|  |  |
| --- | --- |
| **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"). | **UMOWA PRZETWARZANIA DANYCH**  **NINIEJSZA UMOWA** zawarta w dniu [\_\_\_\_\_\_\_\_]  **MIĘDZY:-**  1. PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_], firma zarejestrowaną pod adresem [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] („PPG”); a  2. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_], firmą zarejestrowaną pod adresem [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] („Dostawca”). |
| **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. | **KONTEKST**  (A) Zgodnie z kontraktem dostawy zawartym między PPG a Dostawcą (zwanymi razem „Stronami”) w dniu [\_\_\_\_\_\_\_\_\_\_\_] (Kontrakt dostawy) Dostawca zobowiązuje się dostarczyć wyszczególnione w nim usługi („Usługi”), które mogą obejmować transfer i udostępnianie danych Osobowych między PPG a Dostawcą. |
| (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:** | (B) Strony uzgadniają, że postanowienia tej Umowy zostają włączone do warunków i postanowień Kontraktu dostawy oraz stanowią ich część. W zakresie, w jakim żadne postanowienia tej Umowy nie pozostają sprzeczne z żadnymi warunkami i postanowieniami Kontraktu dostawy, moc nadrzędną mają postanowienia tej Umowy.  **UZGADNIA SIĘ, CO NASTĘPUJE:** |
| 1. DEFINITIONS AND CLAUSES | 1. Definicje i klauzule |
| In this Agreement the following expressions bear the following meanings unless the context otherwise requires: | Jeśli kontekst nie stanowi inaczej, poniższe stwierdzenia użyte w niniejszej Umowie mają następujące znaczenia: |
| 1. **"Agreement Personal Data"** 2. Personal Data which is to be Processed under this Agreement, as more particularly described in **SCHEDULE 1** | 1. **„Dane Osobowe związane z Umową”** 2. Dane Osobowe, które są przetwarzane w ramach tej Umowy, opisane dokładniej w  **WYKAZIE 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 | „**Podmiot Powiązany”**  w odniesieniu do dowolnej osoby oznacza podmiot kontrolujący taką osobę, kontrolowany przez taką osobę lub pozostający pod wspólną kontrolą z taką osobą, w sposób bezpośredni lub pośredni, przez jednego lub większą liczbę pośredników. Do celów niniejszej definicji wyrażenie „kontrola” (w tym także wyrażenia „kontrolowana” i „pod wspólną kontrolą”) użyte w odniesieniu do dowolnej osoby oznacza posiadanie w sposób bezpośredni lub pośredni uprawnień do kierowania lub wpływania na kierowanie zarządzaniem i praktykami takiej osoby z tytułu posiadania, z tytułu wykonywania obowiązków powiernika (trustee) lub zarządcy, papierów wartościowych związanych z prawem głosu, na mocy umowy, w tym umowy kredytowej, bądź z innego tytułu. |
| 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. **„Przepisy Ochrony Danych”** 2. wszystkie obowiązujące przepisy związane z ochroną danych, przetwarzaniem danych Osobowych i prywatnością, między innymi:    1. Ogólne Rozporządzenie o Ochronie Danych (UE) 2016/679;    2. Brytyjska ustawa o ochronie danych (Data Protection Act) i Ogólne Rozporządzenie o Ochronie Danych stosowane na terenie Wielkiej Brytanii na mocy brytyjskiej ustawy o wystąpieniu z Unii Europejskiej (European Union (Withdrawal Act); oraz    3. Szwajcarska federalna ustawa o ochronie danych;   oraz wszelkie przepisy ustawodawcze i przepisy wykonawcze wdrażające je lub przyjęte na ich podstawie, zmieniające je, zastępujące je, przywracające je lub ujednolicające je  oraz odniesienia do **„Administratora Danych”, „Podmiotów Danych”**, **„Danych Osobowych”**, **„Procesu”**, **„Przetworzenia”**, **„Przetwarzania”**, **„Administratora”** oraz **„Organu Nadzorczego”** mają znaczenie zdefiniowane i interpretowane zgodnie z  obowiązującymi przepisami |
| 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 | 1. **„Incydent Bezpieczeństwa Danych”**    1. naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego uszkodzenia, utraty, modyfikacji, nieautoryzowanego ujawnienia lub dostępu do transmitowanych, zapisanych lub przetwarzanych w inny sposób Danych Osobowych związanych z Umową; lub    2. wykrycie lub uzasadnione podejrzenie powstania luki bezpieczeństwa w jakimkolwiek środku technologicznym używanym do ochrony jakichkolwiek Danych Osobowych związanych z Umową, które zostały wcześniej narażone na naruszenie w zakresie 1,, co może skutkować wykorzystaniem lub narażeniem Danych Osobowych związanych z umową; lub    3. jakikolwiek defekt lub jakakolwiek luka bezpieczeństwa, które może wpłynąć na trwałą odporność, bezpieczeństwo i/lub integralność systemów przetwarzających Dane Osobowe związane z Umową |
| 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 | **„Transfer międzynarodowy”**  transfer Danych Osobowych związanych z Umową poza terytorium Wielkiej Brytanii lub Szwajcarii bądź do kraju spoza Europejskiego Obszaru Gospodarczego, gdzie są natychmiast poddawane Przetwarzaniu albo mają zostać poddane Przetwarzaniu po pewnym czasie |
| 1. **"Sub-Processor"** 2. any third party Processor appointed by the Supplier to Process Agreement Personal Data | **„Dalszy Podmiot Przetwarzający”**  jakakolwiek będąca podmiotem przetwarzającym strona trzecia, której Dostawca zlecił Przetwarzanie Danych Osobowych związanych z Umową |
| 1. DATA PROTECTION AND INFORMATION SECURITY | **B. OCHRONA DANYCH I BEZPIECZEŃSTWO INFORMACJI** |
| 1. Authorisation and compliance with laws | 1. UPOWAŻNIENIE I ZGODNOŚĆ Z PRZEPISAMI |
| * 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 upoważnia Dostawcę, w imieniu własnym lub w imieniu Podmiotów powiązanych PPG, do Przetwarzania Danych Osobowych związanych z Umową w okresie obowiązywania niniejszej Umowy i w roli Podmiotu przetwarzającego, wyłącznie do celów oraz w zakresie opisanym w **WYKAZIE 1**. |
| * 1. In performing the Services and its other obligations under this Agreement the Supplier will: | * 1. Świadcząc Usługi oraz realizując zobowiązania wynikające z tej Umowy, Dostawca: |
| * + 1. comply with the Data Protection Laws; and | * + 1. będzie przestrzegać Przepisów Ochrony Danych; oraz |
| * + 1. not cause PPG or any PPG Affiliate to breach any obligation under the Data Protection Laws. | * + 1. nie spowoduje, że PPG albo jakikolwiek Podmiot Powiązany PPG naruszy jakiekolwiek zobowiązanie wynikające z Przepisów Ochrony Danych. |
| 1. processing of agreement personal data | 2. PRZETWARZANIE DANYCH OSOBOWYCH Związanych z UMOWą |
| * 1. The Supplier will: | * 1. Dostawca będzie: |
| 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. Przetwarzać Dane Osobowe związane z Umową wyłącznie zgodnie z udokumentowanymi instrukcjami otrzymanymi od PPG (które mogą mieć postać instrukcji szczegółowych lub instrukcji o charakterze ogólnym, zgodnie z ustaleniami w niniejszej Umowie lub innymi każdoczesnymi uzgodnieniami pomiędzy Stronami) albo odpowiedniego Podmiotu powiązanego PPG (chyba że Dostawca albo odpowiedni Dalszy Podmiot Przetwarzający jest zobowiązany do Przetwarzania Danych Osobowych związanych z Umową w myśl obowiązujących przepisów, którym podlega Dostawca; w takim przypadku Dostawca powiadomi PPG o takich wymogach prawnych przed Przetwarzaniem, z wyjątkiem sytuacji, w której obowiązujące przepisy zabraniają powiadomienia PPG w celu ochrony interesu publicznego; |
| 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. natychmiast informować PPG o ewentualnym, w swojej uzasadnionej ocenie, naruszeniu jakichkolwiek Przepisów Ochrony Danych przez jakiekolwiek instrukcje otrzymane od PPG lub Podmiotu Powiązanego PPG, przy czym Dostawca nie jest zobowiązany do podjęcia dodatkowych starań lub badań w celu ustalenia, czy instrukcje PPG są zgodne z tymi przepisami; |
| 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. bez uszczerbku dla **klauzuli 2.1.1** gwarantować, że Dane Osobowe związane z Umową będą wykorzystywane wyłącznie do celów oraz w zakresie opisanym w **WYKAZIE 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. bez uszczerbku dla **klauzuli 2.1.3** nie będzie bez uzyskania uprzedniej pisemnej zgody PPG lub odpowiedniego Podmiotu powiązanego PPG: |
| 2.1.4.1 convert any Agreement Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data; | * + - 1. konwertować jakichkolwiek Danych Osobowych związanych z Umową na żadne dane zanonimizowane, pseudonimizowane, zdepersonalizowane, zagregowane ani statystyczne; |
| 2.1.4.2 use any Agreement Personal Data for “big data” analysis or purposes; or | * + - 1. wykorzystywać żadnych Danych Osobowych związanych z Umową do analizy ani celów typu „big data”; |
| 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); | 2.1.4.3 dopasowywać ani porównywać żadnych Danych Osobowych związanych z Umową z jakimikolwiek innymi Danymi osobowymi (zarówno Dostawcy, jak i jakiejkolwiek strony trzeciej); |
| * + 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. dbać o to, aby jakakolwiek osoba upoważniona do Przetwarzania Danych Osobowych związanych z Umową uzyskiwała dostęp do tych danych wyłącznie na zasadzie ścisłej potrzeby oraz w związku z wykonywaniem obowiązków wynikających z realizacji tej Umowy oraz wyłącznie jeśli ta osoba: |
| * + - 1. is subject to binding confidentiality obligations in respect of Agreement Personal Data or is under an appropriate statutory obligation of confidentiality; | * + - 1. jest zobowiązana do przestrzegania wiążących wytycznych dotyczących poufności w zakresie Danych Osobowych związanych z Umową albo ma prawny obowiązek zachowania poufności; |
| * + - 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. przestrzega tej **klauzuli B**; oraz       2. jest odpowiednio rzetelna, wykwalifikowana i przeszkolona w zakresie własnych obowiązków dotyczących Przetwarzania Danych Osobowych związanych z Umową; oraz |
| * + 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. na życzenie PPG bezpiecznie usuwać albo zwracać PPG (w formacie zamówionym przez PPG) wszystkie Dane Osobowe związane z Umową niezwłocznie po zakończeniu świadczenia Usług związanych z Przetwarzaniem oraz w dowolnym czasie na żądanie, jak również bezpiecznie usuwać wszelkie pozostałe kopie i niezwłocznie powiadamiać o wykonaniu tego zobowiązania, chyba że obowiązujące przepisy wymagają od Dostawcy przechowywania Danych Osobowych związanych z Umową |
|  |  |
| 1. SECurity measures and incidents | 3. ŚRODKI BEZPIECZEŃSTWA I INCYDENTY |
| * 1. The Supplier will: | * 1. Dostawca będzie: |
| 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. wdrażać oraz pomagać PPG i Podmiotom Powiązanym PPG we wdrażaniu odpowiednich technicznych i organizacyjnych środków zgodnych co najmniej ze standardem przedstawionym w **WYKAZIE 2**, tak aby zapewnić poziom bezpieczeństwa odpowiedni do ryzyka wynikającego z Przetwarzania Danych Osobowych związanych z Umową, w szczególności wynikającego z Incydentów Bezpieczeństwa Danych; |
| 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. powiadamiać PPG niezwłocznie o uzasadnionym podejrzeniu zaistnienia Incydentu Bezpieczeństwa Danych lub o faktycznym zaistnieniu Incydentu Bezpieczeństwa Danych, w tym między innymi o naturze Incydentu Bezpieczeństwa Danych, kategoriach i przybliżonej liczbie Podmiotów Danych i odnośnej dokumentacji Danych Osobowych związanych z Umową, prawdopodobnych konsekwencjach Incydentu Bezpieczeństwa Danych oraz wszelkich proponowanych działaniach zaradczych i pozwalających uniknąć ewentualnych szkodliwych skutków Incydentu BezpieczeństwaDdanych. Jeśli, oraz o ile, nie jest możliwe jednoczesne dostarczenie wszystkich odnośnych informacji, informacje można przekazywać w etapach bez zbędnej zwłoki, lecz Dostawca (oraz Dalsze Podmioty Przetwarzające) nie może opóźniać powiadomienia w ramach tej **klauzuli 3.1.2** na podstawie stwierdzenia, że dochodzenie nie zostało zakończone albo nadal trwa; |
| 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. natychmiast powiadomić PPG, jeśli Dostawca lub Dalszy Podmiot Przetwarzający jest, lub powinien być, świadomy jakiejkolwiek przyczyny uniemożliwiającej zachowanie zgodności z tą **klauzulą 3.1.1**, bez uszczerbku dla swoich zobowiązań zachowania zgodności oraz dla jakichkolwiek praw lub środków zaradczych, które PPG może mieć do dyspozycji w razie naruszenia tej **klauzuli 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. niezwłocznie (w każdym przypadku do 72 godzin) powiadamiać PPG o jakimkolwiek otrzymanym żądaniu wyegzekwowania praw Podmiotu Danych wynikających z Przepisów Ochrony Danych oraz o komunikacji lub skardze odebranej od Podmiotu Danych lub Organu nadzorczego bądź innej strony trzeciej, a dotyczącej Danych Osobowych związanych z Umową; oraz |
| 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. nie będzie, bez uzyskania uprzedniej pisemnej zgody PPG, dokonywać ani zezwalać na dokonywanie żadnych oświadczeń dotyczących Incydentu Bezpieczeństwa Danych, jak również odpowiadać na jakiekolwiek żądanie wyegzekwowania praw Podmiotu Danych wynikających z Przepisów Ochrony Danych oraz na komunikację lub skargę odebraną od Podmiotu Danych lub Organu Nadzorczego, a dotyczącej Danych Osobowych związanych z Umową (z wyłączeniem przypadków, gdy wymagają tego odpowiednie przepisy). |
| 1. supplier assistance | 4. POMOC ZE STRONY DOSTAWCY |
| 4.1 Supplier will assist/provide reasonable assistance to PPG and PPG's Affiliates in: | * 1. Dostawca będzie pomagać lub zapewniać rozsądną pomoc PPG i Podmiotom Powiązanym PPG w następujących sytuacjach: |
| 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. odpowiadanie na żądania egzekwowania praw Podmiotu Danych wynikających z Przepisów Ochrony Danych oraz na komunikację i skargi Podmiotu Danych lub Organów nadzorczych bądź innych stron trzecich, dotyczących Danych Osobowych związanych z Umową, co obejmuje między innymi odpowiednie środki techniczne i organizacyjne, jeśli tylko jest to możliwe; |
| 4.1.2 documenting any Data Security Incidents and reporting any Data Security Incidents to any Supervisory Authority and/or Data Subjects; | * + 1. dokumentowanie jakichkolwiek Incydentów Bezpieczeństwa Danych oraz informowanie o takich incydentach jakichkolwiek Organów Nadzorczych i/lub Podmiotów Danych; |
| 4.1.3 conducting privacy impact assessments of any Processing operations and consulting with Supervisory Authorities, Data Subjects and their representatives accordingly; and | * + 1. przeprowadzanie ocen wpływu jakichkolwiek operacji Przetwarzania na prywatność oraz prowadzenie konsultacji z Organami Nadzorczymi, Podmiotami Danych i ich przedstawicielami; oraz |
| 4.1.4 taking measures to address Data Security Incidents, including without limitation, where appropriate, measures to mitigate their possible adverse effects. | * + 1. podejmowanie środków rozwiązujących Incydenty Bezpieczeństwa Danych , co obejmuje między innymi, jeśli to stosowne, środki umożliwiające unikanie ewentualnych szkodliwych skutków. |
| 1. appointment of subprocessors | 5. Wyznaczanie Dalszych Podmiotów przetwarzających |
| * 1. PPG agrees that the Supplier may engage Sub-Processors for the purposes of Processing Agreement Personal Data, provided that: | * 1. PPG wyraża zgodę na zaangażowanie przez Dostawcę Dalszych Podmiotów Przetwarzających do celów Przetwarzania Danych Osobowych związanych z Umową, przy czym: |
| * + 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     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. Dostawca może zaangażować wyłącznie takie Dalsze Podmioty Przetwarzające, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby Przetwarzanie było zgodne z niniejszą Umową oraz obowiązkami PPG i Dalszych Podmiotów Przetwarzających wynikających z Przepisów Ochrony Danych; oraz     2. Dostawca może w dowolnym momencie wyznaczyć nowy Dalszy Podmiot Przetwarzający pod warunkiem uprzedniego powiadomienia PPG w wyprzedzeniem 15 dni roboczych i przy braku sprzeciwu wobec takich zmian złożonego przez PPG w takim terminie. W przypadku złożenia przez PPG w takim terminie sprzeciwu wobec wyznaczenia nowego Dalszego Podmiotu Przetwarzającego, PPG może dokonać wobec Dostawcy pisemnego wypowiedzenia Usługi, która nie może być świadczona przez Dostawcę bez udziału Dalszego Podmiotu Przetwarzającego, którego sprzeciw dotyczy. |
| * 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 W przypadku wyznaczenia przez Dostawcę Dalszego podmiotu przetwarzającego do celów świadczenia części Usług obejmującej Przetwarzanie Danych Osobowych związanych z Umową Dostawca przed podjęciem Przetwarzania dopilnuje zawarcia pisemnego kontraktu między Dostawcą a Dalszym podmiotem przetwarzającym, określającego realizowane przez Dalszy Podmiot Przetwarzający działania Przetwarzania oraz nakładającego na Dalszy Podmiot Przetwarzający zobowiązania równoważne do tych, jakie ma Dostawca w związku z tą **klauzulą B**. Dostawca dopilnuje, aby Dalsze Podmioty Przetwarzające dotrzymywały wszystkich zobowiązań przedstawionych w tej **klauzuli B** oraz aby Dostawca pozostawał odpowiedzialny za wszelkie działania i zaniechania Dalszych podmiotów przetwarzający tak, jakby sam się ich dopuścił. |
| * 1. The Supplier shall maintain a list of Sub-Processors and shall promptly provide this to PPG on request. | 5.3 Dostawca zobowiązany jest do prowadzenia wykazu Dalszych Podmiotów Przetwarzających i do jego niezwłocznego udostępniania PPG na żądanie. |
| 1. international transfers | 6. Transfery międzynarodowe |
| * 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. Dostawca nie będzie wykonywać Transferu Międzynarodowego bez uzyskania uprzedniej pisemnej zgody PPG. Jeśli PPG udzieli wcześniejszej pisemnej zgody na Transfer międzynarodowy, przed wykonaniem takiego transferu Dostawca przedstawi lub wdroży, w ramach zaspokojenia satysfakcji PPG, odpowiednie środki bezpieczeństwa dot. Transferu Międzynarodowego zgodnie z Przepisami Ochrony Danych oraz zagwarantuje Podmiotom Danych dostępność możliwych do wyegzekwowania praw oraz skutecznych środków prawnych. Takie odpowiednie środki bezpieczeństwa mogą obejmować między innymi: |
| * + 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. kraj lub terytorium do którego odbywa się Transfer międzynarodowy, jest objęty ważną decyzją Komisji Europejskiej stwierdzającą odpowiedni stopnień ochrony lub odpowiedni stopnień ochrony został stwierdzony przy zastosowaniu innej ważnej metody na podstawie obowiązujących Przepisów Ochrony Danych; |
| * + 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: | * + 1. Dostawca zobowiązuje się do wypełniania obowiązków podmiotu odbierającego dane określonych w Standardowych Klauzulach Umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich, przyjętych na podstawie decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. opublikowanej pod numerem dokumentu C(2010) 593 2010/87/UE („Standardowe Klauzule Umowne”). Dostawca przyjmuje do wiadomości fakt, że PPG i Podmioty powiązane PPG wskazane przez PPG będą pełnić rolę podmiotu przekazującego dane. W szczególności i bez ograniczenia powyższego zobowiązania: |
| * + - 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 Dostawca zobowiązuje się do udzielenia Podmiotom Danych praw osoby trzeciej, na rzecz której zawarto umowę, zgodnie z klauzulą 3 Standardowych Klauzul Umownych, przy czym odpowiedzialność Dostawcy jest ograniczona do jego własnych operacji przetwarzania; |
| * + - 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 Dostawca przyjmuje do wiadomości fakt, że obowiązki Dostawcy wynikające ze Standardowych Klauzul Umownych podlegają przepisom prawa państwa członkowskiego (państw członkowskich), w którym (których) PPG lub Podmiot powiązany PPG będący podmiotem przekazującym dane posiada siedzibę; |
| * + - 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 strony oświadczają, że do celów klauzuli 5 lit. h) i klauzuli 11 Standardowych Klauzul Umownych PPG wyraża zgodę na zlecanie przez Dostawcę podwykonawstwa operacji zgodnie z **klauzulą 2** niniejszej Umowy; |
| * + - 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 strony uzgadniają, że wszelkie prawa do kontroli, o których mowa w klauzuli 5 lit. f) i klauzuli 12 ust. 2 Standardowych Klauzul Umownych są wykonywane zgodnie klauzulą 7 niniejszej Umowy. Strony uzgadniają, że w przypadku rozbieżności pomiędzy niniejszą Umową a Standardowymi Klauzulami Umownymi rozstrzygające znaczenie mają Standardowe Klauzule Umowne; oraz |
| * + - 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 szczegółowe informacje dotyczące załączników mających zastosowanie do Standardowych Klauzul Umownych określono w **WYKAZIE 1**, a wymagane środki bezpieczeństwa określono w **WYKAZIE 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 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 | * + 1. Transfer Międzynarodowy dokonywany jest do Stanów Zjednoczonych Ameryki, a, odpowiednio, Dostawca lub Dalszy Podmiot Przetwarzający posiada i utrzymuje przez okres Przetwarzania status bieżącej rejestracji w programie US-EU Privacy Shield. W zakresie, w jakim zastosowanie ma niniejsza klauzula 6.1.3, Dostawca zobowiązuje się do niezwłocznego powiadomienia PPG w formie pisemnej w przypadku, gdy, odpowiednio, Dostawca lub Dalszy Podmiot Przetwarzający zaprzestał utrzymywania takiego statusu, przewiduje jego uchylenie lub cofnięcie lub taki status został w inny sposób zakwestionowany przez organ nadzoru lub gdy według ustalenia własnego, odpowiednio, Dostawca lub Dalszy Podmiot Przetwarzający utracił zdolność do wypełniania obowiązków wynikających z programu Privacy Shield; lub |
| * + 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 odpowiednio, Dostawca lub Dalszy Podmiot Przetwarzający potwierdza, że wszelkie operacje Przetwarzania Danych Osobowych związanych z Umową są objęte wiążącymi regułami korporacyjnymi Dostawcy lub Dalszego Podmiotu Przetwarzającego, których postanowienia zostają włączone do niniejszych postanowień. Dostawca przyjmuje do wiadomości fakt, że PPG jako administratorowi danych przysługuje prawo do skutecznego powoływania się na powyższe wiążące reguły korporacyjne w stosunku do, odpowiednio, Dostawcy lub Dalszego Podmiotu Przetwarzającego, w tym prawo do odszkodowania w przypadku ich naruszenia. |
| * 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. Jeśli odpowiednie środki bezpieczeństwa przedstawione lub wdrożone przez Dostawcę (albo odpowiedniego Administratora danych / Administratora) zgodnie z tą **klauzulą 6** zostaną w dowolnym momencie uznane za dostarczające poziom ochrony nieodpowiedni dla Danych Osobowych związanych z Umową, Dostawca wdroży środki alternatywne wymagane przez PPG lub Podmiot Powiązany PPG, gwarantujące, że odnośny Transfer międzynarodowy i wszystkie wynikające z niego operacje Przetwarzania będą zgodne z Przepisami Ochrony Danych. Dostawca albo odpowiedni Dalszy Podmiot Przetwarzający nie będą zobowiązani warunkami przedstawionymi w tej **klauzuli 6**, jeśli Transfer Międzynarodowy jest wymagany w myśl obowiązujących przepisów Wielkiej Brytanii, Szwajcarii lub Unii Europejskiej albo krajów członkowskich Unii Europejskiej; przy czym Dostawca powiadomi PPG o takich wymogach prawnych przed Transferem międzynarodowym, z wyjątkiem sytuacji, w której obowiązujące przepisy zabraniają powiadomienia PPG w ramach ochrony interesu publicznego. |
| 1. audit rights | 7. prawa dotyczące kontroli |
| * 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. Dostawca będzie:      1. udostępniać PPG i Podmiotom Powiązanym PPG wszelkie informacje niezbędne do potwierdzenia zgodności z obowiązującymi Przepisami Ochrony Danych oraz ze zobowiązaniami wyszczególnionymi w tej **klauzuli B**; oraz |
| 7.1.2 allow for and contribute to audits, including without limitation inspections, conducted by PPG or another auditor mandated by PPG. | * + 1. zezwalać na audyty, w tym między innymi inspekcje, przeprowadzane przez PPG lub innych audytorów upoważnionych przez PPG, oraz współpracować w ramach tych audytów. |
| 1. indemnification | 8. odpowiedzialność odszkodowawcza |
| * 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. Dostawca zobowiązuje się zwolnić PPG i Podmioty powiązane PPG z wszelkich odszkodowań i/lub grzywien nałożonych na PPG lub którykolwiek Podmiot powiązany PPG, wynikających w każdym przypadku albo związanych z jakimkolwiek naruszeniem przez Dostawcę lub dowolny Dalszy Podmiot Przetwarzający jakichkolwiek zobowiązań wynikających z tej **klauzuli B** (co obejmuje między innymi jakiekolwiek nieskuteczne albo opóźnione wykonanie, niedbałe wykonanie oraz brak wykonania jakichkolwiek tych zobowiązań). |
| * 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. Jakiekolwiek naruszenie postanowień tej **klauzuli B** przez Dostawcę lub dowolny Dalszy Podmiot Przetwarzający będzie istotnym naruszeniem tej Umowy, którego nie da się usunąć, niezależnie od tego, czy doszło do jakiejkolwiek straty finansowej albo szkody wizerunkowej, oraz niezależnie od skali strat finansowych albo utraty korzyści, powstałych w wyniku takiego naruszenia. |
| **9.** This Agreement is executed in two versions, in Polish and English. In case of conflict, the English version will prevail. | **9.** Niniejsza umowa została sporządzona w dwóch wersjach językowych: po polsku i po angielsku. W razie rozbieżności pierwszeństwo ma wersja angielska. |
| Signed by PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  ………………………………………….. Signature  ………………………………………….. Name Director | Podpisano przez PPG [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  ………………………………………….. Podpis  ………………………………………….. Imię i nazwisko Dyrektor |
| Signed by Supplier [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]  …………………………………………. Signature  ………………………………………….. Name Director | Podpisano przez Dostawcę [\_\_\_\_\_\_\_\_\_\_\_]  …………………………………………. Podpis  ………………………………………….. Imię i nazwisko Dyrektor |
| |  |  | | --- | --- | | 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. wykaz 1 | | | 1. **Tematyka Przetwarzania** | [SZCZEGÓŁY] | | 1. **Czas Przetwarzania** | [SZCZEGÓŁY] | | 1. **Natura Przetwarzania** | [SZCZEGÓŁY] | | 1. **Cel Przetwarzania** | [SZCZEGÓŁY] | | 1. **Typ Danych Osobowych** | [SZCZEGÓŁY] | | 1. **Kategorie Podmiotów Danych** | [SZCZEGÓŁY] | |
|  |  |
| |  | | --- | | 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. wykaz 2 2. ŚRODKI BEZPIECZEŃSTWA | | **1. Fizyczna kontrola dostępu:**  Osobom nieupoważnionym uniemożliwiony zostaje fizyczny dostęp do obiektów, budynków lub pomieszczeń, w których znajdują się systemy przetwarzania danych służące do Przetwarzania Danych Osobowych związanych z Umową („**Centra danych**”).  Środki:  **Centra danych** zobowiązane są do przestrzegania ścisłych procedur bezpieczeństwa wprowadzanych w życie przez personel ochrony, kamery monitorujące, mechanizmy kontroli dostępu i inne środki w celu zapobiegania zagrożeniom dla wyposażenia i pomieszczeń **Centrum Danych**. Dostęp do systemów i infrastruktury stanowiących wyposażenie **Centrum Danych** otrzymują wyłącznie upoważnieni przedstawiciele. W celu zapewnienia odpowiedniej funkcjonalności urządzenia służące fizycznemu bezpieczeństwu (np., czujniki ruchu, kamery itp.) poddawane są regularnej konserwacji. W **Centrach Danych** wdrażane są w szczególności następujące fizyczne środki bezpieczeństwa:   * Dostawca ochrania swoje aktywa i obiekty przy wykorzystaniu odpowiednich środków w oparciu o wewnętrzną klasyfikację bezpieczeństwa. * Co do zasady, budynki są ochraniane przy wykorzystaniu systemów kontroli dostępu (systemu inteligentnych kart dostępu). * Jako wymóg minimalny, najbardziej zewnętrzna powłoka struktury budynku musi zostać wyposażona w system kluczy certyfikowanych, w tym także nowoczesny, aktywny system zarządzania kluczami. * W zależności od klasyfikacji bezpieczeństwa, budynki, poszczególne powierzchnie i tereny przyległe są chronione przy wykorzystaniu dodatkowych środków. Obejmują one profile dostępowe, nadzór wideo i antywłamaniowe systemy alarmowe * Uprawnienia w zakresie dostępu są indywidualnie udzielane upoważnionym osobom zgodnie z Zasadami Kontroli Dostępu do Systemów i Danych (zob. sekcje 2 i 3 poniżej). Dotyczy to również dostępu dla osób odwiedzających. Goście i odwiedzający budynek Dostawcy podlegają imiennej rejestracji w recepcji i poruszają się w towarzystwie upoważnionego personelu. * Pracownicy Dostawcy i personel zewnętrzny podlegają obowiązkowi noszenia identyfikatora we wszystkich lokalizacjach PPG i Dostawcy | | **2. Kontrola dostępu do systemów:**  Należy uniemożliwić korzystanie z systemów służących do przetwarzania danych bez upoważnienia.  Środki:   * Dostęp do kluczowych systemów, w tym do systemów służących do przechowywania i przetwarzania Danych Osobowych związanych z Umową, udzielany jest na zasadzie uprawnień wielopoziomowych. Procesy zapewniają upoważnionym użytkownikom odpowiednie uprawnienia do dodawania, usuwania i modyfikowania uprawnień innych użytkowników. * Wszyscy użytkownicy uzyskujący dostęp do systemów Dostawcy są identyfikowani przy pomocy unikalnego identyfikatora (identyfikatora użytkownika). * Dostawca dysponuje procedurami, dzięki którym wnioski dotyczące przydzielania uprawnień są realizowane wyłącznie w sposób zgodny z wytycznymi (np. uprawnienia nie są przydzielane bez upoważnienia). W przypadku, gdy dany użytkownik odchodzi z organizacji Dostawcy, jego uprawnienia w zakresie dostępu zostają anulowane. * Dostawca wprowadził zasady dotyczące haseł, które zabraniają udostępniania haseł, określają sposób postępowania w przypadku ujawnienia hasła, określają wymóg regularnej zmiany hasła i modyfikacji haseł domyślnych. Do celów uwierzytelniania przydzielane są indywidualne identyfikatory użytkownika. Wszystkie hasła muszą odpowiadać określonym wymogom minimalnym i podlegają przechowaniu w formie zaszyfrowanej. W przypadku haseł do domen system wymaga zmiany hasła co sześć miesięcy na nowe hasła zgodne z wymogami dotyczącymi złożoności haseł. Każdy komputer wyposażony jest blokadę ekranu chronioną hasłem. * Sieć firmowa dostawcy jest chroniona przed zagrożeniami z sieci publicznej poprzez firewalle. * Dostawca korzysta z aktualnego oprogramowania antywirusowego w punktach dostępu do sieci firmowej (dotyczy to kont e-mail), na wszystkich serwerach plików i na wszystkich stacjach roboczych. * Wdrożono system zarządzania aktualizacjami bezpieczeństwa w celu zapewnienia właściwej aktualizacji systemów pod kątem bezpieczeństwa. * Pełen dostęp zdalny do sieci firmowej Dostawcy i infrastruktury krytycznej jest chroniony w oparciu o silne procedury uwierzytelniania. | | **3. Kontrola dostępu do danych:**  Osoby uprawnione do korzystania z systemów przetwarzania danych uzyskują dostęp wyłącznie do tych Danych Osobowych związanych z Umową, do których mają prawo dostępu. W czasie przetwarzania, wykorzystywania i przechowywania Dane Osobowe związane z Umową nie mogą być czytane, kopiowane, modyfikowane ani usuwane bez upoważnienia.  Środki:   * Dostęp do danych Osobowych, poufnych lub szczególnie chronionych udzielany jest tylko tym osobom, które go rzeczywiście potrzebują. Oznacza to, że pracownicy lub osoby trzecie z zewnątrz mają dostęp do informacji, które są im niezbędne do wykonania powierzonej im pracy. Dostawca wykorzystuje koncepcję uprawnień, w ramach której sposób przydzielania uprawnień i rodzaj przydzielanych uprawnień podlegają udokumentowaniu. Wszystkie dane Osobowe, poufne lub inne dane wrażliwe podlegają ochronie zgodnie z polityką i normami bezpieczeństwa Dostawcy. * Wszystkie serwery produkcyjne usług Dostawcy są eksploatowane w odnośnych Centrach danych. Środki bezpieczeństwa chroniące aplikacje służące do przetwarzania danych Osobowych, poufnych lub innych danych szczególnie chronionych są regularnie kontrolowane. W tym celu Dostawca przeprowadza wewnętrzne i zewnętrzne testy bezpieczeństwa i testy penetracyjne systemów informatycznych. * Dostawca nie zezwala na instalację osobistego oprogramowania lub oprogramowania niezatwierdzonego przez Dostawcę w systemach wykorzystywanych w ramach jakiejkolwiek Usługi informatycznej. * Norma bezpieczeństwa Dostawcy określa sposób usuwania lub niszczenia danych i nośników danych. | | **4. Kontrola przesyłania danych**  W czasie transferu zabronione jest czytanie, kopiowanie, modyfikowanie lub usuwanie Danych Osobowych związanych z Umową bez upoważnienia.  Środki:   * W przypadku fizycznego transportu nośników danych Dostawca wdraża odpowiednio środki w celu zapewnienia uzgodnionych poziomów usług (np. w zakresie szyfrowania). * Dane Osobowe związane z Umową przesyłane wewnętrznymi sieciami Dostawcy podlegają ochronie jak inne dane poufne zgodnie z polityką bezpieczeństwa Dostawcy. * W trakcie przesyłania pomiędzy Dostawcą a PPG wszelkie dane podlegają szyfrowaniu. | | **5. Kontrola wprowadzania danych:**   * Dostępna jest możliwość wstecznego zbadania i ustalenia, czy i przez kogo w organizacji Dostawcy Dane Osobowe związane z Umową były wprowadzane, modyfikowane lub usuwane z systemów przetwarzania danych. * Dostawca udziela dostępu do Danych Osobowych związanych z Umową wyłącznie upoważnionym osobom do potrzeb powierzonej im pracy. * Dostawca wdrożył system dziennika czynności wprowadzania, modyfikacji i usuwania danych. | | **6. Kontrola zadań**  Dane Osobowe związane z Umową przetwarzane na zlecenie mogą być przetwarzane wyłącznie w sposób zgodny z Umową i związanymi z nią instrukcjami PPG.  Środki:   * Dostawca korzysta z mechanizmów kontroli i procesów pozwalających zapewnić zgodność z umowami zawartymi pomiędzy Dostawcą a jego klientami, Dalszymi podmiotami przetwarzającymi lub innymi usługodawcami. * W ramach swojej polityki bezpieczeństwa Dostawca wymaga przynajmniej takiego samego poziomu ochrony, jak w przypadku informacji „poufnych” w rozumieniu normy klasyfikacji informacji Dostawcy.. | | **7. Kontrola dostępności**  Dane Osobowe związane z Umową są chronione przed Incydentami Bezpieczeństwa Danych .  Środki:   * Dostawca korzysta z procesów tworzenia kopii zapasowych i innych środków zapewniających w razie potrzeby szybkie przywrócenie pracy krytycznych systemów biznesowych. * Dostawca korzysta z zasilania awaryjnego (np. UPS, akumulatory, prądnice itp.) w celu zapewnienia dostępności zasilania Centrum Danych. * Dostawca określił plany awaryjne oraz strategie przywracania ciągłości działania i odtwarzania awaryjnego dotyczące usług chmurowych. * Procesy i systemy awaryjne są regularnie testowane. | | **8. Kontrola separacji danych:**  Dane Osobowe związane z Umową nie są Przetwarzane ani przechowywane razem z Danymi osobowymi należącymi do innego klienta Dostawcy.  Środki:   * Dostawca wykorzystuje możliwości techniczne stosowanego oprogramowania (np.: obsługa wielu podmiotów (*multi-tenancy*) lub odrębne systemy) w celu zapewnienia separacji Danych Osobowych związanych z Umową od innych danych. * W miarę możliwości Dostawca utrzymuje dedykowane instancje dla każdego przetwarzania danych. | | **9. Kontrola integralności danych**  Zapewnia nienaruszalność, kompletność i aktualność Danych Osobowych związanych z Umową w trakcie czynności przetwarzania.  Środki:Dostawca wdrożył wielowarstwową strategię obrony jako środek chroniący przed modyfikacjami wprowadzanymi przez osoby nieupoważnione. Dotyczy to mechanizmów kontroli, o których mowa w powyższych sekcjach dotyczących kontroli i środków: W szczególności:   * firewalle; * centrum monitorowania bezpieczeństwa; * oprogramowanie antywirusowe; * kopie zapasowe i przywracanie systemu; * zewnętrzne i wewnętrzne testy penetracyjne; * regularne audyty zewnętrzne pod kątem środków bezpieczeństwa.. | |
|  |  |