in zulke toepasselijke wetten en worden als dusdanig geïnterpreteerd
 |
| 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. **'gegevensveiligheidsincident'**
	1. een inbreuk op de beveiliging die geresulteerd heeft in onbedoelde of onwettige vernietiging, verlies, wijziging of in niet-geautoriseerde vrijgave van, of toegang tot de verstuurde, opgeslagen of anderszins verwerkte Persoonsgegevens uit de Overeenkomst; of
	2. een ontdekking of redelijk vermoeden dat er een kwetsbaarheid zit in een technische maatregel die gebruikt is om de Persoonsgegevens uit de Overeenkomst te beschermen die eerder het slachtoffer van een inbreuk zijn geweest binnen de werkingssfeer van (a), wat kan leiden tot het gebruik of de blootstelling van die Overeenkomst persoonsgegevens; of
	3. elk defect of elke kwetsbaarheid die mogelijk de lopende veerkracht, veiligheid en/of integriteit van de systemen voor de verwerking van de Persoonsgegevens uit de Overeenkomst kan treffen
 |
| 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 overdracht'**
2. een overdracht naar een land buiten de Europese Economische Ruimte, het Verenigd Koninkrijk of Switzerland van de Persoonsgegevens uit de Overeenkomst die worden verwerkt of die na de overdracht moeten worden verwerkt
 |
| 1. **"Sub-Processor"**
2. any third party Processor appointed by the Supplier to Process Agreement Personal Data
 | 1. **'Subverwerker'**
2. een derde Verwerker die door de Leverancier is aangesteld om de Persoonsgegevens uit de Overeenkomst te verwerken
 |
| 1. DATA PROTECTION AND INFORMATION SECURITY
 | 1. GEGEVENSBESCHERMING EN INFORMATIEBEVEILIGING
 |
| 1. Authorisation and compliance with laws
 | 1. Toestemming en compliance
 |
| * 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**.
 | * 1. PPG geeft aan de Leverancier de toestemming om in zijn naam en die van de Affiliates van PPG de Persoonsgegevens uit de Overeenkomst te verwerken voor de duur van deze Overeenkomst als een gegevensverwerker en uitsluitend voor het doeleinde en in de mate zoals beschreven in **SCHEDULE 1.**
 |
| * 1. In performing the Services and its other obligations under this Agreement the Supplier will:
 | 1.2 Bij het uitvoeren van de Diensten en zijn andere verplichtingen volgens deze Overeenkomst, zal de Leverancier: |
| * + 1. comply with the Data Protection Laws; and
 | * + 1. de wetgeving voor gegevensbescherming naleven;
 |
| * + 1. not cause PPG or any PPG Affiliate to breach any obligation under the Data Protection Laws.
 | * + 1. ervoor zorgen dat PPG of een ander de van de Affiliates van PPG geen inbreuk pleegt op een verplichting van de wetgeving voor gegevensbescherming.
 |
| 1. processing of agreement personal data
 | 2. Verwerken van persoonsgegevens |
| * 1. The Supplier will:
 | * 1. De Leverancier moet:
 |
| 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. de Persoonsgegevens uit de Overeenkomst alleen verwerken volgens de gedocumenteerde instructies van PPG (Wat tevens specifieke instructies of algemene instructies kunnen zijn zoals bepaald in deze Overeenkomst of anderszins van tijd tot tijd overeengekomen tussen Partijen ) of de relevante PPG Affiliate, tenzij de Leverancier of de relevante Subverwerker vereist is om Persoonsgegevens uit de Overeenkomst te verwerken om de op Leverancier toepasselijke wetgeving na te leven. In dat geval licht de Leverancier PPG vóór de verwerking in over zulke juridische vereiste, tenzij de toepasselijke wetgeving de melding aan PPG verbieden op grond van het algemeen belang);
 |
| 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 onmiddellijk schriftelijk in te lichten als hij in redelijkheid van mening is dat een instructie van PPG of een Affiliate van PPG inbreuk maakt op de wetgeving voor gegevensbescherming, waarbij wordt verondersteld dat Leverancier geen additionele werkzaamheden of screening hoeft te verrichten om te bepalen of de instructies van PPG compliant zijn;
 |
| 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. onverminderd bepaling **2.1.1,** ervoor zorgen dat de Persoonsgegevens uit de Overeenkomst alleen worden gebruikt voor het doeleinde en in de mate zoals beschreven in **SCHEDULE 1**;
 |
| 2.1.4 without prejudice to clause 2.1.3, not without the prior written consent of PPG or the relevant PPG Affiliate: | * + 1. onverminderd bepaling 2.1.3, niet zonder de voorafgaande schriftelijke toestemming van PPG of het relevante Affiliate van PPG:
 |
| 2.1.4.1 convert any Agreement Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data; | * + - 1. Persoonsgegevens uit de Overeenkomst omzetten naar geanonimiseerde, gepseudonimiseerde, gedepersonaliseerde, samengevoegde of statistische gegevens;
 |
| 2.1.4.2 use any Agreement Personal Data for “big data” analysis or purposes; or | * + - 1. Persoonsgegevens uit de Overeenkomst gebruiken voor 'big data'-analyse of -doeleinden; of
 |
| 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. Persoonsgegevens uit de Overeenkomst overeenstemmen of vergelijken met andere Persoonsgegevens (van de Leverancier of van een derde);
 |
| * + 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. ervoor zorgen dat elk individu dat bevoegd is om Persoonsgegevens uit de Overeenkomst te verwerken, tot deze Persoonsgegevens uit de Overeenkomst toegang heeft volgens een strikte 'need to know'-basis als dit nodig is om zijn rol in de uitvoering van deze Overeenkomst te spelen, en:
 |
| * + - 1. is subject to binding confidentiality obligations in respect of Agreement Personal Data or is under an appropriate statutory obligation of confidentiality;
 | * + - 1. is onderworpen aan bindende vertrouwelijkheidsverplichtingen ten aanzien van Persoonsgegevens verwerkt onder deze Overeenkomst of een gepaste statutaire vertrouwelijkheidsverplichting heeft;
 |
| * + - 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
 | * + - 1. leeft deze **clausule** **B** na; en
			2. is betrouwbaar, gekwalificeerd en opgeleid met betrekking tot zijn verwerking van Persoonsgegevens uit de Overeenkomst;
 |
| * + 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. naar keuze van PPG, alle Persoonsgegevens uit de Overeenkomst onmiddellijk en veilig wissen of terugsturen naar PPG (in de door PPG gekozen indeling) na het einde van de dienstverlening met betrekking tot de verwerking of op elk ogenblik na verzoek, en alle resterende kopieën veilig wissen en onmiddellijk certificeren wanneer deze handeling is uitgevoerd, tenzij toepasselijke wetgeving het bewaren van Persoonsgegevens uit de Overeenkomst door Leverancier verplicht.
 |
|  |  |
| 1. SECurity measures and incidents
 | 3. BEVEILIGINGSMAATREGELEN EN INCIDENTEN |
| * 1. The Supplier will:
 | * 1. De Leverancier moet:
 |
| 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. Adequate technische en organisatorische maatregelen invoeren en PPG en PPG's Affiliates helpen bij het invoeren minimaal volgens de norm in Bijlage 2 om een gepast beveiligingsniveau te verzekeren voor het risico dat bestaat bij de verwerking van Persoonsgegevens uit de Overeenkomst, met name bij een gegevensveiligheidsincident;
 |
| 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. het PPG zonder onredelijke vertraging melden als hij zich bewust is van een redelijkerwijs vermoed of feitelijk gegevensveiligheidsincident, inclusief, zonder beperking, de aard van het gegevensveiligheidsincident, de categorieën en het geraamde aantal betrokken en aantal Persoonsgegevens uit de Overeenkomst, de waarschijnlijke gevolgen van het gegevensveiligheidsincident en elke voorgestelde maatregel die moet worden genomen om het gegevensveiligheidsincident aan te pakken en om de mogelijke negatieve gevolgen te beperken. Waar en voor zover het niet mogelijk is om alle relevante informatie tegelijkertijd te leveren, kan de informatie zonder onredelijke vertraging in fasen worden geleverd, maar de Leverancier (en Subverwerkers) mogen de melding onder deze clausule **3.1.2** niet vertragen met als reden dat een onderzoek onvoltooid of lopende is;
 |
| 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 onmiddellijk inlichten als op welk ogenblik ook de Leverancier of een Subverwerker zich bewust is of dient te zijn van een reden waarom hij **clausule 3.1.1** niet kan naleven **,** onverminderd zijn verplichting omalle rechten of rechtsmiddelen na te leven die PPG kan hebben voor een inbreuk van de **clausule 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 onmiddellijk (en in elk geval binnen de 72 uur) elk verzoek melden dat hij heeft gekregen voor de uitoefening van de rechten van een betrokkenen volgens de wetgeving voor gegevensbescherming, of de communicatie of klacht melden die hij krijgt van een betrokkene of toezichthoudende instantie of andere derde met betrekking tot de Persoonsgegevens uit de Overeenkomst; en
 |
| 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. zonder de voorafgaande schriftelijke toestemming van PPG geen aankondiging maken of toestaan met betrekking tot een gegevensveiligheidsincident of voldoen aan om het even welk verzoek tot uitoefening van de rechten van een betrokkene volgens de wetgeving voor gegevensbescherming of klacht van een betrokkene of toezichthoudende instantie met betrekking tot de Persoonsgegevens uit de Overeenkomst (behalve waar dit verplicht is op grond van toepasselijk recht); en
 |
| 1. supplier assistance
 | 1. LEVERANCIERs ondersteuning
 |
| 4.1 Supplier will assist/provide reasonable assistance to PPG and PPG's Affiliates in: | * 1. De Leverancier moet PPG en de Affiliates van PPG helpen of redelijke hulp bieden bij:
 |
| 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. het voldoen aan verzoeken voor de uitoefening van de rechten van de betrokkenen volgens de wetgeving voor gegevensbescherming en reageren op communicatie en klachten van betrokkenen en toezichthoudende instanties en andere derden met betrekking tot Persoonsgegevens uit de Overeenkomst, inclusief, zonder beperking, met technische en organisatorische maatregelen, voor zover dit mogelijk is;
 |
| 4.1.2 documenting any Data Security Incidents and reporting any Data Security Incidents to any Supervisory Authority and/or Data Subjects;  | * + 1. het documenteren van gegevensveiligheidsincidenten en het rapporteren van gegevensveiligheidsincidenten aan een toezichthoudende instantie en/of betrokkenen;
 |
| 4.1.3 conducting privacy impact assessments of any Processing operations and consulting with Supervisory Authorities, Data Subjects and their representatives accordingly; and | * + 1. het voeren van effectbeoordelingen op het gebied van privacy van verwerkingshandelingen en het overleggen met toezichthoudende instanties, betrokkenen en hun overeenkomstige vertegenwoordigers; en
 |
| 4.1.4 taking measures to address Data Security Incidents, including without limitation, where appropriate, measures to mitigate their possible adverse effects. | * + 1. het nemen van maatregelen om gegevensveiligheidsincidenten aan te pakken, inclusief, zonder beperking en waar toepasselijk, maatregelen om hun mogelijke negatieve gevolgen te beperken.
 |
| 1. appointment of subprocessors
 | 5. Aanwijzing van subverwerkers |
| * 1. PPG agrees that the Supplier may engage Sub-Processors for the purposes of Processing Agreement Personal Data, provided that:
 | * 1. PPG stemt ermee in dat de Leverancier Subverwerkers mag inschakelen voor de doeleinden van het Verwerken van de Persoonsgegevens uit de Overeenkomst, op voorwaarde dat:
 |
| * + 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. De Leverancier zal enkel Subverwerkers inschakelen die voldoende garanties bieden om passende technische en organisatorische maatregelen te implementeren om ervoor te zorgen dat de Verwerking wordt uitgevoerd in overeenstemming met deze Overeenkomst en de verplichtingen van PPG en Subverwerkers onder de Wetten voor Gegevensbescherming; en
 |
| 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. De Leverancier kan te allen tijde een nieuwe Subverwerker aanwijzen, mits PPG 15 werkdagen van te voren op de hoogte wordt gesteld en PPG geen bezwaar maakt tegen dergelijke wijzigingen binnen dat tijdsbestek. Indien PPG bezwaar maakt tegen de benoeming van een nieuwe Subverwerker binnen een dergelijke termijn, kan PPG, door middel van een schriftelijke kennisgeving aan de Leverancier, de Dienst beëindigen die niet door de Leverancier kan worden geleverd zonder gebruik te maken van de Subverwerker waartegen bezwaar wordt gemaakt.
 |
| * 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 for all acts and omissions of Sub-Processors as if they were its own.
 | * 1. Als de Leverancier een Subverwerker aanstelt voor het verwerken van Persoonsgegevens uit de Overeenkomst, dan zorgt de Leverancier ervoor dat er voorafgaand de verwerking een schriftelijke overeenkomst is gesloten tussen de Leverancier en de Subverwerker, die de verwerkingsactiviteiten van de Subverwerker beschrijft en de Subverwerker overeenkomstige voorwaarden oplegt als die in deze clausule **B** aan de Leverancier zijn opgelegd. De Leverancier zorgt ervoor dat de Subverwerkers alle verplichtingen in deze bepaling **B** naleven. Bovendien blijft de Leverancier verantwoordelijk en aansprakelijk voor alle handelingen en omissies van Subverwerkers alsof het de zijne zijn.
 |
| * 1. The Supplier shall maintain a list of Sub-Processors and shall promptly provide this to PPG on request.
 | * 1. De Leverancier zal een lijst met Subverwerkers bijhouden en deze op eerste verzoek aan PPG verstrekken.
 |
| 1. international transfers
 | 6. internationale doorgifte |
| * 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. De Leverancier verricht geen Internationale overdracht zonder de voorafgaande schriftelijke toestemming van PPG. Als PPG zijn voorafgaande schriftelijke toestemming voor een Internationale overdracht geeft, dan moet de Leverancier vóór deze Internationale overdracht naar tevredenheid van PPG gepaste voorzorgsmaatregelen voor die Internationale overdracht aantonen of invoeren, in overeenstemming met de wetgeving voor gegevensbescherming en moet hij ervoor zorgen dat afdwingbare rechten en doeltreffende juridische rechtsmiddelen beschikbaar zijn voor betrokkenen. Zulke geschikte voorzorgsmaatregelen kunnen, zonder beperking de volgende zaken omvatten:
 |
| * + 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. het land of grondgebied naar waar de Internationale overdracht moet gebeuren, is onderwerp van een geldige geschiktheidsbeslissing (*adequacy decision*) uitgegeven door de Europese Commissie of de geschiktheid is beoordeeld door een andere valide methode onder geldende Wetten voor Gegevensbescherming;
 |
| * + 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 de Leverancier ermee instemt te voldoen aan de verplichtingen van een gegevensimporteur zoals uiteengezet in de Modelcontractsbepalingen voor de overdracht van persoonsgegevens aan in derde landen gevestigde gegevensverwerkers, zoals vastgesteld bij het besluit van de Europese Commissie van 5 februari 2010, C(2010) 593 2010/87/EU (de "Modelcontractsbepalingen"). De Leverancier erkent dat PPG en de door PPG opgegeven Affiliates, gegevensexporteur zullen zijn. In het bijzonder, en zonder beperking van bovenstaande verplichting: |
| * + - 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;
 | * + - 1. De Leverancier stemt ermee in om derde-rechten toe te kennen aan de Betrokkenen zoals uiteengezet in artikel 3 van de Modelcontractsbepalingen, met dien verstande dat de aansprakelijkheid van de Leverancier beperkt zal zijn tot de eigen verwerkingsactiviteiten van de Leverancier;
 |
| * + - 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;
 | * + - 1. de Leverancier stemt ermee in dat de verplichtingen van de Leverancier onder de Modelcontractsbepalingen worden beheerst door het recht of de wetten van de Lidstaat of Lidstaten waarin PPG of PPG's Affiliate (die de gegevensexporteur is) is gevestigd;
 |
| * + - 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;
 | * + - 1. de Partijen komen overeen dat voor de toepassing van artikel 5(h) en 11 van de Modelcontractsbepalingen, PPG instemt met onderaanneming door de Leverancier in overeenstemming met het bepaalde in **artikel 2** van deze Overeenkomst;
 |
| * + - 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
 | * + - 1. de partijen komen overeen dat eventuele rechten op controle, ingevolge de artikelen 5(f) en 12(2) van de Modelcontractsbepalingen, zullen worden uitgeoefend in overeenstemming met artikel 7 van deze Overeenkomst. De partijen komen overeen dat in geval van tegenstrijdigheid tussen deze Overeenkomst en de Modelcontractsbepalingen, de Modelcontractsbepalingen prevaleren; en
 |
| * + - 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**;
 | * + - 1. de details van de bijlagen die van toepassing zijn op de Modelcontractsbepalingen zijn zoals uiteengezet in **SCHEDULE 1** en de vereiste veiligheidsmaatregelen zijn zoals uiteengezet in **SCHEDULE 2**.
 |
| * + 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 if 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 de Internationale overdracht vindt plaats naar de VS en de Leverancier of Subverwerker, al naar gelang het geval, is geregistreerd voor de duur van de Verwerking onder het US-EU Privacy Shield. Indien dit artikel 6.1.3 van toepassing is, zal de Leverancier PPG onverwijld schriftelijk in kennis stellen van het feit dat de Leverancier of de Subverwerker niet langer mee kan voldoen aan de vereisten van het Privacy Shield, dat haar registratie ter discussie zal komen (bijvoorbeeld door een toezichthoudend orgaan) of dat de registratie zal verlopen of worden ingetrokken; of |
| * + 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 de Leverancier of Subverwerker, al naar gelang het geval, bevestigt dat de Verwerking van Persoonsgegevens uit de Overeenkomst door de bindende bedrijfsregels van de Leverancier of Subverwerker, waarvan de voorwaarden in deze voorwaarden zijn opgenomen, worden gedekt. De Leverancier stemt ermee in dat PPG, als verantwoordelijke voor de verwerking van gegevens, het recht heeft om deze bindende bedrijfsregels tegen de Leverancier of Subverwerker af te dwingen, indien relevant, met inbegrip van een recht op schadevergoeding in het geval dat de regels worden overtreden. |
| * 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. Als men op een gegeven ogenblik meent dat de gepaste voorzorgsmaatregelen die door de Leverancier (of de relevante gegevensverwerker/verwerker) aangetoond of ingevoerd zijn in overeenstemming met deze clausule 6 niet een gepast beveiligingsniveau hebben met betrekking tot de Persoonsgegevens uit de Overeenkomst, dan moet de Leverancier alternatieve maatregelen nemen zoals die vereist kunnen zijn door PPG of PPG's Affiliate om ervoor te zorgen dat de relevante Internationale overdracht en alle daaruit voortvloeiende verwerking de wetgeving voor gegevensbescherming naleeft. De Leverancier of de relevante Subverwerker hoeft de voorwaarden in deze clausule 6 niet na te leven als hij een Internationale overdracht moeten doen om de Toepasselijke wetten van het Verenigd Koninkrijk, Zwitserland of de Europese Unie of een lidstaat van de Europese Unie na te leven. In dat geval licht de Leverancier PPG vóór de Internationale overdracht in over zulke juridische vereiste, tenzij de toepasselijke wetgeving de melding aan PPG verbiedt op grond van het algemeen belang.
 |
| 1. audit rights
 | 7. AUDIT RECHTEN |
| * 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. De Leverancier moet:
		1. alle informatie aan PPG en de Affiliates van PPG ter beschikking stellen die nodig is om de naleving van toepasselijke Wetten voor Gegevensbescherming de verplichtingen in deze **clausule** B aan te tonen; en
 |
| 7.1.2 allow for and contribute to audits, including without limitation inspections, conducted by PPG or another auditor mandated by PPG.  | * + 1. audits toestaan en eraan bijdragen, inclusief, zonder beperking, inspecties door PPG of een andere auditeur die daartoe door PPG is gemachtigd.
 |
| 1. indemnification
 | 8. vrijwaring |
| * 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. De Leverancier moet PPG en Affiliates van PPG vrijwaren tegen alle schadevergoedingen en/of boetes die PPG en de Affiliates van PPG worden opgelegd, in elk geval als ze voortvloeien uit of in verband staan met een inbreuk van de Leverancier of een Subverwerker op een verplichting onder deze clausule B (inclusief, zonder beperking, het niet of te laat of slecht naleven van elk van die verplichtingen).
 |
| * 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.
 | * 1. Elke inbreuk van deze clausule B door de Leverancier of een Subverwerker is een wezenlijke inbreuk van deze Overeenkomst die niet kan worden verholpen, ongeacht of ze tot financiële of imagoschade leidt, en ongeacht van de omvang van een financieel verlies of verlies van inkomsten die optreden ten gevolge van zulke inbreuk.
 |
| **9.** This Agreement is executed in two versions, in Dutch and English. In case of conflict, the English version will prevail. | **9.** Deze overeenkomst wordt opgesteld in twee talen, in het Nederlands en Engels. In geval van conflicten is de Engelse versie leidend. |
| Signed by PPG [ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] …………………………………………..Signature…………………………………………..NameDirector | Ondertekend door [PPG \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] …………………………………………..Handtekening…………………………………………..NaamDirecteur |
| Signed by Supplier [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ………………………………………….Signature …………………………………………..NameDirector | Ondertekend door Leverancier [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] ………………………………………….Handtekening …………………………………………..NaamDirecteur |
|

|  |
| --- |
| 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. BIJLAGE 1
 |
| 1. **Onderwerp van verwerking**
 | [DETAILS] |
| 1. **Duur van verwerking**
 | [DETAILS] |
| 1. **Aard van verwerking**
 | [DETAILS] |
| 1. **Doeleinde van verwerking**
 | [DETAILS] |
| 1. **Type persoonsgegevens**
 | [DETAILS] |
| 1. **Categorieën betrokkenen**
 | [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.
 |

 |

|  |
| --- |
| 1. SCHEDULE 1
2. BEVEILIGINGSMAATREGELEN
 |

1. Fysieke toegangscontrole:Onbevoegden wordt verhinderd fysieke toegang te krijgen tot locaties, gebouwen of ruimtes waar gegevensverwerkingssystemen zich bevinden die Persoonsgegevens uit de Overeenkomst ("Datacentra").Maatregelen:De datacentra houden zich aan strikte beveiligingsprocedures die worden gehandhaafd door bewakers, bewakingscamera's, bewegingsdetectoren, toegangscontrolemechanismen en andere maatregelen om te voorkomen dat apparatuur en faciliteiten van het datacentrum worden gecompromitteerd. Alleen bevoegd personeel heeft toegang tot systemen en infrastructuur binnen het datacentrum. Om een goede functionaliteit te waarborgen, wordt de fysieke beveiligingsapparatuur (zoals bewegingssensoren, camera's, enz.) regelmatig gecontroleerd en onderhouden. In de datacenters zijn de volgende fysieke beveiligingsmaatregelen in voldoende detail geïmplementeerd:- De leverancier beschermt zijn activa en faciliteiten met behulp van de juiste middelen op basis van een interne veiligheidsclassificatie.- In het algemeen worden gebouwen beveiligd door middel van toegangscontrolesystemen (smart card access system).- Als minimumvereiste moet de buitenste laag van het gebouw worden uitgerust met een gecertificeerd sleutelsysteem voorzien van modern, actief sleutelbeheer.- Afhankelijk van de veiligheidsclassificatie worden gebouwen, afzonderlijke zones en omliggende terreinen verder beschermd door aanvullende maatregelen. Hiertoe behoren specifieke toegangsprofielen, videobewaking en inbraakalarmsystemen.- Toegangsrechten worden aan geautoriseerde personen op individuele basis toegekend volgens de systeem- en datatoegangscontrolemaatregelen (zie paragraaf 2 en 3 hieronder). Dit geldt ook voor de toegang van bezoekers. Gasten en bezoekers van het gebouw van de Aanbieder dienen zich bij de receptie te registreren en zich te laten vergezellen door bevoegd personeel. - Medewerkers en extern personeel van Aanbieder dienen hun ID-kaart te dragen op alle locaties van PPG en Aanbieder.2. Toegangscontrole van het systeem:Het gebruik van gegevensverwerkingssystemen zonder toestemming daartoe dient te worden voorkomen.Maatregelen:- Meerdere autorisatieniveaus worden gebruikt om toegang te verlenen tot gevoelige systemen met inbegrip van systemen die Persoonsgegevens uit de Overeenkomst opslaan en verwerken. Er bestaan processen om ervoor te zorgen dat geautoriseerde gebruikers de juiste autorisatie hebben om gebruikers toe te voegen, te verwijderen of te wijzigen.- Alle gebruikers hebben toegang tot de systemen van de Leverancier middels unieke identificatie (gebruikers-ID).- De Leverancier beschikt over procedures om ervoor te zorgen dat de gevraagde autorisatiewijzigingen alleen worden doorgevoerd in overeenstemming met geschikte richtlijnen (er worden bijvoorbeeld geen rechten verleend zonder autorisatie). Als een gebruiker de Leverancier verlaat (eg. er niet langer werkt), worden zijn toegangsrechten ingetrokken.- De Leverancier heeft een wachtwoordbeleid opgesteld dat het delen van wachtwoorden verbiedt, regelt wat te doen als een wachtwoord wordt onthuld, eist dat wachtwoorden regelmatig worden gewijzigd en dat standaardwachtwoorden worden gewijzigd. Gepersonaliseerde gebruikers-ID's worden toegewezen voor authenticatie. Alle wachtwoorden moeten aan bepaalde minimumeisen voldoen en worden versleuteld opgeslagen. In het geval van domeinwachtwoorden dwingt het systeem om de zes maanden een wachtwoordwijziging af die voldoet aan de vereisten voor complexe wachtwoorden. Elke computer heeft een met een wachtwoord beveiligde screensaver.- Het bedrijfsnetwerk van de leverancier wordt beschermd door firewalls.- De leverancier gebruikt up-to-date antivirussoftware op toegangspunten tot het bedrijfsnetwerk (voor e-mailaccounts) en op alle bestandsservers en alle werkstations.- Een beveiligings-, patch- en updatebeheer is geïmplementeerd om de inzet van relevante beveiligingsupdates te garanderen.- Volledige toegang op afstand tot het bedrijfsnetwerk en de kritieke infrastructuur van de leverancier wordt beschermd door sterke authenticatie.3. Controle op de toegang tot de gegevens:Alleen Personen die toegewezen rechten hebben op de gegevensverwerkingssystemen krijgen toegang tot de Persoonsgegevens uit de Overeenkomst en de Persoonsgegevens uit de Overeenkomst mogen niet worden gelezen, gekopieerd, gewijzigd of verwijderd zonder toestemming gedurende de verwerking, het gebruik en de opslag.Maatregelen:- Toegang tot persoonlijke, vertrouwelijke of gevoelige informatie wordt verleend op een "need-to-know"-basis. Met andere woorden, werknemers of externe derden hebben toegang tot de informatie die zij nodig hebben om hun werk te voltooien. De Leverancier gebruikt autorisatieconcepten die vastleggen hoe autorisaties worden toegekend en welke autorisaties worden toegekend. Alle persoonlijke, vertrouwelijke of anderszins gevoelige gegevens worden beschermd in overeenstemming met het beveiligingsbeleid en de normen van de Leverancier.- Alle productieservers van een Dienst van de Leverancier worden beheerd in de desbetreffende Datacentra. Veiligheidsmaatregelen ter bescherming van toepassingen die persoonlijke, vertrouwelijke of andere gevoelige informatie verwerken, worden regelmatig gecontroleerd. Hiertoe voert de Leverancier interne en externe veiligheidscontroles en penetratietests uit op de IT-systemen.- De Leverancier staat niet toe dat persoonlijke software of andere software die niet door de Leverancier is goedgekeurd, wordt geïnstalleerd op systemen die worden gebruikt voor een IT-service.- Een beveiligingsstandaard van de Leverancier regelt hoe gegevens en gegevensdragers worden verwijderd of vernietigd.4. Controle op de doorgifte van gegevens:Persoonsgegevens uit de Overeenkomst mogen niet worden gelezen, gekopieerd, gewijzigd of verwijderd zonder toestemming tijdens de overdracht.Maatregelen:- Bij fysiek transport van gegevensdragers worden bij de Leverancier adequate maatregelen getroffen om de overeengekomen serviceniveaus (bijvoorbeeld versleuteling) te waarborgen.- Persoonsgegevens uit de Overeenkomst die over de interne netwerken van de Leverancier worden overgedragen, worden beschermd als alle andere vertrouwelijke gegevens volgens het beveiligingsbeleid van de Leverancier.- Wanneer de gegevens tussen de Leverancier en PPG worden overgedragen, worden alle gegevens versleuteld.5. Controle op de invoer van gegevens:- Het is mogelijk om achteraf te onderzoeken en bij de Leverancier vast te stellen of en door wie bij Persoonsgegevens uit de Overeenkomst zijn ingevoerd, gewijzigd of verwijderd uit gegevensverwerkingssystemen.- De Leverancier verleent alleen geautoriseerde personen toegang tot de Persoonsgegevens uit de Overeenkomst zoals vereist in het kader van hun werkzaamheden. - Leverancier heeft een registratiesysteem voor invoer, wijziging en verwijdering geïmplementeerd.6. Taakcontrole:Persoonsgegevens uit de Overeenkomst die in opdracht worden verwerkt, zullen uitsluitend worden verwerkt in overeenstemming met de Overeenkomst en de bijbehorende instructies van PPG.Maatregelen:- De Leverancier maakt gebruik van controles en processen om de naleving van contracten tussen de Leverancier en zijn klanten, Subverwerkers of andere dienstverleners te waarborgen.- Als onderdeel van het beveiligingsbeleid van de Leverancier vereisen Persoonsgegevens uit de Overeenkomst ten minste hetzelfde beschermingsniveau als "vertrouwelijke" informatie volgens de informatieclassificatiestandaard van de Leverancier.7. Controle op beschikbaarheid:Persoonsgegevens uit de Overeenkomst worden beschermd tegen incidenten op het gebied van gegevensbeveiliging en overige gegevensveiligheidsincidenten.Maatregelen:- De Leverancier maakt gebruik van back-upprocessen en andere maatregelen die zorgen voor een snel herstel van bedrijfskritische systemen waar en wanneer dat nodig is.- De Leverancier maakt gebruik van ononderbroken stroomvoorzieningen (bijvoorbeeld: UPS, batterijen, generatoren, etc.) om de beschikbaarheid van stroom voor het Data Center te waarborgen.- De leverancier heeft noodplannen opgesteld, evenals bedrijfs- en noodherstelstrategieën voor clouddiensten.- Noodprocessen en -systemen worden regelmatig getest.8. Controle op gegevensscheiding:Persoonsgegevens uit de Overeenkomst worden niet Verwerkt of opgeslagen met Persoonsgegevens van een andere klant van Leverancier.Maatregelen:- Leverancier maakt gebruik van de technische mogelijkheden van de ingezette software (bijvoorbeeld: multi-tenancy of afzonderlijke systemen) om tot gegevensscheiding tussen de Persoonsgegevens van de Overeenkomst en andere gegevens te komen.- Leverancier onderhoudt, waar mogelijk, specifieke instanties per gegevensverwerking.9. Controle op de integriteit van de gegevens:Zorgt ervoor dat de Overeenkomst Persoonsgegevens tijdens de verwerking intact, volledig en actueel blijven:Maatregelen:De Leverancier heeft een beveiligingsstrategie met meerdere lagen geïmplementeerd als bescherming tegen ongeoorloofde wijzigingen. Dit betreft de controles zoals vermeld in de controle- en meetsecties zoals hierboven beschreven. In het bijzonder:- Firewalls;- Veiligheidsmonitoringcentrum;- Antivirussoftware;- Back-up en herstel;- Externe en interne penetratietesten;- Regelmatige externe audits om beveiligingsmaatregelen aan te tonen. |
|  |  |