

WARUNKI UŻYTKOWANIA Symphony Cloud

1. Zakres umowy

- Commend International GmbH z siedzibą pod adresem Saalachstrasse 51, 5020 Salzburg, Austria ("COMMEND", "my", "nas", "nasz") obsługuje oparte na chmurze rozwiązanie komunikacyjne skupiające się na aplikacjach zapewniających bezpieczeństwo, ochronę i produktywność ("Symphony" lub "Platforma"). Platforma obejmuje zarówno interfejs internetowy, jak i aplikacje mobilne.
- Platforma jest dystrybuowana przez podmioty stowarzyszone COMMEND, czyli wszystkie podmioty bezpośrednio lub pośrednio kontrolowane przez COMMEND lub jej spółkę holdingową, a także wszystkie podmioty, w których COMMEND ma i/lub będzie mieć udział, niezależnie od tego, czy jest to udział bezpośredni czy pośredni, większościowy czy mniejszościowy („Partnerzy dystrybucyjni”).
- Niniejsze warunki korzystania z Symphony („Warunki”) regulują relacje pomiędzy COMMEND a użytkownikiem Platformy („Użytkownik”) po zarejestrowaniu przez Użytkownika Konta. Niniejsze Warunki mają zastosowanie do każdego Użytkownika w odniesieniu do jego Subskrypcji bez względu na jego umowę z Partnerem Dystrybucyjnym.
- Niniejsze Warunki mają zastosowanie z wyłączeniem wszelkich innych warunków. W związku z tym potencjalnie sprzeczne warunki Użytkownika nie mają zastosowania.
- Ponieważ COMMEND stale się rozwija technologicznie, możemy od czasu do czasu zmieniać niniejsze Warunki, aby dodać dodatkowe funkcje lub dostosować klauzule ze względu na zmiany technologiczne. W takim przypadku udostępniemy Użytkownikom zaktualizowaną wersję pod adresem <https://www.commend.com/rd/cloud-terms-of-use-en>. Ponadto poinformujemy zarejestrowanych Użytkowników o zmianach za pośrednictwem poczty elektronicznej z wyprzedzeniem co najmniej 14 dni przed datą wejścia w życie zaktualizowanych Warunków. Jeśli zarejestrowany Użytkownik zakończy subskrypcję w ciągu 14 dni, uznaje się, że wyraża zgodę na zaktualizowane Warunki.
- Wszelkie inne zmiany Regulaminu zostaną uznane za zaakceptowane, jeśli COMMEND powiadomi zarejestrowanych Użytkowników o zmianach za pośrednictwem poczty elektronicznej z wyprzedzeniem co najmniej 14 dni przed datą wejścia w życie zaktualizowanego Regulaminu, a Użytkownik nie sprzeciwi się zmianom w ciągu 14 dni. W przypadku, gdy zarejestrowany Użytkownik zaprzeczy zmianom, uzgodniona wersja Regulaminu pozostaje w mocy.

2. Zakres usług

- Dokładna zawartość i zakres aktualnych funkcji i usług Platformy zostały opisane pod adresem <https://www.commend.com/rd/cloud-scope-of-service-en>.
- Usługi obejmują standardowe usługi wsparcia klienta danego Partnera Dystrybucyjnego uzgodnione bezpośrednio pomiędzy Użytkownikiem a Partnerem Dystrybucyjnym. Użytkownik może nabyć rozszerzone usługi wsparcia za pośrednictwem oddzielnej umowy z COMMEND lub odpowiednim Partnerem Dystrybucyjnym.
- COMMEND zastrzega sobie prawo do zmiany funkcji Platformy, jej aktualizacji i aktualizacji w dowolnym momencie, przy zachowaniu podstawowych funkcji Platformy. Ponadto COMMEND może dodawać nowe funkcje do Platformy. COMMEND może według własnego uznania korzystać z oprogramowania i produktów osób trzecich lub budować swoją Platformę i jej funkcjonalności w oparciu o oprogramowanie i produkty osób trzecich, na które Użytkownik musi uzyskać licencję.
- Jeżeli zakres usług obejmuje również oprogramowanie i produkty osób trzecich, które muszą być licencjonowane przez Użytkownika, COMMEND wskaże je odpowiednio w ofercie, chyba że Użytkownik jest tego świadomy. Składając zamówienie, Użytkownik upoważnia firmę COMMEND do zamówienia oprogramowania i produktów stron trzecich w imieniu i na rachunek Użytkownika. W takim przypadku zostaje nawiązany bezpośredni stosunek umowny między stroną trzecią a Użytkownikiem. Wszelkie roszczenia wynikające z tego stosunku będą rozstrzygane bezpośrednio i wyłącznie pomiędzy tymi stronami.
- COMMEND może od czasu do czasu i według własnego uznania angażować strony trzecie do świadczenia usług.

3. Rejestracja i konto użytkownika

- Aby móc aktywnie korzystać z Platformy, Użytkownicy muszą prawidłowo zarejestrować konto ("Konto"), wypełniając formularz rejestracyjny na naszej stronie internetowej, podając swój adres e-mail i wybierając hasło. Użytkownicy mogą podawać wyłącznie dokładne i kompletne informacje oraz niezwłocznie aktualizować informacje o swoim Koncie. Użytkownicy mogą zmienić informacje o swoim Koncie w dowolnym momencie za pośrednictwem Platformy.
- Użytkownicy ponoszą wyłączną odpowiedzialność za zachowanie poufności danych logowania do Konta (adresu e-mail i hasła). Użytkownicy zwolnią firmę COMMEND z odpowiedzialności za wszelkie szkody i koszty wynikające z zaniedbania obowiązku zachowania poufności danych logowania do Konta. Użytkownicy zobowiązani są do niezwłocznego powiadomienia firmy COMMEND w przypadku powzięcia informacji o nieuprawnionym użyciu danych logowania do Konta lub o jakimkolwiek innym naruszeniu bezpieczeństwa Platformy.
- COMMEND zastrzega sobie prawo do ograniczenia Użytkownikowi dostępu do Platformy w uzasadnionych przypadkach oraz czasowego lub bezterminowego zablokowania Konta, w szczególności w przypadku:
 - Użytkownik narusza niniejszy Regulamin lub obowiązujące przepisy prawa; lub
 - Działania Użytkownika mogą spowodować straty lub odpowiedzialność wobec innych Użytkowników lub wobec nas.
- Użytkownik może w każdej chwili usunąć swoje Konto w ramach Platformy. Usunięcie Konta nie ma wpływu na już istniejące roszczenia COMMEND lub jej Partnerów Dystrybucyjnych wobec Użytkownika w związku z Subskrypcją i aktywnością na Platformie.

4. Ograniczenia i obowiązki dotyczące użytkowania

- Ważne jest, aby Platforma była używana bezpiecznie i zgodnie z obowiązującymi przepisami prawa. W związku z tym Użytkownikom zabrania się w szczególności korzystania z Platformy ("Ograniczenia użytkowania"):
 - kopiowania, modyfikowania lub tworzenia dzieł pochodnych lub ulepszeń Platformy;
 - wynajmowania, wypożyczania, sprzedawania, udzielania sublicencji, cedowania, dystrybuowania, publikowania, przekazywania lub w inny sposób udostępniania jakiegokolwiek części Platformy nieupoważnionym osobom trzecim;
 - dekompilowania, dezasemblowania, odtwarzania kodu źródłowego, dekodowania, kopiowania, przenoszenia, uzyskiwania dostępu do kodu źródłowego Platformy lub w inny sposób korzystania z Platformy lub jakichkolwiek treści, z wyjątkiem przypadków dozwolonych przez prawo autorskie;
 - naruszania prawa (w tym prawa do prywatności i ochrony danych) innych osób;
 - przesyłania jakiegokolwiek materiałów, które promują, dostarczają lub odnoszą się do nielegalnych działań lub promują fizyczną krzywdę lub obrażenia wobec jakiegokolwiek osoby lub grupy;
 - przesyłania jakiegokolwiek materiałów, które mogą naruszać prawa własności intelektualnej lub inne prawa osób trzecich;
 - korzystania z Platformy w sposób, który
 - może przerwać, zawiesić, spowolnić lub utrudnić działanie Platformy,
 - stanowi włamanie lub próbę włamania się do Platformy lub naszej infrastruktury IT,
 - spowoduje przekierowanie zasobów systemowych platformy,
 - może spowodować nieproporcjonalne obciążenie infrastruktury Platformy,
 - stanowi atak na środki bezpieczeństwa i uwierzytelniania Platformy lub naszej infrastruktury IT;
 - włamywania się do systemu komputerowego strony trzeciej za pośrednictwem Platformy lub angażowania się w jakiegokolwiek działania, które mogą uszkodzić, kontrolować, zakłócać lub przechwytywać całość lub część systemu komputerowego strony trzeciej lub naruszać jego integralność lub bezpieczeństwo; rozpowszechniania jakiegokolwiek części Platformy w jakiegokolwiek formie bez uprzedniego pisemnego upoważnienia;

- i) nielegalnego przetwarzania danych osób, których dane dotyczą, wprowadzania stronicznych danych, algorytmów lub wzorców lub w inny sposób szkodenia osobom, których dane dotyczą, w szczególności poprzez wykorzystanie sztucznej inteligencji;
 - j) korzystania z Platformy do celów innych niż te, do których została zaprojektowana.
2. Użytkownik w pełni zabezpieczy firmę COMMEND przed wszelkimi roszczeniami, szkodami, zobowiązaniami, kosztami, stratami i wydatkami wynikającymi z
- niedbalstwa naruszenia niniejszych Warunków przez użytkownika,
 - niedbalstwa naruszenia przez użytkownika praw osób trzecich i/lub
 - jakiegokolwiek działania Użytkownika, które w wyniku zaniedbania wyrządziło szkodę spółce COMMEND lub osobie trzeciej.
3. Jeśli Użytkownik korzysta z usług asystenta głosowego opartego na sztucznej inteligencji, przyjmuje do wiadomości, że funkcja ta powinna być regularnie szkolona przez firmę COMMEND. W związku z tym w ramach wdrażania usług asystenta głosowego opartego na sztucznej inteligencji użytkownik zamieszcza oświadczenie COMMEND o wyrażeniu zgody na wykorzystanie zebranych danych do własnych celów szkoleniowych i udostępni użytkownikom końcowym politykę prywatności COMMEND. Sformułowanie zostanie dostarczone z góry przez COMMEND.

5. Subskrypcja

Partnerzy Dystrybucyjni COMMEND oferują różne modele subskrypcji w celu korzystania z Platformy ("Subskrypcja"). W związku z tym umowa dotycząca Subskrypcji będzie zawierana oddzielnie z danym Partnerem Dystrybucyjnym.

6. Własność intelektualna

1. COMMEND udziela Użytkownikowi niewyłącznego, niezbywalnego i niepodlegającego sublicencjonowaniu prawa do korzystania z Platformy w okresie obowiązywania Subskrypcji oraz w zakresie niezbędnym do korzystania z funkcji Platformy. Ponadto wszystkie elementy Platformy, takie jak teksty, zdjęcia, ilustracje, a także projekt i struktura Platformy, oprogramowanie bazowe i baza danych pozostają wyłączną własnością intelektualną firmy COMMEND lub jej partnera i podlegają ochronie praw autorskich. O ile COMMEND nie wyrazi na to wyraźnej zgody na piśmie, elementy te nie mogą być kopiowane, przesyłane, udostępniane, prezentowane, wykonywane, modyfikowane, tłumaczone ani wykorzystywane przez Użytkownika.
2. COMMEND jest uprawniony do kontroli, analizy i audytu sposobu korzystania z Platformy przez Użytkownika w celu sprawdzenia, czy Użytkownik przestrzega niniejszych Warunków. W związku z tym Użytkownik zapewni spółce COMMEND wszelkie wymagane informacje oraz odpowiedni dostęp do swoich systemów i ksiąg, tak aby spółka COMMEND mogła w uzasadniony sposób ocenić przestrzeganie Regulaminu przez Użytkownika.
3. Użytkownik niniejszym przyznaje firmie COMMEND niewyłączne, zbywalne, podlegające sublicencjonowaniu, nieodpłatne, ogólnosiątkowe i bezterminowe prawo do wykorzystywania, hostowania, przechowywania i powielania wszystkich danych, informacji i treści dostarczanych za pośrednictwem Konta Użytkownika (w szczególności zdjęć, filmów i plików audio). To prawo do użytkowania jest ograniczone do celu obsługi i ulepszania Platformy oraz jej usług/funkcjonalności.
4. Użytkownicy oświadczają i gwarantują, że posiadają wszelkie prawa, uprawnienia i upoważnienia niezbędne do przyznania spółce COMMEND praw określonych powyżej.

7. Gwarancja i dostępność platformy

1. COMMEND świadczy swoje usługi i Platformę z należytą starannością.
2. COMMEND gwarantuje, że Platforma jest dostępna dla Użytkownika przez 99% każdego miesiąca kalendarzowego. Jednakże następujące okoliczności nie będą brane pod uwagę przy obliczaniu dostępności Platformy:
 - konserwacyjne i serwisowe ogłaszane na naszej stronie internetowej z wyprzedzeniem co najmniej pięciu dni

kalendarzowych;

- wszelkie awarie systemu, oprogramowania, sieci lub sprzętu występujące poza sferą wpływu lub kontroli COMMEND lub wynikające z działania Siły Wyższej;
 - awarie lub błędy spowodowane przez Użytkownika lub osoby trzecie, które można przypisać Użytkownikowi, w szczególności z powodu niewłaściwej obsługi, nieprzestrzegania specyfikacji technicznych i warunków użytkowania lub korzystania z niekompatybilnych urządzeń.
3. Dane przetwarzane za pośrednictwem Platformy (w szczególności zdjęcia, filmy i pliki audio) są dostarczane głównie przez Użytkowników lub osoby trzecie korzystające z systemu. Ze względu na duży zakres treści, informacji, materiałów i danych, COMMEND nie ma wpływu na legalność tych treści, nie przyjmuje ich jako własnych i udostępnia treści bez jakichkolwiek gwarancji, zarówno wyraźnych, jak i dorozumianych.

8. Odpowiedzialność

1. COMMEND nie ponosi odpowiedzialności za szkody spowodowane lekkim zaniedbaniem. Niniejsze ograniczenie odpowiedzialności nie ma zastosowania do szkód spowodowanych naszym rażącym niedbalstwem lub umyślnym działaniem, uszczerbkiem na życiu, szkodą na osobie lub uszczerbkiem na zdrowiu oraz roszczeniami wynikającymi z ustawy o odpowiedzialności za produkt.
2. Ponadto spółka COMMEND nie ponosi odpowiedzialności za wady lub niedostarczenie Platformy spowodowane okolicznościami pozostającymi poza naszą kontrolą. Okoliczności takie obejmują strajki, wojny, katastrofy naturalne, awarie Internetu.
3. Użytkownik ponosi wyłączną odpowiedzialność za:
 - a) informacje, dane i inne treści przetwarzane przez Użytkownika za pośrednictwem Platformy,
 - b) infrastrukturę informatyczną Użytkownika, w tym komputery, oprogramowanie, bazy danych i sieci oraz
 - c) wszelki dostęp do Platformy i korzystanie z niej przez systemy Użytkownika lub za ich pośrednictwem.
4. Platforma może zawierać zintegrowane usługi stron trzecich i łączy umożliwiające dostęp do stron internetowych lub usług stron trzecich ("Usługi stron trzecich"), które nie są własnością COMMEND ani nie są przez nią kontrolowane. Takie usługi stron trzecich podlegają własnym warunkom użytkowania. Nie kontrolujemy Usług stron trzecich i nie ponosimy odpowiedzialności za ich zawartość. Firma COMMEND nie ponosi odpowiedzialności za techniczną dostępność Usług Zewnętrznych, ich treści, reklam, produktów i/lub usług.

9. Ochrona danych

5. Wrażliwe traktowanie wszystkich danych osobowych ma dla firmy COMMEND ogromne znaczenie. W związku z tym spółka COMMEND przestrzega obowiązujących przepisów o ochronie danych i wdrożyła odpowiednie i najnowocześniejsze środki bezpieczeństwa danych. Więcej informacji na temat przetwarzania danych osobowych przez spółkę COMMEND można znaleźć w naszej Polityce prywatności pod adresem <https://www.commend.com/rd/cloud-privacy-policy-en>.
6. W celu uniknięcia wątpliwości COMMEND należy zakwalifikować jako administratora danych wszystkich danych osobowych dotyczących Użytkowników, którzy korzystają z Symphony w ramach działalności czysto osobistej lub domowej. W pozostałych przypadkach COMMEND działa jako podmiot przetwarzający dane Użytkownika i zawiera z nim odrębną umowę powierzenia przetwarzania danych.

10. Warunki

7. Subskrypcja Użytkownika jest zasadniczo zawierana na okres uzgodniony między odpowiednim Partnerem Dystrybucyjnym a Użytkownikiem.
8. W celu uniknięcia wątpliwości, COMMEND będzie świadczyć swoje usługi zgodnie z niniejszymi Warunkami przez okres trwania odpowiedniej Subskrypcji uzgodnionej pomiędzy Partnerem Dystrybucyjnym a Użytkownikiem, pod warunkiem przestrzegania przez Użytkownika niniejszych Warunków.
9. Ponadto dostęp Użytkownika do Platformy może zostać zablokowany przez COMMEND ze skutkiem natychmiastowym z ważnego powodu w przypadku naruszenia niniejszych Warunków.

11. Prawo właściwe i jurysdykcja

1. Niniejsze Warunki i wszelkie spory prawne wynikające z korzystania z Platformy podlegają prawu Republiki Austrii, z wyjątkiem norm kolizyjnych i Konwencji Narodów Zjednoczonych o sprzedaży.
2. W przypadku sporów dotyczących niniejszych Warunków i korzystania z Platformy właściwe są sądy w Salzburgu w Austrii.

UMOWA LICENCYJNA NA OPROGRAMOWANIE ATLAS Access

1. Cel i zastosowanie

1. Niniejsza Umowa Licencyjna na Oprogramowanie ma zastosowanie do świadczenia Usług przez TKH Security na rzecz Klienta za pośrednictwem Platformy.
2. Niniejsza Umowa Licencyjna na Oprogramowanie nie obejmuje warunków sprzedaży Sprzętu Klientowi, w tym gwarancji i zobowiązań związanych ze sprzedażą i użytkowaniem Sprzętu. Ogólne warunki TKH Security, określone w odpowiedniej ofercie, mają zastosowanie do sprzedaży i użytkowania Sprzętu.
3. Niniejsza Umowa Licencyjna na Oprogramowanie, wraz z Umową o Przetwarzanie Danych, stanowi kompletną Umowę dotyczącą Usług świadczonych przez TKH Security oraz korzystania przez Klienta z Usług i dostępu do nich za pośrednictwem Platformy. Zastępuje ona wszelkie wcześniejsze umowy między Stronami lub wszelkie wcześniej stosowane przez TKH Security ogólne warunki dotyczące tych kwestii. W przypadku jakichkolwiek rozbieżności między Umową licencyjną na oprogramowanie a Umową o przetwarzaniu danych, ta ostatnia ma pierwszeństwo.
4. Wszelkie zasady, warunki lub postanowienia, które są sprzeczne, modyfikują, uzupełniają lub odbiegają od niniejszej Umowy, są ważne tylko wtedy, gdy zostały uzgodnione na piśmie przez obie Strony. Zastosowanie jakichkolwiek innych potencjalnych warunków sprzedaży lub innych warunków Klienta jest wyraźnie wykluczone.
5. Terminy pisane wielką literą w niniejszej Umowie Licencyjnej na Oprogramowanie mają znaczenie określone w Załączniku 1, z wyjątkiem terminów pisanych wielką literą w Umowie DPA, które są w niej zdefiniowane.

2. Zmiany umowy

1. TKH Security zastrzega sobie prawo do zmiany niniejszej Umowy w dowolnym momencie. W tym celu TKH Security powiadomi Klienta drogą elektroniczną (np. za pośrednictwem poczty elektronicznej, aplikacji internetowej lub aplikacji mobilnej) o wszelkich modyfikacjach. Po otrzymaniu takiego powiadomienia Klient ma piętnaście (15) dni kalendarzowych na wyraźne odrzucenie tych modyfikacji, jak określono w powiadomieniu TKH Security. Brak odrzucenia modyfikacji w tym okresie oznacza akceptację zmienionej Umowy.
2. Jeśli Klient nie odrzuci modyfikacji w określonym terminie, zostaną one uznane za zaakceptowane i w pełni obowiązujące. Ponadto, jeśli Klient zawrze nową Umowę z TKH Security, wyżej wymienione zmiany zostaną również uznane za zaakceptowane przez Klienta.

3. Zawarcie umowy

1. Klient przyjmuje do wiadomości, że Usługi opisane w niniejszej Umowie Licencyjnej na Oprogramowanie nie mogą być świadczone w połączeniu z jakimkolwiek innym sprzętem niż Sprzęt dostarczony przez TKH Security lub Partnera TKH Security.
2. Warunki określone w Dokumentacji Partnera, uzgodnione między Partnerem TKH Security a Klientem, nie będą wiążące ani egzekwowalne wobec TKH Security ani żadnej innej spółki z Grupy TKH Security, chyba że zostanie to wyraźnie uzgodnione w niniejszej Umowie.
3. Umowę uznaje się za sformalizowaną i wykonaną dopiero po zaakceptowaniu przez Klienta niniejszej Umowy Licencyjnej Oprogramowania, poprzez kliknięcie pola "Akceptuję" lub innego równoważnego pola, oraz po pomyślnym zakończeniu procesu Rejestracji opisanego w Artykule 4 poniżej.

4. Rejestracja

1. Po zaakceptowaniu Oferty Klient otrzyma Dane Konta, za pomocą których będzie mógł dokonać Rejestracji na Platformie.
2. Po zakończeniu Rejestracji, która obejmuje akceptację niniejszej Umowy licencyjnej oprogramowania i Umowy o przetwarzaniu danych, Klient może uzyskać dostęp do Witryny, podłączyć swoje środowisko EntraID i korzystać z Usług.
3. Klient jest odpowiedzialny za ostrożne i poufne obchodzenie się z

Danymi Konta, przyjmując na siebie pełne ryzyko. Obejmuje to podjęcie uzasadnionych wysiłków, takich jak wdrożenie odpowiednich środków bezpieczeństwa, w celu zapobieżenia nieautoryzowanemu dostępowi do Usług za pośrednictwem Danych Konta i Strony Klienta. Klient przyjmuje do wiadomości pełną odpowiedzialność za wszelkie działania podejmowane przy użyciu jego Danych Konta (jak wyszczególniono w Artykule 15 poniżej), przy czym TKH Security nie ponosi żadnej odpowiedzialności w przypadku podejrzenia utraty, kradzieży lub niewłaściwego wykorzystania Danych Konta przez osoby trzecie.

5. Serwis

1. W okresie obowiązywania niniejszej Umowy i tak długo, jak Klient wypełnia wszelkie stosowne zobowiązania i przestrzega niniejszej Umowy Licencyjnej Oprogramowania, TKH Security przyznaje Klientowi określoną w Wycenie kwotę osobistego, ograniczonego, niewyłącznego i niezbywalnego prawa (praw) do korzystania z Usług.
2. Prawo użytkowania przyznane Klientowi przez TKH Security na mocy Artykułu 5.1. podlega następującym zakazom:
 - a) Klientowi nie wolno sprzedawać, odsprzedawać, przenosić, cedować, dystrybuować ani w inny sposób wykorzystywać komercyjnie Subskrypcji i/lub prawa dostępu do Usług bez wyraźnej uprzedniej zgody TKH Security. Subskrypcji i/lub prawa dostępu i korzystania z Usług bez wyraźnej i uprzedniej zgody TKH Security.
 - b) Klient nie zezwoli żadnym nieupoważnionym osobom na dostęp do Usług lub korzystanie z nich.
 - c) Klient powstrzyma się od dokonywania jakichkolwiek zmian na Platformie.
 - d) Klientowi nie wolno modyfikować, dekompilować, odtwarzać kodu źródłowego ani kopiować Platformy, Usług ani żadnych ich składników.
 - e) Klient nie będzie korzystał z Usług i Platformy w sposób niezgodny z prawem, nielegalny, oszukańczy lub szkodliwy. Obejmuje to angażowanie się lub ułatwianie jakichkolwiek niezgodnych z prawem, nielegalnych, oszukańczych lub szkodliwych działań lub korzystanie z Usług w celach naruszających prawa osób trzecich.
 - f) Klient nie będzie korzystał z Usług lub Platformy w sposób, który może spowodować uszkodzenie Usług lub Platformy lub zakłócić dostępność Usług. W szczególności, ale nie wyłącznie, Klient nie będzie wykorzystywał Usług i Platformy do inicjowania lub rozpowszechniania Złośliwego oprogramowania..
3. Klient nie ma prawa dostępu do kodu oprogramowania (w tym kodu obiektowego, kodu pośredniego i kodu źródłowego) Platformy, ani w okresie obowiązywania niniejszej Umowy, ani po jej wygaśnięciu.

6. Usługi wsparcia

1. Na życzenie Klienta TKH Security może oferować usługi wsparcia technicznego w kwestiach dotyczących korzystania i działania Platformy. Usługi te będą zgodne ze standardowymi zasadami wsparcia TKH Security lub w sposób szczegółowo określony w pisemnym porozumieniu obu Stron.
2. Klient zachowuje możliwość zawarcia z Partnerem umowy o świadczenie usług wsparcia technicznego. W celu wyjaśnienia, wszelkie skargi dotyczące świadczenia usług wsparcia uzgodnionych między Klientem a Partnerem powinny być kierowane do Partnera. TKH Security nie ponosi odpowiedzialności za jakiegokolwiek bezpośrednie lub pośrednie szkody wynikające ze świadczenia takich usług wsparcia.

7. Aplikacja mobilna i aplikacja internetowa

1. Strony przyjmują do wiadomości i zgadzają się, że ich odpowiednie prawa, obowiązki i zobowiązania dotyczące Aplikacji mobilnej i/lub Aplikacji internetowej oraz wszelkie zobowiązania wynikające z korzystania z tych Aplikacji mogą podlegać odrębnym warunkom różniącym się od niniejszej Umowy licencyjnej oprogramowania.
2. Strony przyjmują do wiadomości i zgadzają się, że świadczenie Usług za pośrednictwem Aplikacji Mobilnej i/lub Aplikacji Internetowej jest uzależnione od dostępności wyżej wymienionej aplikacji w danym kraju oraz warunków określonych w Umowie Licencyjnej Użytkownika Końcowego.

8. Opłaty i metody płatności

1. W zamian za przyznane prawa i obietnice złożone przez TKH Security w ramach niniejszej Umowy, Klient zobowiązuje się zapłacić TKH Security kwoty określone w odpowiedniej Wycenie. Klient zgadza się w pełni opłacić wszystkie faktury, bez potrąceń lub innych odliczeń, nie później niż w terminie ich wymagalności.
2. W przypadku zakupu Usług Subskrypcji od Partnera, Opłaty uiszczane przez Klienta za każdą Subskrypcję za dostęp i korzystanie z Usług są określone w odpowiedniej Dokumentacji Partnera lub w inny sposób uzgodnione między Klientem a Partnerem. Odpowiednia faktura wystawiona przez Partnera musi zostać w pełni opłacona przed aktywacją Subskrypcji.
3. TKH Security zastrzega sobie prawo do corocznego dostosowywania Opłat abonamentowych.

9. Odnowienie i anulowanie subskrypcji

1. W przypadku Subskrypcji zarządzanych za pomocą rozliczeń cyklicznych, Subskrypcja zostanie automatycznie odnowiona na koniec okresu Subskrypcji i obciążona za pomocą metody płatności wskazanej przez Klienta, chyba że Klient anuluje swoją Subskrypcję. Klient może anulować Subskrypcję zgodnie z warunkami zawartymi w Ofercie i nadal będzie mieć dostęp do Usług do końca okresu Subskrypcji. Płatności za Subskrypcję nie podlegają zwrotowi (chyba że niniejsza Umowa Licencyjna Oprogramowania stanowi inaczej), a TKH Security nie zapewnia zwrotów ani kredytów za okres między datą anulowania a końcem okresu rozliczeniowego.
2. Jeżeli Klient nie uiścił Opłat należnych Partnerowi lub TKH Security w terminie i w związku z tym zalega z płatnościami, TKH Security jest uprawniona do rozwiązania Umowy ze skutkiem natychmiastowym oraz do natychmiastowego zawieszenia Usług i odmowy dostępu do Platformy i/lub Usług. W takim przypadku Klient ponosi odpowiedzialność za wszelkie bezpośrednie i pośrednie szkody poniesione przez TKH Security, obejmujące między innymi utratę zysków i koszty związane ze środkami sądowymi i pozasądowymi.

10. Serwisowanie i konserwacja oraz inne ograniczenia użytkowania

1. W przypadku, gdy TKH Security zaplanuje z wyprzedzeniem jakąkolwiek ogólną konserwację Platformy i/lub Usług, która może mieć wpływ na dostępność wyżej wymienionych, TKH Security powiadomi Klienta z wyprzedzeniem o zaplanowanej konserwacji.
2. Bez uszczerbku dla powyższego, TKH Security jest uprawniona w dowolnym momencie do natychmiastowego zablokowania, zawieszenia lub ograniczenia korzystania z (części) Usług i/lub dostępu do (części) Platformy i/lub podjęcia innych środków, jeśli uzna to za konieczne w opinii TKH Security, w celach konserwacyjnych lub w celu zapewnienia zgodności z wymogami ustawowymi, bez prawa Klienta do żądania odszkodowania za jakiegokolwiek poniesione szkody lub straty (ani bezpośrednie, ani pośrednie). W każdym przypadku TKH Security doloży uzasadnionych starań, aby zminimalizować takie zakłócenia w świadczeniu Usług.
3. Jeśli to możliwe, TKH Security poinformuje Klienta z wyprzedzeniem o takich środkach. W przypadku, gdy takie wcześniejsze powiadomienie nie jest możliwe ze względu na okoliczności, po zawieszeniu TKH Security przekaże Klientowi pisemne powiadomienie określające przyczynę zawieszenia.
4. Klient jest zobowiązany do zapewnienia wszelkiej współpracy wymaganej przez TKH Security w celu serwisowania i konserwacji, w tym do zaprzestania korzystania z Usług przez Klienta, jeśli TKH Security uzna to za konieczne.

11. Dostępność i zawieszenie usług

1. TKH Security doloży wszelkich starań, aby utrzymać dostępność Usług dla Klienta, ale TKH Security nie gwarantuje 100% dostępności.
2. TKH Security gwarantuje dostępność Usług na poziomie 99,9% mierzoną w skali miesiąca. Niezależnie od tego, następujące elementy nie będą uwzględniane w procentowym wskaźniku dostępności:
 - a) Czas, w którym TKH Security wykonuje usługi konserwacyjne zgodnie z treścią Artykułu 10. Przerwy spowodowane okolicznościami pozostającymi poza kontrolą TKH Security, w tym, bez ograniczeń, zdarzeniami siły wyższej (określonymi w Artykule

16.)

- a) Wszelkie zakłócenia w świadczeniu Usług spowodowane działaniem lub zaniechaniem Klienta lub osób trzecich, w tym złośliwym oprogramowaniem.
 - b) Wszelkie zakłócenia w świadczeniu Usług spowodowane poprawkami lub zmianami wprowadzonymi w Sprzęcie przez Klienta lub osoby trzecie, uszkodzeniem Sprzętu lub naruszeniem przez Klienta obowiązku utrzymywania Sprzętu w należytych stanie.
 - c) Wszelkie zakłócenia w świadczeniu Usług wynikające z korzystania z Platformy lub Usług w systemie nieobsługiwany przez TKH Security lub wynikające z połączenia Usług z innym oprogramowaniem niedostarczanym przez TKH Security.
 - d) Zawieszenie świadczenia Usług w przypadkach dozwolonych na mocy postanowień niniejszej Umowy Licencyjnej na Oprogramowanie.
3. W przypadku, gdy TKH Security nie spełni wymogu 99,9% miesięcznego czasu sprawności, z zastrzeżeniem warunków niniejszego dokumentu, Klient będzie uprawniony do kredytów usługowych w oparciu o następujące wskaźniki:
 - a) Dostępność miesięczna Procentowy kredyt serwisowy
 - b) Mniej niż 99,9%, ale co najmniej 98,9% 5% opłaty podzielone przez 12
 - c) Mniej niż 98,9%, ale co najmniej 95,9% 10% opłaty podzielone przez 12
 - d) Mniej niż 95,9% 15% opłaty podzielone przez 12
 4. Miesięczny procentowy czas sprawności oznacza dla danego miesiąca kalendarzowego wynik (łączna liczba minut w danym miesiącu kalendarzowym minus łączna liczba minut przestoju zgłoszona przez Klienta w danym miesiącu kalendarzowym) podzielony przez (łączna liczba minut w ramach subskrypcji Klienta pomnożona przez łączną liczbę minut w danym miesiącu kalendarzowym).
 5. W przypadku, gdy TKH Security nie utrzyma wspomnianej dostępności Usług w odpowiednim okresie każdej aktywowanej Subskrypcji, bez wystąpienia którejkolwiek z okoliczności przewidzianych w Artykułach 11.2 powyżej i 11.6 poniżej, Klient może ubiegać się o kredyt usługowy zgodnie z Artykułem 11.3 powyżej. Klient zwróci się o takie odszkodowanie do TKH Security w ciągu pięciu (5) dni roboczych od następnego miesiąca, podając datę oraz czas rozpoczęcia i zakończenia każdego okresu niedostępności, który wystąpił w poprzednim miesiącu. W ciągu trzydziestu (30) dni kalendarzowych od złożenia wniosku przez Klienta, TKH Security odrzuci wniosek w pisemnym uzasadnionym powiadomieniu lub wypłaci Klientowi uzgodnione odszkodowanie. Klient przyjmuje do wiadomości i zgadza się, że wyżej wymienione uzgodnione odszkodowania są odpowiednią i jedyną rekompensatą za wszelkie straty lub szkody (bezpośrednie lub pośrednie) spowodowane przez Klienta w wyniku niedostępności Usług. Ponadto Klient zgadza się nie kierować żadnych roszczeń w związku z brakiem dostępności Usług do Partnera lub Grupy TKH Security, zrzekając się wszelkich praw, jakie może posiadać w tym zakresie na mocy jakiegokolwiek jurysdykcji.
 6. Bez uszczerbku dla innych przypadków zawieszenia przewidzianych w innych artykułach niniejszej Umowy Licencyjnej Oprogramowania, TKH Security może zawiesić Usługi i odmówić dostępu do Platformy, bez prawa Klienta do jakiegokolwiek odszkodowania lub rekompensaty, jeżeli:
 - a) TKH Security uzna za konieczne uniemożliwienie lub zakończenie korzystania z Usług zabronionego na mocy niniejszej Umowy licencyjnej oprogramowania.
 - b) Po powiadomieniu Klienta, jeśli Klient dopuści się istotnego naruszenia niniejszej Umowy.
 - c) Klient nie uiszcza Opłat należnych TKH Security lub Partnerowi w terminie zgodnie z Artykułem 8.1 i 8.2.
 - d) Zawieszenie świadczenia Usług pozostaje bez uszczerbku dla wszelkich praw lub zobowiązań powstałych przed zawieszeniem.

12. Poufność

1. Strony zobowiązują się nie ujawniać Informacji Poufnych osobom trzecim bez uprzedniej pisemnej zgody drugiej Strony. Niemniej jednak Strony niniejszym wyraźnie upoważniają do udostępniania Informacji Poufnych członkom Grupy TKH Security, Partnerowi TKH Security i/lub

- Instalatorowi w celu zagwarantowania świadczenia Usług.
- Obowiązek zachowania poufności dotyczy zarówno Stron, jak i ich przedstawicieli. Zgodnie z niniejszym postanowieniem termin przedstawiciel oznacza każdego pracownika, dyrektora, agenta, konsultanta, doradcę lub jakąkolwiek inną osobę z nimi związaną.
 - W celu uniknięcia ujawnienia Informacji Poufnych, każda ze Stron zobowiązuje się do przyjęcia wszelkich ustaleń i środków, jakie uzna za stosowne w celu zachowania Informacji Poufnych, w szczególności wszelkich niezbędnych środków związanych z jej pracownikami, którzy mają dostęp do Informacji Poufnych.
 - Jeśli którakolwiek ze Stron lub jej przedstawiciele naruszają niniejsze zobowiązania do zachowania poufności, Strona naruszająca zwołni drugą Stronę z odpowiedzialności za wszelkie bezpośrednie szkody lub straty poniesione przez drugą Stronę w wyniku wspomnianego naruszenia.
 - W przypadku, gdy Strona zostanie wezwana przez organ sądowy lub administracyjny do przekazania Informacji Poufnych, niezwłocznie poinformuje o tym drugą Stronę.
 - Niniejsze zobowiązanie do zachowania poufności pozostaje w mocy przez czas nieokreślony, dopóki Informacje Poufne zachowują swój poufny i tajny charakter.
 - W celu uniknięcia wątpliwości, wszelkie wcześniejsze umowy o zachowaniu poufności lub umowy o zachowaniu poufności, które Strony mogły podpisać lub które Klient mógł podpisać z Partnerem, pozostają w mocy i są ważne, a niniejsze postanowienie nie ma na nie wpływu i nadal ma zastosowanie do informacji ujawnionych na ich podstawie.

13. Ochrona danych

- Wszelkie Dane Osobowe, do których TKH Security uzyskuje dostęp w związku z Usługami, których Klient jest Administratorem lub Podmiotem Przetwarzającym, będą przetwarzane przez TKH Security jako Podmiot Przetwarzający lub Podprzetwarzający (zgodnie z definicją tych terminów w RODO). W tym zakresie obowiązki każdej ze Stron wynikające z takiego przetwarzania Danych Osobowych będą regulowane przez obowiązującą w danym czasie Umowę o Przetwarzaniu Danych. Umowa powierzenia przetwarzania danych może zostać zmieniona zgodnie z procedurą określoną w artykule 2.

14. Obowiązki i użytkowanie przez Klienta

- Klient jest zobowiązany do przestrzegania wszystkich zobowiązań, instrukcji, nakazów i ograniczeń wynikających z prawa i obowiązujących przepisów, a także z niniejszej Umowy, Dokumentacji Użytkownika i wszelkich innych warunków podanych do wiadomości Klienta drogą elektroniczną przez TKH Security.
- Klient gwarantuje prawidłowość i kompletność danych Klienta, informacji i akceptacji przekazanych przez Klienta TKH Security przy zawieraniu Umowy.
- Klient zobowiązany jest do terminowego przekazywania TKH Security wszelkich danych i informacji umożliwiających prawidłowe wykonanie Umowy przez TKH Security.
- Klient we własnym zakresie i na własny rachunek oraz w odpowiednim czasie zadba o odpowiedni sprzęt i aparaturę, systemy i infrastrukturę teleinformatyczną, przyłącza, zasilacze, łącze internetowe, oprogramowanie i wszelkie inne wymagania zapewniające prawidłowe funkcjonowanie Sprzętu i/lub Usług.
- Klient nie będzie dokonywał ani zezwalał na nieautoryzowane, niezgodne z prawem lub niewłaściwe korzystanie ze Sprzętu, Aplikacji Mobilnej, Aplikacji Internetowej, Subskrypcji i/lub Usług. Klient zabezpieczy TKH Security przed wszelkimi roszczeniami osób trzecich oraz przed wszelkimi stratami lub szkodami (bezpośrednimi lub pośrednimi) spowodowanymi jakimkolwiek nieautoryzowanym, niezgodnym z prawem lub niewłaściwym użyciem Sprzętu, Subskrypcji i/lub Usług.
- Klient nie będzie wprowadzać, przetwarzać, przechowywać ani rozpowszechniać danych z naruszeniem odpowiednich przepisów ustawowych i wykonawczych, praw osób trzecich i/lub praw TKH Security, w tym jej praw własności intelektualnej.
- Klient jest odpowiedzialny za udzielenie dostępu do korzystania z Usług Użytkownikom, których chce upoważnić. Klient nie zezwala osobom trzecim (innym niż Użytkownicy) na korzystanie z Umowy Licencyjnej na Oprogramowanie ATLAS Access - marzec 2024 Strona 6 z 12

Subskrypcji lub korzystanie z Usług bez uprzedniej wyraźnej pisemnej zgody TKH Security.

- Klient podejmie odpowiednie środki, aby zapobiec narażeniu systemów i infrastruktury teleinformatycznej TKH Security na wszelkiego rodzaju złośliwe oprogramowanie, w tym wirusy komputerowe, hacking, spam, oprogramowanie szpiegujące i tym podobne szkodliwe pliki, a także podejmie odpowiednie środki, aby zapobiec nadmiernemu przeciążeniu systemu, niestabilności i/lub wadliwej funkcjonalności systemów i infrastruktury teleinformatycznej TKH Security.
- W tym zakresie Klientowi wyraźnie zabrania się sprzedaży, wynajmu, dzierżawy, przekazywania, przyznawania użytkowania lub w jakikolwiek inny sposób ujawniania Usług i/lub związanej z nimi dokumentacji osobom trzecim, chyba że TKH Security udzieli uprzedniej wyraźnej pisemnej zgody.
- Niewypełnienie któregokolwiek z wyżej wymienionych obowiązków zwalnia TKH Security z wszelkiej odpowiedzialności wynikającej z niniejszej Umowy.

15. Odpowiedzialność

- Usługi, Witryna, Aplikacja internetowa i Aplikacja mobilna są dostarczane w stanie "takim, w jakim są", a wszelkie inne oświadczenia, gwarancje, ustne lub pisemne, wyraźne lub dorozumiane, wynikające z przebiegu transakcji, przebiegu wykonania, zastosowania handlowego, jakości informacji, cichego korzystania lub w inny sposób (w tym dorozumiane gwarancje, warunki lub warunki przydatności handlowej, zadowalającej jakości, przydatności do określonego celu, tytułu, braku ingerencji lub nienaruszania) są, w najszerszym zakresie dozwolonym przez obowiązujące prawo, wyłączone z niniejszej Umowy.
- TKH Security gwarantuje jedynie prawidłowe funkcjonowanie swoich Usług za pośrednictwem API na Platformie Strony Trzeciej, ale nie może zagwarantować dostępu do nich, ani funkcjonowania i dostępności innych usług na wyżej wymienionej platformie. W związku z tym TKH Security ponosi odpowiedzialność wyłącznie za prawidłowe funkcjonowanie Usług na Platformie Strony Trzeciej za pośrednictwem API.
- Całkowita łączna odpowiedzialność TKH Security z tytułu lub związana z jakąkolwiek Szkodą Bezpośrednią w żadnym wypadku nie przekroczy łącznej kwoty Opłat faktycznie zapłaconych przez Klienta za zakup Subskrypcji w ciągu ostatnich dwunastu (12) miesięcy.
- W żadnym wypadku TKH Security (ani żaden z jej podmiotów stowarzyszonych, pracowników, dyrektorów lub udziałowców) nie ponosi odpowiedzialności wobec Klienta lub jakiegokolwiek innej osoby za Szkody Pośrednie, w tym za jakiegokolwiek powyższe straty lub szkody wynikające z korzystania przez Klienta z Usług, Aplikacji Mobilnej, Aplikacji Internetowej i/lub Witryny świadczonych na mocy niniejszej Umowy, lub wynikające z jakiegokolwiek naruszenia niniejszej Umowy lub rozwiązania niniejszej Umowy, niezależnie od tego, czy taka odpowiedzialność jest dochodzona na podstawie umowy, czynu niedozwolonego (w tym zaniedbania lub odpowiedzialności na zasadzie ryzyka) lub w inny sposób i niezależnie od tego, czy można ją przewidzieć, nawet jeśli TKH Security zostało poinformowane lub było świadome możliwości wystąpienia takiej straty lub szkody.
- Powyższe ograniczenia nie mają zastosowania w przypadkach;
 - złośliwości lub oszustwa;
 - umyślnego działania;
 - odpowiedzialności za śmierć lub obrażenia ciała spowodowane zaniedbaniem;
 - wylączenie lub ograniczenie nie jest dozwolone przez obowiązujące prawo.
- Klient przyjmuje na siebie pełną odpowiedzialność, bez żadnych ograniczeń, za Szkody Bezpośrednie lub Pośrednie, w tym wszelkie straty lub szkody wynikające z korzystania przez Klienta z Usług, Aplikacji Mobilnej, Aplikacji Internetowej i/lub Witryny świadczonych na mocy niniejszej Umowy lub wynikające z jakiegokolwiek naruszenia niniejszej Umowy lub rozwiązania niniejszej Umowy.
- Klient zobowiązuje się zwolnić TKH Security z odpowiedzialności zgodnie z obowiązującym prawem za wszelkie szkody i zobowiązania powstałe w wyniku lub w jakikolwiek sposób związane z wykonywaniem Umowy i korzystaniem z Usług.

16. Force Majeure

1. Żadna ze Stron nie będzie odpowiedzialna za, ani żadna ze Stron nie zostanie uznana za naruszającą niniejszą Umowę Licencyjną Oprogramowania z powodu niewykonania swoich zobowiązań wynikających z niniejszej Umowy w wyniku przyczyny pozostającej poza jej kontrolą, w tym działania siły wyższej, wroga publicznego lub terrorysty, działania jakiegokolwiek organu wojskowego, cywilnego lub regulacyjnego, zmiany jakiegokolwiek prawa lub regulacji, pożaru, powodzi, trzęsienia ziemi, lub innego podobnego zdarzenia, kradzieży lub przestępstwa popełnionego przez niepowiązane strony trzecie, zakłócenia lub przerwy w komunikacji (w tym w Internecie lub innym środowisku sieciowym), zasilania lub innych mediów, niedostępności dostaw lub jakiegokolwiek innej przyczyny, podobnej lub różnej od którejkolwiek z powyższych, której Strona niewykonująca Umowy nie mogła zapobiec przy zachowaniu należytej staranności.

17. Prawa własności intelektualnej

1. Wszelkie Prawa Własności Intelektualnej do Sprzętu, jakiegokolwiek oprogramowania, stron internetowych, Platformy, baz danych, sprzętu lub innych materiałów dostarczonych Klientowi w ramach Umowy, takich jak analizy, dokumentacja, raporty lub oferty, nawet te, które mogą wynikać ze świadczenia Usług, są wyłączną własnością TKH Security, jej licencjodawców lub dostawców. Żadne z postanowień niniejszej Umowy nie może być rozumiane jako przeniesienie własności jakichkolwiek Praw Własności Intelektualnej z TKH Security na Klienta.
2. Klient uzyskuje, w zakresie, w jakim ma to zastosowanie, wyłącznie prawa do użytkowania wyraźnie przyznane na mocy niniejszej Umowy Licencyjnej na Oprogramowanie oraz przepisów prawa i wyłącznie w Okresie Obowiązywania Umowy. Wszelkie prawa użytkowania, do których uprawniony jest Klient, nie mogą być przenoszone na osoby trzecie.
3. Klientowi zabrania się usuwania lub zmieniania jakichkolwiek praw autorskich, znaków towarowych, nazw handlowych lub innych oznaczeń Praw Własności Intelektualnej w Sprzęcie, Platformie, oprogramowaniu, witrynach internetowych, bazach danych, wyposażeniu lub materiałach. Obejmuje to wszelkie oznaczenia dotyczące ich poufnego charakteru.
4. Klientowi zabrania się odtwarzania, dezasemblacji, rekonstrukcji, dekompilacji, inżynierii wstecznej kodu źródłowego lub innego przetwarzania, modyfikowania lub dostosowywania Platformy, Usług lub Sprzętu, w całości lub w części, w jakikolwiek sposób.
5. TKH Security ma prawo do zmiany konfiguracji technicznej Platformy i Usług w dowolnym momencie według własnego uznania i bez konieczności uzyskania zgody Klienta.

18. Okres obowiązywania i rozwiązanie umowy

1. Niniejsza Umowa wchodzi w życie z dniem spełnienia wszystkich warunków określonych w Artykule 4.2. i pozostaje w mocy przez początkowy okres obowiązywania Subskrypcji (tj. jeden rok od daty subskrypcji) oraz jej przedłużenia.
2. Bez uszczerbku dla innych artykułów niniejszej Umowy, Strona będzie uprawniona do wcześniejszego rozwiązania Umowy wyłącznie w przypadku naruszenia Umowy, gdy Strona naruszająca nie naprawi naruszenia po otrzymaniu odpowiedniego pisemnego zawiadomienia o naruszeniu, określającego jak najwięcej szczegółów i rozpoczynającego rozsądny okres, który w żadnym wypadku nie może przekroczyć jednego (1) miesiąca, w którym należy naprawić naruszenie.
3. TKH Security nigdy nie będzie zobowiązana do (i) zwrotu, refundacji lub zwrotu Opłat lub jakichkolwiek innych opłat już otrzymanych, lub (ii) zapłaty jakiegokolwiek odszkodowania z powodu rozwiązania Umowy z jednego z wyżej wymienionych powodów (z wyjątkiem przypadku rozwiązania Umowy z powodu poważnego naruszenia przez TKH Security istotnych zobowiązań wynikających z niniejszej Umowy).
4. Wszystkie prawa użytkownika i dostępu do Usług wygasają ze skutkiem natychmiastowym w momencie rozwiązania Umowy z jakiegokolwiek przyczyny. W związku z tym, po rozwiązaniu Umowy z jakiegokolwiek przyczyny, TKH Security zaprzestanie świadczenia Usług.
5. W celu uniknięcia wątpliwości, rozwiązanie niniejszej Umowy nie wpływa w żaden sposób na ważność Umowy o Przetwarzaniu Danych, którą Klient zawarł z TKH Security, a która pozostaje w mocy zgodnie z jej własnymi warunkami.
6. We wszystkich przypadkach, w których Umowa zostanie rozwiązana z

jakiegokolwiek przyczyny, będzie ona nadal regulować stosunki między Stronami w zakresie niezbędnym do ich rozwiązania.

19. Przeniesienie lub udostępnienie praw i obowiązków

1. TKH Security zastrzega sobie prawo do przeniesienia swoich praw i/lub obowiązków wynikających z Umowy na osobę trzecią bez konieczności uzyskania zgody Klienta, pod warunkiem, że TKH Security zapewni, że taka osoba trzecia zgodzi się przestrzegać praw i obowiązków określonych w Umowie.
2. Klient nie jest uprawniony do przeniesienia lub udostępnienia jakichkolwiek praw i/lub obowiązków wynikających z Umowy i/lub Umowy osobom trzecim bez uprzedniej pisemnej zgody TKH Security. Z wyjątkiem przypadku, gdy własność lub zarządzanie lokalem lub budynkiem, w którym zainstalowany jest Sprzęt związany z Witryną, zostanie przeniesione na osobę trzecią. W takim przypadku Klient powinien zaktualizować odpowiednie Dane Witryny i dane Klienta na Platformie.
3. TKH Security ma prawo do całkowitego lub częściowego podzlecenia wykonania Usług za pośrednictwem Platformy lub ich części dowolnej firmie bez konieczności uzyskania zgody Klienta.

20. Postanowienia końcowe

1. Jeżeli którykolwiek z artykułów Umowy zostanie uznany za nieważny lub zniszczony, nie ma to wpływu na ważność pozostałych klauzul Umowy. W takim przypadku Strony zaangażują się w dyskusje dotyczące treści nowego artykułu, który będzie jak najściślej odpowiadał pierwotnemu artykułowi.
2. W przypadku niejasności dotyczących interpretacji jednego lub kilku artykułów Umowy, będą one interpretowane w duchu tych artykułów.
3. Jeżeli między Stronami zaistnieje sytuacja, która nie jest uregulowana w Umowie, wówczas sytuacja ta musi zostać oceniona zgodnie z duchem Umowy.
4. Niniejsza Umowa podlega i będzie interpretowana zgodnie z prawem holenderskim. Wszelkie spory powstałe pomiędzy Klientem a TKH Security podlegają wyłącznie jurysdykcji właściwego sądu w Hadze (Den Haag), Holandia.
5. Oficjalnym językiem Umowy jest język angielski. W przypadku jakichkolwiek rozbieżności między wersją angielską a jakąkolwiek inną wersją, na którą można przetłumaczyć Umowę (wyłącznie w celu ułatwienia zrozumienia przez Klienta), pierwszeństwo ma treść wersji angielskiej.

ZAŁĄCZNIK Definicje

Szczegóły konta: Kod klienta, hasło, nazwa klienta, kody aktywacyjne i inne dane dotyczące Klienta, które umożliwiają mu dostęp do Witryny.

Umowa: Całość umowy zawartej między TKH Security a Klientem, na którą składają się niniejsza Umowa licencyjna na oprogramowanie oraz Umowa o przetwarzaniu danych (wraz z załącznikami).

API: Interfejs programowania aplikacji (lub inna podobna technologia lub komponent oprogramowania) oferowany przez TKH Security za pośrednictwem platformy, która umożliwia Klientowi korzystanie z niektórych usług TKH Security bez bezpośredniego dostępu do nich.

Informacje poufne: Obejmują: (i) wszystkie informacje dotyczące sprzętu, usług lub subskrypcji, niezależnie od ich wsparcia (projekty, podręczniki, oprogramowanie, sprzęt itp.); (ii) wszelkie inne informacje, które strony uznają za poufne na mocy niniejszej umowy; oraz (iii) wszelkie informacje techniczne, finansowe, handlowe, przemysłowe lub strukturalne dotyczące działalności TKH Security i jej grupy.

Klient: osoba prawna, która zawiera niniejszą Umowę w celu korzystania z Usług i uzyskania do nich dostępu w celach zawodowych. Umowa o przetwarzaniu danych (lub DPA): umowa dodatkowa zawarta między TKH Security a Klientem, na podstawie której TKH Security przetwarza Dane osobowe zgodnie z postanowieniami punktu 13.1.

Szkody bezpośrednie: wszelkie rzeczywiste i materialne szkody lub straty, inne niż szkody pośrednie, wyrządzone którejkolwiek ze Stron jako bezpośrednia i nieunikniona konsekwencja naruszenia Umowy przez drugą Stronę.

Przestój: każdy okres dłuższy niż pięć (5) minut, podczas którego Usługi nie działają i nie są dostępne do użytku w standardowych warunkach kontroli dostępu. Obejmuje to wyłącznie następujące scenariusze:

Brak możliwości tworzenia lub modyfikowania praw dostępu: Obejmuje to każdy okres dłuższy niż pięć (5) minut, podczas którego Użytkownicy nie mogą tworzyć nowych praw dostępu lub modyfikować istniejących w Aplikacji mobilnej, uniemożliwiając w ten sposób prawidłowe zarządzanie uprawnieniami kontroli dostępu.

Niedostępność usług synchronizacji: Dotyczy to okresów, w których usługi zaplecza, niezbędne do synchronizacji tokenów dostępu z Aplikacją mobilną, są niedostępne.

Brak możliwości uzyskania dostępu do zabezpieczonych pomieszczeń za pomocą sprzętu: Scenariusz ten obejmuje przypadki, w których użytkownicy nie mogą uzyskać dostępu do pomieszczeń zabezpieczonych za pomocą sprzętu za pośrednictwem aplikacji mobilnej. Nie obejmuje to przestoju wynikających z awarii sprzętu zamków lub nieprawidłowej konfiguracji systemu, które wykraczają poza zakres niniejszej umowy.

Środowisko Entra ID: Usługa zarządzania tożsamością i dostępem w chmurze firmy Microsoft, wykorzystywana do:

- Uwierzytelniania i autoryzacji użytkowników podczas logowania się na platformie.
- Przyznawania i odbierania uprawnień użytkownikom Entra ID na platformie.
- Zarządzania gośćmi: zaproszenia

Umowa licencyjna użytkownika końcowego (EULA): Obowiązująca umowa licencyjna użytkownika końcowego zawarta między upoważnionymi użytkownikami klienta a TKH Security w odniesieniu do licencji klienta i korzystania z platformy.

Oplaty: Oplaty uiszczane przez klienta za zakup każdej subskrypcji w celu uzyskania dostępu i korzystania z usług za pośrednictwem platformy, zgodnie z postanowieniami punktu 8.

Sprzęt: Kompatybilny sprzęt zakupiony przez Klienta bezpośrednio w TKH Security lub u Partnera, który jest wymagany do uzyskania dostępu i korzystania z Usług przez Klienta.

Szkody pośrednie: Szkody następne, utrata zysków, utracone oszczędności, utrata wartości firmy lub reputacji Klientów, TKH Security, Grupy TKH Security lub Partnera TKH Security lub innych stron trzecich oraz wszelkie inne formy szkód pośrednich wyrządzonych którejkolwiek ze Stron, które nie są bezpośrednią, przewidywalną i konieczną konsekwencją naruszenia Umowy przez Stronę.

Prawa własności intelektualnej: Wszystkie prawa własności intelektualnej i przemysłowej w rozumieniu holenderskich lub międzynarodowych konwencji dotyczących własności intelektualnej, w tym inne prawa własności i potencjalne prawa licencyjne, kody źródłowe, oprogramowanie, prawa do baz danych i inne prawa przysługujące TKH Security lub jej Grupie w najszerszym zakresie prawnym.

Złośliwe oprogramowanie: aplikacje, kod wykonywalny lub złośliwa zawartość oraz wszelkie programy komputerowe zaprojektowane specjalnie w celu infiltracji i uszkodzenia sieci i komputerów bez zgody TKH Security lub które TKH Security uznaje za szkodliwe dla Platformy. Złośliwe oprogramowanie obejmuje między innymi wszelkiego rodzaju zagrożenia dla bezpieczeństwa komputera i sieci, w tym wirusy, oprogramowanie szpiegujące, robaki, trojany lub rootkity.

Aplikacja mobilna: Aplikacja mobilna Platformy, którą należy pobrać z autoryzowanego sklepu z aplikacjami mobilnymi.

Strony: TKH Security i Klient, zwani indywidualnie „Stroną”.

Dokumentacja partnera: Wszelka dokumentacja umowna zawarta między partnerem TKH Security a Klientem (w formie pisemnej lub cyfrowej) dotycząca zakupu sprzętu i/lub subskrypcji przez Klienta, która obejmuje opłaty za dostęp do Usług i korzystanie z nich.

Platforma: Platforma aplikacji do kontroli dostępu ATLAS, w której zarejestrowany jest Klient, zarządzana przez TKH Security i wykorzystywana przez TKH Security do świadczenia Usług, składająca się z aplikacji internetowej i/lub aplikacji mobilnej.

Oferta: Oferta handlowa przedstawiona Klientowi przez TKH Security i zaakceptowana przez Klienta, zawierająca liczbę użytkowników oprogramowania ATLAS, a w niektórych przypadkach również sprzęt i powiązane usługi.

Rejestracja: Proces, który należy wykonać w celu aktywacji Witryny zgodnie z postanowieniami artykułu 4.

Usługa(-i): Rozwiązanie do kontroli dostępu oparte na chmurze ATLAS, dostarczane zdalnie przez TKH Security Klientowi, dla którego Klient wykupił subskrypcję i w odniesieniu do którego niniejsza Umowa została zaakceptowana.

Witryna: Konto umożliwiające Klientowi dostęp do Usług i korzystanie z nich za pośrednictwem Platformy w celu zarządzania kontrolą dostępu do obiektu, w którym zainstalowany jest powiązany z nim sprzęt.

Umowa licencyjna na oprogramowanie: Niniejsza umowa licencyjna na oprogramowanie zawarta między TKH Security a Klientem dotycząca korzystania z Usług i dostępu do nich.

Subskrypcja: Powtarzająca się subskrypcja, którą Klient musi wykupić, aby otrzymywać Usługi.

Platforma strony trzeciej: każda platforma, dodatek, usługa, produkt, aplikacja lub integracja nie dostarczana przez TKH Security, którą Klient wybiera do integracji lub włączenia do użytku z Usługą(-ami).

TKH Security: TKH Security B.V. jest holenderską spółką z siedzibą pod adresem Werner von Siemensstraat 7, 2712PN Zoetermeer, Holandia. Zarejestrowana w holenderskiej Izbie Handlowej pod numerem 30191139.

Grupa TKH Security (zwana również „Grupą”): Oznacza spółki stowarzyszone i zależne TKH Security wymienione na stronie internetowej TKH Security (tkhsecurity.com), w tym spółkę macierzystą TKH Group N.V.

Partner TKH Security (zwany również „Partnerem”): Każdy z partnerów TKH Security, który zajmuje się komercjalizacją Sprzętu i/lub Usług i za pośrednictwem którego Klient może nabyć Subskrypcję w celu korzystania z Usług i/lub Sprzętu.

Użytkownik(owie): Osoba fizyczna lub osoby fizyczne upoważnione przez Klienta do uzyskania dostępu do Usług i korzystania z nich.

Dokumentacja użytkownika: Wszelkie dokumenty wskazane przez TKH Security jako takie, niezależnie od tego, czy mają formę elektroniczną, które mogą obejmować dokumentację użytkownika dotyczącą Sprzętu i Usług.

Aplikacja internetowa: Oznacza aplikację internetową Platformy.

UMOWA O PRZETWARZANIE DANYCH ATLAS Access

1. Definicje

Pojęcia używane w niniejszej Umowie są identyczne z pojęciami zdefiniowanymi w RODO, chyba że w dalszej części Umowy określono inaczej.

Umowa: niniejsza umowa o przetwarzanie danych wraz z wszelkimi załącznikami.

Autoriteit Persoonsgegevens (holenderski organ ochrony danych): Organ nadzorczy w zakresie zgodności z RODO zgodnie z art. 51 RODO.

Naruszenie: naruszenie związane z danymi osobowymi.

Podmiot danych: osoba fizyczna, której dotyczą dane osobowe.

Dane Osobowe: wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby, które są gromadzone w celu korzystania z Usług zgodnie z definicją zawartą w Umowie Głównej.

Podmiot(-y) przetwarzający(-e): osoba fizyczna lub prawna, która przetwarza część zadań Przetwarzającego w imieniu Przetwarzającego.

2. Rodzaj danych osobowych i kategorie osób, których dane dotyczą

1. Podmiot przetwarzający przetwarza w imieniu Administratora kategorie danych osobowych określone w Załączniku 1.

3. Prawa i obowiązki osób, których dane dotyczą

1. Na żądanie i koszt Administratora Przetwarzający zrobi wszystko, co Administrator uzna za konieczne, aby spełnić żądanie Osoby, której dane dotyczą, w celu realizacji jej praw. Prawa te obejmują między innymi prawo Podmiotu Danych do dostępu, prawo do usunięcia danych, prawo do ograniczenia przetwarzania oraz prawo do przenoszenia danych.

4. Instrukcje od kontrolera

1. Podmiot przetwarzający będzie przetwarzał dane osobowe wyłącznie w imieniu i na rzecz Administratora oraz na podstawie pisemnych instrukcji wydanych przez Administratora, chyba że przepisy prawa stanowią inaczej.
2. Podmiot przetwarzający stosuje się do obowiązku prawnego lub nakazu sądowego i w takim przypadku powiadomi Administratora z wyprzedzeniem, chyba że nie jest to dozwolone na mocy prawa lub nakazu sądowego.
3. Podmiot przetwarzający niezwłocznie powiadomi Administratora danych, jeśli w opinii Podmiotu przetwarzającego polecenie Administratora danych spowodowałoby naruszenie prawa i/lub nakazu sądowego, przy założeniu, że odpowiedzialność za przetwarzanie danych będzie w pełni spoczywać na Administratorze danych.
4. Podmiot przetwarzający nie będzie przetwarzał danych osobowych do własnych celów i/lub przekazywał ich osobom trzecim, z wyjątkiem przypadków, w których takie przekazanie jest dozwolone na mocy Umowy Głównej.
5. Podmiot Przetwarzający samodzielnie przetwarza dane osobowe, do których ma dostęp na podstawie Umowy Głównej. Przetwarzanie danych osobowych przez Podprzetwarzającego jest dozwolone wyłącznie po uzyskaniu uprzedniej pisemnej zgody Administratora.
6. Jeżeli Przetwarzający, z zachowaniem postanowień art. 4.5, zaangażuje Podprzetwarzającego, Przetwarzający nałoży na Podprzetwarzającego obowiązki w zakresie ochrony danych o poziomie ochrony określonym w art. 28 ust. 3 w związku z ust. 4 RODO.
7. Podmiot przetwarzający jest zawsze zobowiązany do dalszego przechowywania i przetwarzania danych osobowych w Europejskim Obszarze Gospodarczym, z zastrzeżeniem uprzedniej i pisemnej zgody Administratora uzyskanej w tym celu, do której to zgody Administrator może dołączyć warunki i którą to zgodę Administrator może odmówić z własnych powodów.

8. Strony uzgadniają, że strona/strony określone w Załączniku 2 będą działać jako Podprzetwarzający dla Przetwarzającego i uzyskają dostęp do danych osobowych.
9. Podmiot przetwarzający będzie przechowywać dane osobowe na serwerach strony określonej w Załączniku 2.
10. Podmiot przetwarzający wyraźnie nie ma kontroli nad celem i sposobami przetwarzania danych osobowych, które przetwarza w ramach realizacji Umowy Głównej.
11. Podmiot przetwarzający będzie przestrzegać RODO oraz innych obowiązujących przepisów prawa i regulacji, w szczególności przepisów prawa i regulacji dotyczących ochrony danych osobowych.
12. Podmiot przetwarzający będzie wykonywał co najmniej następujące zadania dotyczące danych osobowych podczas wykonywania Umowy Głównej:
 - a) przechowywanie danych osobowych;
 - b) tworzenie kopii zapasowych danych osobowych;
 - c) przekazanie danych osobowych Administratorowi;
 - d) gwarantując dostęp do danych osobowych wyłącznie Administratorowi lub Podmiotom Danych za pośrednictwem Administratora; 4.13 Podmiot Przetwarzający powstrzyma się od wszelkich działań, które mogłyby ograniczyć możliwości i prawa Administratora lub Podmiotów Danych do swobodnego dostępu do danych osobowych.
13. Podmiot przetwarzający nie będzie przechowywał żadnych danych osobowych z wyjątkiem.

5. Środki bezpieczeństwa i audyty

1. Podmiot przetwarzający jest zobowiązany do zapewnienia odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych osobowych przed utratą lub jakąkolwiek formą niezgodnego z prawem przetwarzania, jak określono w art. 32 RODO. W każdym przypadku Podmiot przetwarzający będzie przez cały czas stosował odpowiednie środki bezpieczeństwa określone w art. 32 RODO i zasadniczo będzie przez cały czas zapewniał odpowiedni poziom bezpieczeństwa, biorąc pod uwagę charakter danych i ryzyko związane z Przetwarzaniem. Plan bezpieczeństwa zawarty w Załączniku 3 do niniejszej Umowy będzie częścią niniejszej Umowy, a środki w nim określone muszą być utrzymywane jako minimalny poziom ochrony.
2. Podmiot przetwarzający podejmie wszelkie niezbędne środki, aby zapobiec niepotrzebnemu gromadzeniu i dalszemu przetwarzaniu danych osobowych, innych niż wymagane do wykonania Umowy Głównej.
3. Na pierwsze żądanie Administratora Przetwarzający zaoferuje, na koszt Administratora, wszelką współpracę, która może być w uzasadniony sposób wymagana w celu umożliwienia Administratorowi sprawdzenia (lub zlecenia sprawdzenia), a także zbadania (lub zlecenia zbadania), czy przetwarzanie danych osobowych odbywa się zgodnie z umową i czy Przetwarzający podjął wszelkie odpowiednie techniczne i organizacyjne środki bezpieczeństwa przed utratą lub jakąkolwiek formą niewłaściwego przetwarzania.
4. Administrator jest uprawniony do sprawdzenia (lub zlecenia sprawdzenia) wypełnienia postanowień niniejszej Umowy maksymalnie raz w roku, chyba że w opinii Administratora z ważnego powodu pożądanym jest audyt okresowy. Administrator jest uprawniony do samodzielnego przeprowadzenia takiego audytu lub do zlecenia jego przeprowadzenia niezależnemu biegłemu rewidentowi, biegłemu informatykowi lub audytorowi posiadającemu odpowiednie uprawnienia. Administrator poniesie koszty takiego audytu. Koszty personelu Przetwarzającego, który kieruje audytem, ponosi Kontroler. Audyt nie może niepotrzebnie zakłócać działalności Przetwarzającego. Administrator powiadomi Przetwarzającego o audytach na piśmie co najmniej dziesięć dni przed ich rozpoczęciem, podając opis elementów, które mają zostać poddane audytowi, chyba że Administrator zażąda przeprowadzenia (lub zleci przeprowadzenie) audytu określonego w zdaniu drugim niniejszego Artykułu 5.4 z istotnych powodów.
5. W przypadku Naruszenia Przetwarzający powiadomi Administratora o tym Naruszeniu i (spodziewanych) konsekwencjach tak szybko, jak to możliwe - ale nie później niż w ciągu 48 godzin - po jego wykryciu. W takim przypadku Przetwarzający przekaze dodatkowe informacje o

charakterze Naruszenia, imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innej osoby kontaktowej, prawdopodobne konsekwencje Naruszenia, sposób, w jaki zajmie się Naruszeniem oraz sposób, w jaki ograniczy negatywne konsekwencje Naruszenia. Podmiot przetwarzający określa ramy czasowe, w których podejmie te środki. Na pierwsze żądanie Administratora Przetwarzający zapewni również wszelką uzasadnioną współpracę w zakresie powiadomienia holenderskiego organu ochrony danych.

6. Podmiot przetwarzający niezwłocznie powiadomi również Administratora o wszelkich Naruszeniach, w tym o faktach dotyczących Naruszenia w związku z danymi osobowymi, odpowiednich konsekwencjach i podjętych środkach naprawczych. Dokumentacja ta musi umożliwiać holenderskiemu organowi ochrony danych weryfikację zgodności z art. 33 RODO.
7. W przypadku, gdy Przetwarzający zaniedba podjęcia uzasadnionych środków przeciwko Naruszeniu i nie podejmie odpowiednich środków w terminie wyznaczonym przez Administratora, Administrator jest uprawniony do zlecenia wykonania tych środków na koszt Przetwarzającego. Przetwarzający jest zobowiązany do pełnej współpracy w tym zakresie.
8. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania i udostępnione mu informacje, będzie pomagał Administratorowi na jego koszt w wypełnianiu jego obowiązków zgodnie z RODO, w tym między innymi obowiązku zabezpieczenia, obowiązku powiadomienia, przeprowadzenia oceny skutków dla ochrony danych i uprzednich konsultacji w przypadku przetwarzania o wysokim ryzyku.

6. Poufność

1. Podmiot przetwarzający gwarantuje, że przez cały czas będzie działał zgodnie ze swoimi obowiązkami prawnymi w zakresie poufności, w tym między innymi z obowiązkiem zachowania poufności określonym w art. 90 RODO. Podmiot przetwarzający nie będzie bezpośrednio ani pośrednio udostępniać danych osobowych osobom trzecim, chyba że Umowa główna, przepisy prawa lub nakaz sądowy stanowią inaczej.
2. Podmiot przetwarzający zobowiąże (umownie) swoich podwładnych, którzy mają dostęp do danych osobowych, a także zaangażowane przez niego strony trzecie, które mają taki dostęp, do zachowania poufności zgodnie z wymogami RODO i niniejszej Umowy.
3. Podmiot przetwarzający jest zobowiązany do niezwłocznego zgłaszania Administratorowi żądania ujawnienia lub wydania danych osobowych.

7. Niszczenie i tworzenie kopii zapasowych

1. W przypadku rozwiązania niniejszej Umowy, Przetwarzający, obciążając kosztami, udostępni Administratorowi dane osobowe wraz z innymi przetwarzanymi danymi w formacie pliku elektronicznego, powszechnie używanego na rynku.
2. Z zastrzeżeniem innych wiążących zobowiązań prawnych, Przetwarzający jest zobowiązany, na pierwsze pisemne żądanie po rozwiązaniu Umowy Głównej, do zniszczenia wszystkich Danych Osobowych Administratora.

8. Odpowiedzialność

1. Podmiot przetwarzający ponosi odpowiedzialność za wszelkie szkody wynikające z niewykonania niniejszej Umowy lub jakichkolwiek wymogów określonych w obowiązujących przepisach prawa i/lub regulacjach, w tym między innymi w RODO, i zwalnia Administratora z odpowiedzialności za szkody i koszty - w tym między innymi koszty pomocy prawnej - w tym zakresie, maksymalnie do wysokości jednokrotności kwot zafakturowanych przez Podmiot przetwarzający na podstawie Umowy głównej w roku poprzedzającym roszczenie, z wyjątkiem przypadku umyślności lub świadomej lekkomyślności po stronie Podmiotu przetwarzającego.
2. Jeżeli Administrator zostanie pozwany przez Podmiot danych lub osobę trzecią za szkody, które Podmiot danych lub osoba trzecia rzekomo poniosła w związku z przetwarzaniem danych osobowych, Administrator ma prawo regresu wobec Przetwarzającego, jeżeli Przetwarzający nie dopełnił jakichkolwiek obowiązków wynikających z przepisów prawa lub niniejszej Umowy, maksymalnie do jednokrotności kwot zafakturowanych przez Przetwarzającego na podstawie Umowy głównej w roku poprzedzającym roszczenie, z wyjątkiem przypadku umyślnego

lub świadomego lekkomyślnego działania ze strony Przetwarzającego.

3. Administrator zwalnia Przetwarzającego z odpowiedzialności z tytułu roszczeń Podmiotów Danych i osób trzecich, w tym z tytułu nałożonych kar i należnych odszkodowań, w zakresie, w jakim roszczenia te wynikają z naruszenia przez Administratora obowiązujących przepisów prawa i regulacji, w tym RODO.

9. Postanowienia końcowe

1. Podmiotowi przetwarzającemu nie wolno (w całości lub w części) przenosić lub zlecać osobom trzecim swoich zobowiązań wynikających z niniejszej Umowy, chyba że Administrator wyrazi na to uprzednią pisemną zgodę i z zastrzeżeniem postanowień Umowy głównej.
2. Strony wyraźnie uzgadniają, że ogólne warunki Administratora (zakupu) nie mają zastosowania do niniejszej Umowy.
3. Niniejsza Umowa zostanie zawarta na okres obowiązywania Umowy Głównej.
4. Niniejsza Umowa wchodzi w życie po jej podpisaniu przez obie Strony.
5. W przypadku, gdy jedno lub więcej postanowień niniejszej Umowy okaże się nieważne, pozostałe postanowienia Umowy pozostaną w pełni w mocy. W takim przypadku Strony są zobowiązane do zastąpienia nieważnego postanowienia postanowieniem, które jest prawnie wiążące i w jak najniższym stopniu - biorąc pod uwagę cel i intencję niniejszej Umowy - odbiega od nieważnego postanowienia.
6. Niniejsza Umowa może zostać przedterminowo rozwiązana w całości lub w części wyłącznie za pisemną zgodą Stron. W przypadku braku takiej pisemnej zgody, niniejsza Umowa nie może zostać w całości lub w części rozwiązana na drodze pozasądowej. Jeżeli niniejsza Umowa zawiera jakiegokolwiek postanowienia, które ze względu na swój charakter mają obowiązywać po jej rozwiązaniu, pozostaną one w pełni w mocy.
7. Zmiany lub uzupełnienia niniejszej Umowy są wiążące tylko wtedy, gdy zostały uzgodnione na piśmie.
8. W przypadku zmiany przepisów ustawowych i wykonawczych w taki sposób, że Umowa przestanie spełniać wymogi określone w przepisach ustawowych i/lub wykonawczych, Strony dostosują Umowę we wzajemnym porozumieniu zgodnie ze zmienionymi przepisami ustawowymi i/lub wykonawczymi.

10. Prawo właściwe i właściwość sądu

1. Niniejsza Umowa, jak również wszystkie stosunki prawne, do których Umowa ma zastosowanie lub które powinny wynikać z Umowy, podlegają prawu holenderskiemu.
2. Wszelkie spory, które mogą powstać między Stronami w związku z niniejszą Umową lub w jej wyniku, będą rozstrzygane przez sąd w Hadze (Den Haag), Holandia.

LISTA ZAŁĄCZNIKÓW

1 - Kategorie podmiotów danych i dane osobowe

Przechowywanie danych

Cel - Hosting

Kategorie osób, których dane dotyczą - Użytkownicy końcowi klienta

Kategorie danych osobowych - Patrz Załącznik 1A

Transfer do kraju trzeciego - Nie

Dostęp do danych osobowych

Cel - przeprowadzanie serwisu i konserwacja systemów technicznych:

- diagnozowanie i rozwiązywanie usterek;
- aktualizowanie nowych wersji oprogramowania
- umieszczanie poprawek i hotfixów;
- tworzenie kopii zapasowych;
- przenoszenie techniczne

Kategorie osób, których dane dotyczą - Użytkownicy końcowi klienta

Kategorie danych osobowych - Patrz Załącznik 1A

Transfer do kraju trzeciego - Nie

1A – Uprawnienia ATLAS Microsoft Entra ID

[UPRAWNIENIA ATLAS MS ENTRAID](#)

2 - Podprocesor(y)

Strona: Amazon Web Services EMEA SARL

Adres: 38 Avenue John F. Kennedy, L-1855

Miejsce prowadzenia działalności: Luxembourg

Miejsce centrum danych: Frankfurt am Main - Germany

3 - Plan bezpieczeństwa

- Przydzielono obowiązki związane z bezpieczeństwem informacji.
- Zmiany w danych lub przetwarzaniu informacji są wprowadzane wyłącznie w ramach procedury zarządzania zmianami.
- Podmiot przetwarzający przeszkolił wybranych i sprawdzonych pracowników oraz posiada doświadczenie w tej dziedzinie (w tym w zakresie odpowiedniego bezpieczeństwa informacji).
- Podmiot przetwarzający posiada certyfikat uprawniający do profesjonalnego oferowania i wspierania swoich usług i produktów związanych z bezpieczeństwem na rzecz klienta.
- Podmiot przetwarzający okresowo przeprowadza własne audyty wewnętrzne w celu zapewnienia niezbędnego dowodu zgodności z normami i wymaganiami.
- Podmiot przetwarzający skoordynował odpowiednie procedury dotyczące komunikacji, wsparcia i działań zarządczych.
- Ustanowiono polityki bezpieczeństwa, które są również wdrażane.
- Środki bezpieczeństwa dostępu fizycznego, w tym kontrola organizacyjna.
- Alarm antywłamaniowy.
- Środki przeciwko złośliwemu oprogramowaniu.
- Sejf do przechowywania plików danych.
- Odpowiednia kontrola dostępu logicznego przy użyciu uwierzytelniania dwuskładnikowego, danych biometrycznych itp.
- Automatyczne rejestrowanie dostępu do danych, w tym procedura kontroli.
- Kontrola przypisanych uprawnień.
- Szyfrowanie danych osobowych podczas transmisji.
- Szyfrowanie danych osobowych podczas przechowywania.
- Zarządzanie ciągłością działania, plany ciągłości działania.
- Procedura tworzenia kopii zapasowych i odzyskiwania danych.

POLITYKA PRYWATNOŚCI DLA UŻYTKOWNIKÓW APLIKACJI MOBILNYCH ATLAS Access

Przetwarzanie danych osobowych

Podczas korzystania z aplikacji ATLAS Access przetwarzamy następujące dane osobowe:

Proces kontroli dostępu

W procesie kontroli dostępu otrzymamy imię i nazwisko oraz adres e-mail użytkownika od naszego klienta, administratora obiektu, który przyznał użytkownikowi dostęp za pośrednictwem systemu ATLAS do tego obiektu. Adres e-mail zostanie wykorzystany do zaproszenia użytkownika do zarejestrowania urządzenia mobilnego. Rejestrując urządzenie mobilne w aplikacji ATLAS Access, wygenerujemy identyfikator urządzenia mobilnego w celu identyfikacji urządzenia mobilnego. Ten identyfikator urządzenia mobilnego jest specyficzny dla urządzenia i jest używany dla każdego mobilnego dostępu do tego urządzenia. Jeśli zarejestrujesz nowe urządzenie lub aplikacja zostanie ponownie zainstalowana, dla tej nowej instalacji zostanie wygenerowany nowy identyfikator urządzenia mobilnego.

Po zarejestrowaniu urządzenia mobilnego tokeny dostępu będą generowane i przechowywane w aplikacji mobilnej zgodnie z lokalizacjami, do których użytkownik może wejść. Po przyłożeniu urządzenia mobilnego do czytnika wysyłany jest token dostępu, który zostanie zweryfikowany w celu przyznania dostępu.

Po przyłożeniu urządzenia mobilnego do czytnika do aplikacji ATLAS Access zostanie wysłana informacja zwrotna zawierająca lokalizację drzwi, a w procesie zostaną przetworzone poniższe dane:

- nazwa podana przez administratora obiektu
- adres e-mail podany przez administratora obiektu
- identyfikator urządzenia mobilnego losowo wygenerowany numer identyfikujący urządzenie mobilne
- identyfikator osobisty losowo wygenerowany numer identyfikujący użytkownika

Dzienniki dostępu

W dziennikach dostępu w celu świadczenia usług aplikacji przetwarzamy dane użytkownika podczas korzystania z aplikacji, na przykład gdy żąda on dostępu za pomocą urządzenia mobilnego. Oprócz danych osobowych wymienionych powyżej, dzienniki te zawierają również dane o lokalizacji przyznanego dostępu i czasie wejścia:

- imię i nazwisko
- adres e-mail
- identyfikator urządzenia mobilnego
- aktywność dostępu informacje o miejscach, w których przyznano lub odmówiono dostępu.

Cel przetwarzania danych

Gdy użytkownik korzysta z naszej aplikacji, przetwarzamy wyżej wymienione dane osobowe w celu identyfikacji użytkownika za pośrednictwem urządzenia mobilnego i zarządzania jego prawem dostępu do danej lokalizacji.

Okres przechowywania

Nie przechowujemy danych użytkownika dłużej niż jest to konieczne do celów, dla których je przetwarzamy. Po wygenerowaniu dostępu usuniemy aktywność dostępu po trzydziestu (30) dniach. Imię i nazwisko, adres e-mail oraz identyfikator urządzenia mobilnego i identyfikator osobisty będą przechowywane tak długo, jak długo użytkownik będzie korzystał z aplikacji.

Podstawa prawna przetwarzania danych

Podczas korzystania z naszej aplikacji art. 6 ust. 1 lit. a) RODO służy jako podstawa prawna przetwarzania, w przypadku którego uzyskujemy zgodę na określony cel przetwarzania. Korzystanie z tej aplikacji odbywa się za zgodą użytkownika, a dane osobowe, które otrzymujemy od administratora obiektu, do którego użytkownik uzyskał dostęp, są przekazywane na podstawie prawnie uzasadnionych interesów (art. 6 ust. 1 lit. f) RODO) tego obiektu.

Przekazywanie danych stronom trzecim

Nasze środowisko chmury jest hostowane przez firmę w Unii Europejskiej. Ponadto korzystamy z usług podmiotów zewnętrznych w zakresie konserwacji naszych systemów. Używamy Google Crashlytics do monitorowania naszej aplikacji, a dane udostępniane w tym celu Google Crashlytics nie zawierają danych osobowych.

Wszystkie strony trzecie, z których korzystamy, są wybierane przez nas na podstawie ścisłych kryteriów ochrony danych. Zawarliśmy z nimi umowy dotyczące przetwarzania danych. Działają one zgodnie ze wszystkimi odpowiednimi przepisami prawa i regulacjami, naszymi wymogami bezpieczeństwa i przetwarzają dane osobowe wyłącznie w uzgodnionych celach. Oświadczamy, że dane osobowe użytkownika nie zostaną odsprzedane.

Twoje prawa

Użytkownik może skontaktować się z nami, jeśli chce skorzystać z prawa do:

- dostępu do przetwarzanych przez nas danych osobowych
- usunięcia swoich danych osobowych
- ograniczenia przetwarzania danych osobowych;
- przenoszenia danych osobowych;
- wniesienia sprzeciwu wobec przetwarzania przez nas danych osobowych;
- niepodlegania zautomatyzowanemu podejmowaniu indywidualnych decyzji.

Wycofanie zgody

Użytkownik zawsze może wyciąć swoją zgodę na przetwarzanie jego danych w celu korzystania z aplikacji ATLAS. Możesz nas o tym poinformować pocztą elektroniczną za pośrednictwem powyższego adresu e-mail.

Użytkownik może wykonywać swoje prawa wobec TKH Security, w tym wyciąć zgodę, wyłącznie w odniesieniu do danych, które przetwarzamy jako administrator.

Przetwarzamy również dane jako podmiot przetwarzający dla naszych klientów. W przypadku jakichkolwiek pytań lub chęci skorzystania z przysługujących praw w odniesieniu do tych danych, należy skontaktować się z klientem. Klientem tym jest zarządca nieruchomości, do której użytkownik uzyskał dostęp za pośrednictwem ATLAS Access Control.