base.

# REGULAMIN BASE

## UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

**(„Umowa Powierzenia")**

zawarta pomiędzy:

**Użytkownikiem** w rozumieniu Regulaminu („**Administrator**")

oraz

**BaseLinker sp. z o.o.** z siedzibą we Wrocławiu, Pl. Solny 15, 50-062 Wrocław, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS 0000795513, NIP 8971868567, REGON 383907714, e-mail: privacy@base.com („**Procesor**")

Administrator i Procesor zwani są dalej łącznie „**Stronami**", a każdy z osobna „**Stroną**".

### 1. Przedmiot Umowy Powierzenia

1.1. Przedmiotem Umowy Powierzenia jest, odpowiednio, powierzenie lub podpowierzenie przez Administratora Procesorowi przetwarzania danych osobowych, w związku z wykonywaniem umów zawartych przez Strony („**Umowy Główne**"), stosownie do art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1) („**RODO**").

1.2. Administrator powierza Procesorowi przetwarzanie danych osobowych w zakresie określonym w Umowie Powierzenia i w celu realizacji Umowy Głównej, a Procesor zobowiązuje się do przetwarzania danych osobowych zgodnie z Regulaminem i RODO.

1.3. Umowa Powierzenia ma odpowiednie zastosowanie do przypadków, gdy Administrator jest procesorem powierzonych danych osobowych – w takim przypadku Procesor staje się dalszym procesorem.

1.4. Umowa Powierzenia nie ma zastosowania do przypadków, w których Procesor przetwarza dane osobowe jako samodzielny administrator.

### 2. Zakres powierzenia przetwarzania

2.1. Administrator powierza Procesorowi przetwarzanie danych osobowych w następującym zakresie:

(a) kategorie osób, których dane dotyczą: personel, podwykonawcy, klienci, dostawcy lub kontrahenci Administratora;

(b) kategorie danych osobowych: w zakresie niezbędnym do realizacji Umowy Głównej oraz dane wprowadzone lub , w szczególności imię i nazwisko, przedrostek – Pan/Pani, nazwa firmy, NIP, adres siedziby, adres e-mail, adres dostawy, numer telefonu, szczegóły zamówienia.

2.2. Procesor jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie,

usuwanie lub niszczenie. Zakres operacji przetwarzania zależy od instrukcji Administratora, wydawanych co do zasady przez realizację Umowy Głównej.

## 3. Przetwarzanie wyłącznie na udokumentowane polecenie Administratora

3.1. Procesor będzie przetwarzał dane osobowe wyłącznie na podstawie postanowień Umowy Powierzenia oraz udokumentowanych poleceń Administratora.

3.2. Przetwarzanie danych osobowych w zakresie przekraczającym pkt. 2 wymaga zmiany Umowy Powierzenia.

3.3. Powyższe nie dotyczy przypadku, gdy Procesor działa w celu realizacji obowiązku, który nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Procesor, a realizacji tego obowiązku nie da się pogodzić z postanowieniami Umowy Powierzenia. Wówczas przed rozpoczęciem przetwarzania Procesor informuje Administratora o przedmiotowym obowiązku prawnym, o ile mające zastosowanie prawo nie zabrania udzielania takiej informacji.

## 4. Obowiązek zachowania tajemnicy

4.1. Procesor upoważnia do przetwarzania powierzonych mu danych osobowych wyłącznie tych członków swojego personelu, którzy zostali przeszkoleni z zakresu ochrony danych osobowych oraz są zaangażowanie w wykonywanie Umowy Głównej.

4.2. Procesor zapewnia, aby osoby, o których mowa w pkt. 4.1:

(a) przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej, oraz

(b) zobowiązały się do zachowania danych osobowych w tajemnicy lub aby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

## 5. Bezpieczeństwo przetwarzania

5.1. Procesor zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić zgodność przetwarzania z RODO, w tym stopień bezpieczeństwa przetwarzania odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą, prowadząc oraz aktualizując wyniki analizy ryzyka oraz realizując plan postępowania z ryzykiem. W szczególności, Procesor zobowiązany jest zapewnić ochronę powierzonych danych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, niedozwolonym ujawnieniem lub dostępem, przesłaniem, przechowywaniem lub przetwarzaniem w inny sposób, co mogłoby w szczególności prowadzić do fizycznego, materialnego lub niematerialnego uszkodzenia.

5.2. Środki bezpieczeństwa wdrożone przez Procesora zostały określone w Załączniku A.

5.3. Procesor zapewnia objęcie powierzonych danych osobowych wdrożonym w ramach organizacji Procesora systemem zarządzania bezpieczeństwem informacji w oparciu o normę ISO/IEC 27001.

5.4. Procesor nie może wykorzystywać danych osobowych dla innych celów niż wskazane w Umowie Powierzenia, w szczególności Procesor nie może bez wyraźnej zgody przekazać danych osobowych osobom trzecim, ani tworzyć kopii i duplikatów danych osobowych, z tym że zastrzeżenie powyższe nie obejmuje tworzenia kopii zapasowych w celu zapewnienia właściwego przetwarzania danych osobowych.

## 6. Dalsze powierzenie przetwarzania

6.1. Procesor może korzystać z usług dalszych procesorów w związku z realizacją Umowy Głównej. Lista dalszych procesorów, którym Procesor powierza przetwarzanie danych osobowych, stanowi Załącznik B.

6.2. Procesor zawiadamia Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych procesorów poprzez aktualizację Załącznika B. Administrator ma możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni od otrzymania zawiadomienia

poprzez wypowiedzenie Umowy Głównej ze skutkiem natychmiastowym. Dalsze wykonywanie Umowy Głównej przez Administratora oznacza, że Administrator nie wnosi sprzeciwu wobec aktualizacji Załącznika B.

6.3. Korzystanie z usług dalszego procesora jest dopuszczalne jedynie na podstawie umowy, która nakłada na ten podmiot takie same obowiązki ochrony danych, jakimi na podstawie Umowy Powierzenia objęty jest pierwotny Procesor.

6.4. Jeżeli ten dalszy procesor nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego dalszego procesora spoczywa na pierwotnym Procesorze.

6.5. Administrator uprawnia Procesora do nadawania upoważnień, wydawania instrukcji i poleceń rozumieniu art. 29 RODO w stosunku do dalszych procesorów.

## 7. Przekazywanie danych osobowych

7.1. W zakresie niezbędnym do prawidłowej obsługi infrastruktury teleinformatycznej Procesora oraz sprawnego funkcjonowania procesów w organizacji Procesora, w tym przechowywania dokumentów lub komunikacji między osobami zaangażowanymi w realizację Umowy Głównej, Procesor może przekazywać lub autoryzować przekazywanie powierzonych danych osobowych poza Europejski Obszar Gospodarczy.

7.2. Przekazywania danych osobowych do państw trzecich będzie się odbywać na podstawie decyzji, o której mowa w art. 45 ust. 3 RODO, a w razie jej braku – Procesor zapewni odpowiedni poziom ochrony poprzez rozwiązania określone w art. 46 RODO, w szczególności poprzez standardowe klauzule umowne przyjęte przez Komisję Europejską.

## 8. Odpowiadanie na żądania osoby, której dane dotyczą

8.1. Procesor stosuje środki organizacyjne i techniczne, umożliwiające Administratorowi wywiązanie się z obowiązku odpowiadania na żądania osoby, której dane dotyczą.

8.2. Jeżeli podmiot danych osobowych będzie wykonywać swoje prawo do dostępu, sprostowania, uzupełnienia, usunięcia, lub ograniczenia przetwarzania danych osobowych względem Administratora, Procesor będzie zobowiązany do realizacji prawa podmiotu danych osobowych zgodnie z poleceniami Administratora.

8.3. W razie wpływu do Procesora żądania w zakresie realizacji praw osób, których dotyczą powierzone dane, Procesor informuje o tym Administratora nie później niż 7 dni od otrzymania żądania. Udzielając informacji o żądaniu, Procesor przekazuje dane nadawcy i treść żądania.

## 9. Usunięcie lub zwrot danych osobowych

Nie później niż 30 dni po wygaśnięciu lub rozwiązaniu ostatniej Umowy Głównej pozostającej w mocy lub po otrzymaniu żądania Administratora, Procesor usunie wszelkie dane osobowe przetwarzane na podstawie Umowy Powierzenia oraz usunie wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych przez Procesora lub dane osobowe są przechowywane w kopiach zapasowych infrastruktury informatycznej Procesora utworzonych w zwykłym toku działalności.

## 10. Raportowanie

10.1. Na wniosek Administratora, Procesor udostępnia informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z art. 28 i art. 32-36 RODO.

10.2. Procesor bez zbędnej zwłoki, jednak nie później niż w ciągu 36 godzin od stwierdzenia naruszenia ochrony danych osobowych, zawiadomi o tym fakcie Administratora. Jeżeli Procesor nie będzie w stanie przekazać Administratorowi wyczerpujących informacji o stwierdzonym naruszeniu, wówczas będzie ich udzielać sukcesywnie bez zbędnej zwłoki.

## 11. Inspekcje

11.1. W celu weryfikacji spełniania obowiązków wynikających z Umowy Powierzenia, Administrator ma prawo przeprowadzenia inspekcji w zakresie, w jakim Procesor przetwarza dane powierzone przez Administratora. Administrator może przeprowadzić inspekcję samodzielnie lub przez osobę upoważnioną, nie częściej niż raz na 12 miesięcy, a ponadto w przypadku wystąpienia incydentu.

11.2. Przeprowadzenie inspekcji nastąpi w terminie uzgodnionym przez Strony, jednak nie wcześniej niż 5 Dni Roboczych od zawiadomienia Procesora o zamiarze przeprowadzenia inspekcji. Zawiadomienie powinno określać zakres inspekcji, osoby zaangażowane w jej przeprowadzenie i proponowany termin. Po otrzymaniu zawiadomienia o planowanej inspekcji Procesor ma prawo zawiadomić Administratora o nowym proponowanym terminie przeprowadzenia inspekcji, przypadającym nie później niż 10 Dni Roboczych po terminie zaproponowanym przez Administratora.

11.3. Wszelkie informacje i dokumenty, które zostaną udostępnione Administratorowi lub upoważnionej przez niego osobie, bądź sporządzone przez Administratora lub osobę przez niego upoważnioną, w związku z inspekcją, w tym wyniki inspekcji, są poufne i stanowią tajemnicę handlową Procesora („**Informacje Poufne**"). Administrator jest zobowiązany do zachowania w poufności Informacji Poufnych i gwarantuje, że osoby przez niego upoważnione zachowają w poufności Informacje Poufne, w szczególności Administrator i osoby upoważnione:

(a) powstrzymają się od ujawniania Informacji Poufnych osobom trzecim bez uprzedniej wyraźnej zgody Procesora wyrażonej w formie dokumentowej pod rygorem nieważności;

(b) nie będą wykorzystywać Informacji Poufnych do celów innych niż przeprowadzenie inspekcji, w szczególności do celów komercyjnych.

11.4. Administrator będzie zobowiązany do dostarczenia Procesorowi pisemnego zobowiązania osoby upoważnionej do przeprowadzenia inspekcji, do zachowania poufności w odniesieniu do Informacji Poufnych w zakresie określonym powyżej. Procesor ma prawo odmówić udzielenia odpowiedzi i dostępów osobie upoważnionej do przeprowadzenia inspekcji w imieniu Administratora, w przypadku gdy warunek określony w zdaniu poprzedzającym nie zostanie spełniony.

11.5. Inspekcja może zostać przeprowadzona w Dni Robocze. Inspekcja może zostać przeprowadzona wyłącznie w zakresie obejmującym kontrolę właściwej dokumentacji oraz uzyskania niezbędnych wyjaśnień dotyczących realizacji jej postanowień, oraz wyłącznie w zakresie, w jakim nie wymaga dostępu do systemów i urządzeń elektronicznych i informatycznych, z których Procesor korzysta przy świadczeniu usług, ponieważ zasoby te mogą przetwarzać także inne dane osobowe, nieobjęte stosunkiem powierzenia pomiędzy Stronami. Inspekcja będzie przeprowadzana w sposób niezakłócający bieżącej działalności Procesora, w przeciwnym wypadku Procesor ma prawo zawiesić inspekcję, jednocześnie wskazując Administratorowi proponowany termin jej wznowienia.

11.6. W przypadku, gdy inspekcja będzie nadmiernie uciążliwa lub wykracza poza zakres wskazany w zawiadomieniu o zamiarze przeprowadzenia inspekcji, Procesor może wstrzymać inspekcję i uzależnić jej kontynuację od uiszczenia opłaty dodatkowej, uwzględniając administracyjne koszty udzielenia informacji, udostępnienia dokumentów, prowadzenia komunikacji lub podjęcia innych żądanych lub koniecznych działań w związku z inspekcją.

11.7. Procesor ma prawo odmówić przekazania Administratorowi informacji objętych tajemnicą prawnie chronioną, w tym tajemnicą przedsiębiorstwa Procesora lub podmiotów trzecich, a także informacji stanowiących dane osobowe nie objęte Umową Powierzenia, jeśli informacje te mogą zostać zastąpione innymi informacjami (w tym oświadczeniami Procesora), zaś w przypadku gdy nie będzie to możliwe – informacje te zostaną udostępnione Administratorowi (lub wyznaczonym

przez niego osobom) wyłącznie w lokalizacji i pod nadzorem osoby wskazanej przez Procesora, po uprzednim zawarciu przez Strony i wszystkie osoby upoważnione przez Administratora do przeprowadzenia inspekcji, stosownej umowy zobowiązującej do należytej ochrony tych informacji.

## 12. Odpowiedzialność procesora

12.1. Procesor ponosi odpowiedzialność względem Administratora za wszelkie naruszenia wynikłe z niewykonania lub nienależytego wykonania Umowy Powierzenia.

12.2. Procesor nie ponosi żadnej odpowiedzialności wobec Administratora za szkodę powstałą wskutek nałożenia na Administratora przez organ nadzorczy administracyjnej kary pieniężnej lub innej sankcji administracyjnej z tytułu naruszenia ochrony danych osobowych przez Administratora.

## 13. Postanowienia końcowe

13.1. Niniejsza Umowa Powierzenia zostaje zawarta na czas trwania Umów Głównych.

13.2. Terminy pisane wielką literą, a inaczej niezdefiniowane, mają znaczenie nadane im w Regulaminie.

13.3. Terminy „dane osobowe", „przetwarzanie", „ograniczanie przetwarzania", „naruszenie ochrony danych osobowych" lub inne terminy zdefiniowane w RODO mają znaczenie nadane im w RODO i stosuje się je w odniesieniu do Administratora.

13.4. W sprawach nieuregulowanych Umową Powierzenia zastosowanie będą miały postanowienia Regulaminu oraz przepisy Kodeksu cywilnego oraz RODO.

13.5. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy Powierzenia będzie sąd właściwy dla siedziby Procesora.

13.6. W celach związanych z Umową Powierzenia, punktem kontaktowym po stronie Procesora jest adres e-mail: privacy@base.com.

base.

*ZAŁĄCZNIK A*

**ŚRODKI BEZPIECZEŃSTWA PROCESORA**

## Stan wdrożenia RODO

Projekt wdrożenia RODO został ukończony, Procesor posiada i utrzymuje wymagane przez RODO dokumenty, w tym rejestr wszystkich kategorii czynności przetwarzania.

System ochrony danych osobowych jest stale utrzymywany i poddawany regularnym przeglądom. Niezależne audyty systemu ochrony danych osobowych przeprowadzane są raz w roku, w razie potrzeby przeprowadzane są także audyty *ad hoc.*

Poziom bezpieczeństwa odpowiada zidentyfikowanym ryzykom i jest stale podnoszony. Procesor zapewnia poziom bezpieczeństwa powierzonych danych adekwatny do ryzyka naruszenia praw i wolności osób fizycznych, a w szczególności środki ochrony powierzonych danych osobowych przed przypadkowym zniszczeniem, utratą, modyfikacją i nieuprawnionym ujawnieniem.

Utrzymywane są aktualne wyniki analizy ryzyka dla zasobów przetwarzających powierzone dane osobowe. Realizowany jest plan postępowania z ryzykiem mający na celu utrzymywanie i stałe doskonalenie poziomu bezpieczeństwa danych osobowych. W razie identyfikacji podatności mogącej powodować istotne ryzyko, jest ona uwzględniana w ramach planu postępowania z ryzykiem, wraz z nadaniem odpowiedniego priorytetu.

Procesor przyjął dokumentację ochrony danych obejmująca wszystkie aspekty zgodności z RODO. Funkcjonujące w organizacji polityki i procedury są na bieżąco konsultowane, wyjaśniane i w razie potrzeby - aktualizowane we współpracy z zespołem inspektora ochrony danych.

W związku z pełnym wdrożeniem normy ISO/IEC 27001, w organizacji funkcjonuje także kompleksowa dokumentacja systemu zarządzania bezpieczeństwem informacji, która obejmuje swoim zakresem także system ochrony danych osobowych.

## Polityki i procedury ochrony danych osobowych

Procesor przygotował i przyjął polityki i procedury ochrony danych osobowych zgodnie z art. 24 ust. 2 RODO oraz z wymogami polskiego organu nadzorczego.

Polityki i procedury ochrony danych osobowych zostały zakomunikowane personelowi Procesora.

Procesor przygotował i wdrożył politykę bezpieczeństwa lub instrukcję zarządzania zasobami teleinformatycznymi.

Procesor przygotował procedurę niezwłocznego zgłaszania naruszeń bezpieczeństwa informacji do Administratora.

Osoby dokonujące operacji na danych osobowych zostały odpowiednio upoważnione do przetwarzania danych osobowych na podstawie art. 29 RODO.

Procesor prowadzi rejestr wszystkich kategorii czynności przetwarzania, który obejmuje wszystkie informacje wymagane na mocy art. 30 ust. 2 RODO.

Procesor jest w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych.

## Świadomość pracowników

Procesor zapewnia, że przed dopuszczeniem do przetwarzania danych osobowych zatrudniony członek personelu zostanie zapoznany z obowiązującymi politykami i procedurami ochrony danych.

Procesor zapewnia podnoszenie wiedzy swoich członków personelu poprzez okresowe szkolenia i inne działania mające na celu podnoszenie świadomości w zakresie ochrony danych osobowych i bezpieczeństwa informacji.

Pracownicy i współpracownicy Procesora, którzy biorą udział w przetwarzaniu danych osobowych, są zobowiązani do zachowania ich w tajemnicy.

Członkowie personelu Procesora, którzy biorą udział w przetwarzaniu powierzonych danych osobowych, otrzymali stosowne upoważnienia do przetwarzania danych osobowych, zaś ich dostępy do danych i uprawnienia są ograniczane zgodnie z zasadą wiedzy koniecznej.

## Zarządzanie naruszeniami, żądania osób fizycznych, wsparcie Administratora w wykazaniu zgodności z RODO

Procesor wdrożył procedurę postępowania w przypadku wykrycia możliwości naruszenia ochrony danych.

Procesor posiada środki umożliwiające realizację praw osób, których dane dotyczą, w szczególności prawa do ograniczenia przetwarzania oraz prawa do bycia zapomnianym.

Procesor terminowo zawiadamia Administratora w razie stwierdzenia naruszenia ochrony danych osobowych - w terminie wynikającym z postanowień Umowy Powierzenia. Procesor udziela odpowiedzi na pytania Administratora w zakresie i w terminach niezbędnych do wypełnienia powiązanych obowiązków wynikających z RODO.

## Inspektor ochrony danych oraz pozostałe funkcje związane z ochroną danych

Procesor wyznaczył inspektora ochrony danych, którego status odzwierciedla wymogi art. 38 RODO oraz który realizuje wszystkie zadania wskazane w art. 39 RODO.

Kontakt do inspektora ochrony danych: privacy@base.com.

Inspektor ochrony danych jest niezależny, zaś decyzje w odniesieniu do celów i sposobów przetwarzania spoczywają na przedstawicielu najwyższego kierownictwa oraz właścicielach procesów i zasobów.

W związku z funkcjonowaniem systemu zarządzania bezpieczeństwem informacji, powołano osoby pełniące funkcje odpowiadające wymogom normy ISO/IEC 27001, w szczególności Chief Information Security Officer.

## Kodeksy postępowania i mechanizmy certyfikacji, bezpieczeństwo informacji

Procesor wdrożył pełny system zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001 i posiada aktualny certyfikat potwierdzający prawidłowe wdrożenie i utrzymywanie systemu zarządzania bezpieczeństwem informacji (SZBI), zgodnie z ww. normą.

## Audyt i analiza ryzyka

Procesor poddaje swój system ochrony danych osobowych regularnemu, niezależnemu audytowi oraz testom bezpieczeństwa.

Procesor regularnie identyfikuje i klasyfikuje zasoby przetwarzające dane osobowe, w tym pod kątem posiadanych i planowanych zabezpieczeń, zidentyfikowanych podatności, prawdopodobieństwa wystąpienia i wagi zagrożeń.

Poziom bezpieczeństwa informacji jest dodatkowo monitorowany poprzez stosowanie kluczowych wskaźników efektywności (KPIs).

## Podwykonawcy

Procesor korzysta wyłącznie z usług takich podmiotów trzecich/podwykonawców, którzy zostali wcześniej zweryfikowani pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych.

Procesor weryfikuje adekwatność gwarancji udzielanych przez dalsze podmioty przetwarzające, w tym gdzie zasadne - poprzez zwrócenie się o wypełnienie kwestionariuszy i udzielenie odpowiedzi.

## Lokalizacje przetwarzania danych i transfery danych, przetwarzanie danych w chmurze

Co do zasady, Procesor przetwarza dane osobowe w centrach danych dostarczanych przez wyspecjalizowane dalsze podmioty przetwarzające, wskazane w Regulaminie Base, przy czym głównym dostawcą infrastruktury teleinformatycznej jest Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luksemburg. Gwarancje bezpieczeństwa od tego podmiotu opisane są pod adresem: https://aws.amazon.com/security/

Wszystkie powierzone dane osobowe są przechowywane wyłącznie w ramach infrastruktury dostarczanej przez wyspecjalizowane dalsze podmioty przetwarzające. Na okoliczność przetwarzania danych na własnych zasobach, Procesor wdrożył jednak zasady bezpieczeństwa fizycznego oraz zasady dotyczące bezpieczeństwa pracy zdalnej.

W zakresie, w jakim powierzone dane przetwarzane są w chmurze AWS, Procesor dokonuje oceny środków bezpieczeństwa stosowanych przez dostawcę, jak również uzupełnia je stosując wybrane przez Chief Information Security Officer i właścicieli zasobów narzędzia i rozwiązania konfiguracyjne. W szczególności, stosowane są szyfrowanie danych, weryfikacja poprawności rozwiązań konfiguracyjnych, monitorowanie użycia, skanowanie podatności, filtrowanie ruchu sieciowego, logowanie zdarzeń, zarządzanie dostępami, separacja, segmentacja i rozwiązania z zakresu redundancji i load balancingu.

## Bezpieczeństwo fizyczne

Fizyczne lokalizacje przetwarzania danych osobowych są objęte środkami kontroli dostępu, w tym tam gdzie to zasadne, systemu kart dostępowych, monitoringu wizyjnego, agencji ochrony oraz alarmu przeciwwłamaniowego.

Zasoby uczestniczące w przetwarzaniu danych przez Procesora są fizycznie odseparowane od innych organizacji.

Wdrożono zabezpieczenia minimalizujące ryzyko związane ze stratami w wyniku zagrożeń fizycznych i środowiskowych, w tym tam gdzie to zasadne - odpowiednie systemy wykrywania zagrożeń, w tym systemy przeciwpożarowe.

Uprawnienia dostępowe do obszaru przetwarzania danych osobowych są regularnie sprawdzane i w razie potrzeby cofane.

Uregulowano proces bezpiecznego usuwania danych oraz bezpiecznego wycofania z użycia nośników danych.

Dokumenty w formie papierowej są zabezpieczane przed nieuprawnionym dostępem zgodnie z zasadą czystego biurka, a po upływie ustalonych okresów przetwarzania - niszczone za pomocą niszczarki o standardzie nie niższym niż odpowiadający poufnym dokumentom.

## Kontrola dostępu do systemów informatycznych

Uprawnienia w ramach systemów informatycznych są nadawane zgodnie z zasadą wiedzy koniecznej, wdrożono politykę haseł.

Członkowie personelu są zobowiązani do stosowania zasady czystego biurka i ekranu.

Tam gdzie adekwatne, stosowane są środki kontroli dostępu, takie jak szyfrowanie, podwójne uwierzytelnianie i VPN.

## Bezpieczeństwo techniczne, konserwacja i testowanie sprzętu

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed awariami zasilania.

Konserwacja sprzętu i oprogramowania jest zgodna z zaleceniami dostawcy.

Przyjęto i stosuje się procedurę usuwania i niszczenia zasobów wycofywanych z użytku.

Zabezpieczenia serwerowni odpowiadają aktualnym standardom bezpieczeństwa.

Procesor zapewnia regularne testowanie, mierzenie i ocenę skuteczności środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania.

## Ciągłość działania

Procesor posiada plan ciągłości działania.

Wdrożono odpowiednie mechanizmy monitorowania i wykrywania zdarzeń, które mogą wpływać na bezpieczeństwo informacji i ciągłość działania.

Procesor jest w stanie sprawnie przywrócić dostępność i dostęp do danych osobowych w przypadku incydentu fizycznego lub technicznego.

Procesor wdrożył zasady tworzenia kopii zapasowych, obejmujące ich odpowiedni zakres, częstotliwość i testowanie.

Procesor wdrożył procedury odzyskiwania i testowania po awarii.

Wdrożono środki uniemożliwiające wykonanie nieautoryzowanych kopii danych z systemu informatycznego oraz zabezpieczające wykonane kopie zapasowe.

## Pozostałe wymogi RODO

Procesor wdraża nowe rozwiązania zgodnie z zasadą *privacy by design*.

Procesor przetwarza dane zgodnie z zasadą *privacy by default*.

Procesor prowadzi inwentaryzację zasobów wykorzystywanych przy przetwarzaniu danych osobowych.

***ZAŁĄCZNIK B***

**LISTA DALSZYCH PROCESORÓW**

1. Amazon Web Services EMEA SARL

   38 Avenue John F. Kennedy, L-1855 Luksemburg

   (spółka działająca przez swój oddział w Polsce:

   Amazon Web Services EMEA SARL sp. z o.o. Oddział w Polsce,

   Generation Park Z, 9th Floor, ul. Towarowa 28, 00-839 Warszawa)
2. OVH sp. z o.o.

   ul. Swobodna 1, 50-088 Wrocław
3. Bezpieczna Firma sp. z o.o.

   ul. Traktorowa 126/104, 91-116 Łódź
4. Google Ireland Ltd

   Gordon House Barrow Street Dublin 4, D04E5W5 Ireland
5. Slack Technologies, LLC

   500 Howard St San Francisco, CA 94105 United States
6. Twilio Ireland Limited

   25 – 28 North Wall Quay, North Wall, Dublin 1, D01 H104, Ireland
7. Cloudflare Inc.,

   101 Townsend Street San Francisco, CA 94107, USA
8. podmioty świadczące usługi wsparcia technicznego i bezpieczeństwa informatycznego, w tym usługi audytów bezpieczeństwa systemów informatycznych;
9. podmioty świadczące usługi prawne;
10. spółki powiązane Procesora, w zakresie, w jakim są zaangażowane w realizację Umowy Głównej.