IBM Trusteer Mobile

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze. Odpowiednie dokumenty zamówienia zawierają ceny i dodatkowe informacje dotyczące zamówienia Klienta.

1. Usługa Przetwarzania w Chmurze

Usługa IBM Trusteer Mobile pomaga wykrywać w czasie rzeczywistym czynniki ryzyka związane z urządzeniami i sesjami. Ułatwia utrzymanie integralności aplikacji, w którą została wbudowana, dzięki wykorzystaniu zaawansowanych funkcji analitycznych oraz wykrywaniu w czasie rzeczywistym czynników ryzyka związanych z urządzeniami. IBM Truster Mobile ocenia urządzenie w celu sprawdzenia, czy zostało ono uszkodzone przez szkodliwe oprogramowanie, trojany zdalnego dostępu, techniki jailbreaking lub rooting, ataki nakładkowe lub aplikacje do kradzieży wiadomości SMS. Dodatkowe wskaźniki obejmujące wszystkie kanały są przetwarzane w trybie ciągłym z wykorzystaniem zaawansowanych technologii, które umożliwiają wykrywanie nieprawidłowych zachowań, sprzeczności dotyczących nawigacji oraz przypadków wyłudzania informacji.

1.1 Produkty oferowane

Klient może dokonać wyboru spośród następujących produktów oferowanych.

1.1.1 Oferty IBM Trusteer Mobile SDK for Business i/lub IBM Trusteer Mobile SDK for Retail

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zostały zaprojektowane z myślą o wprowadzeniu kolejnej warstwy ochrony, tak aby zapewnić bezpieczny dostęp w sieci WWW do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji Usług Przetwarzania w Chmurze w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji metodą pharming. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android.

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zawierają prawnie zastrzeżony pakiet narzędzi do tworzenia oprogramowania dla urządzeń mobilnych („SDK”). Jest to pakiet oprogramowania zawierający dokumentację, prawnie zastrzeżone biblioteki programistyczne oraz inne powiązane pliki i elementy określane nazwą „biblioteka IBM Trusteer dla urządzeń mobilnych”, a także „komponent środowiska wykonawczego” lub „Element Podlegający Redystrybucji”, czyli prawnie zastrzeżony kod wygenerowany przez pakiet IBM Trusteer Mobile SDK, który można osadzać w autonomicznych, chronionych aplikacjach Klienta dla urządzeń mobilnych z systemem operacyjnym iOS lub Android (oraz integrować z takimi aplikacjami), w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze („Zintegrowana przez Klienta Aplikacja dla Urządzeń Mobilnych”).

Oferta IBM Trusteer Mobile SDK for Retail jest dostępna w pakietach po 100 Uprawnionych Uczestników lub w pakietach po 100 Urządzeń Klienckich, natomiast oferta IBM Trusteer Mobile SDK for Business jest dostępna w pakietach po 10 Uprawnionych Uczestników lub w pakietach po 10 Urządzeń Klienckich.

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może uzyskiwać za pośrednictwem aplikacji TMA dane o zdarzeniach i oceny trendów ryzyka. IBM Trusteer Pinpoint Detect i IBM Trusteer Pinpoint Verify są używane w ramach logowania do usługi TMA. Klient może odbierać za pośrednictwem Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych informacje dotyczące analizy ryzyka i urządzeń mobilnych w odniesieniu do urządzeń Uprawnionych Uczestników, którzy pobrali Zintegrowaną przez Klienta Aplikację dla Urządzeń Mobilnych. Pozwala to Klientowi opracować strategię zapobiegania oszustwom w celu egzekwowania działań zmierzających do ograniczenia skutków takiego ryzyka. Na potrzeby niniejszej oferty pojęcie „urządzenia mobilne” obejmuje wyłącznie obsługiwane telefony komórkowe i tablety, natomiast nie obejmuje komputerów typu PC lub MAC.

Klient może:

a. wykorzystywać pakiet IBM Trusteer Mobile SDK do użytku wewnętrznego, wyłącznie na potrzeby opracowywania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych;

b. osadzić Element Podlegający Redystrybucji (wyłącznie w postaci kodu wynikowego) w Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, tak aby stanowił on integralną, nieodłączną część tej aplikacji, przy czym każdy fragment Elementu Podlegającego Redystrybucji

zmodyfikowany lub wbudowany zgodnie z niniejszą licencją będzie podlegał niniejszemu Opisowi Usług;

c. prowadzić sprzedaż i dystrybucję Elementu Podlegającego Redystrybucji przeznaczonego do pobrania na urządzenia mobilne Uprawnionych Uczestników lub do pobrania przez posiadacza Urządzenia Klienckiego, pod następującymi warunkami:

- Z wyjątkiem przypadków wyraźnie dozwolonych w niniejszej Umowie, Klient nie ma prawa (1) używać, kopiować, modyfikować ani dystrybuować pakietu SDK; (2) deasemblować, dekompilować ani przeprowadzać translacji pakietu SDK innymi metodami (z wyjątkiem przypadków wyraźnie dozwolonych przez przepisy prawa bez możliwości ich wyłączenia w ramach umowy); (3) udzielać dalszych licencji, wypożyczać lub wydzierżawiać pakietu SDK; (4) usuwać żadnych plików z informacjami o prawach autorskich ani plików informacyjnych zawartych w Elemencie Podlegającym Redystrybucji; (5) używać tej samej nazwy ścieżki, która została użyta w oryginalnych plikach/modułach Elementu Podlegającego Redystrybucji; (6) używać nazw ani znaków towarowych IBM oraz jego licencjodawców i dystrybutorów w powiązaniu ze sprzedażą Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych bez uprzedniej pisemnej zgody IBM lub odpowiedniego licencjodawcy bądź dystrybutora.
- Element Podlegający Redystrybucji musi pozostać nierozłącznie zintegrowany ze Zintegrowaną przez Klienta Aplikacją dla Urządzeń Mobilnych; ponadto musi mieć wyłącznie postać kodu wynikowego i spełniać wszystkie wytyczne, instrukcje i specyfikacje zawarte w pakiecie SDK i jego dokumentacji. Umowa licencyjna z użytkownikiem końcowym Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych musi zawierać zapis informujący użytkownika końcowego, że Elementu Podlegającego Redystrybucji nie wolno i) używać do jakichkolwiek innych celów niż umożliwienie działania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, ii) kopiować (z wyjątkiem tworzenia kopii zapasowej), iii) przeznaczać do dalszej dystrybucji lub przekazywać, iv) deasemblować, dekompilować ani w inny sposób poddawać translacji, o ile nie zezwalają na to przepisy prawa bez możliwości ich wyłączenia w ramach umowy. Umowa licencyjna zawarta przez Klienta musi chronić prawa IBM w stopniu co najmniej równoważnym warunkom niniejszej Umowy.
- Pakiet SDK może być wdrażany tylko w ramach wewnętrznych testów programistycznych i jednostkowych prowadzonych przez Klienta na urządzeniach mobilnych określonych przez Klienta jako testowe. Klient nie jest upoważniony do używania pakietu SDK w celu przetwarzania lub symulowania obciążeń produkcyjnych ani testowania skalowalności jakiegokolwiek kodu, programu lub systemu. Klient nie jest uprawniony do używania jakiejkolwiek części pakietu SDK do innych celów.

Klient ponosi wyłączną odpowiedzialność za tworzenie i testowanie Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz za świadczenie wsparcia dla niej. Klient odpowiada za świadczenie pełnego zakresu usług pomocy technicznej w odniesieniu do Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz wszelkich modyfikacji w Elemencie Podlegającym Redystrybucji, wprowadzonych przez Klienta w sposób dozwolony w niniejszym dokumencie.

Klient może zainstalować Elementy Podlegające Redystrybucji oraz pakiet IBM Security Mobile SDK i używać ich wyłącznie po to, aby ułatwić sobie korzystanie z Usług Przetwarzania w Chmurze.

IBM nie gwarantuje, że aplikacje lub dane wyjściowe wytworzone z użyciem narzędzi mobilnych wchodzących w skład pakietu IBM Security Mobile SDK będą zgodne operacyjnie, kompatybilne lub zdolne funkcjonować w połączeniu z konkretnym systemem operacyjnym platformy mobilnej lub konkretnym urządzeniem mobilnym.

Komponenty Źródłowe i Materiały Przykładowe – usługa IBM Trusteer Mobile SDK może zawierać pewne komponenty w formie kodu źródłowego (zwane dalej „Komponentami Źródłowymi”) i inne materiały określane jako Materiały Przykładowe. Klient ma prawo kopiować i modyfikować Komponenty Źródłowe i Materiały Przykładowe wyłącznie do użytku wewnętrznego pod warunkiem, że takie użycie materiałów jest objęte uprawnieniami licencyjnymi określonymi niniejszą Umową, jednak z zastrzeżeniem, że Klient nie może zmieniać ani usuwać jakichkolwiek informacji i uwag dotyczących praw autorskich zawartych w Komponentach Źródłowych lub Materiałach Przykładowych. IBM udostępnia Komponenty Źródłowe i Materiały Przykładowe bez zobowiązania do wsparcia oraz W STANIE, W JAKIM SIĘ ZNAJDUJĄ („AS IS”). Zastrzeżenie: Komponenty Źródłowe i Materiały Przykładowe są dostarczane wyłącznie jako przykład sposobu wdrażania Produktu Osadzanego w rozwiązaniu CIMA. Komponenty Źródłowe i Materiały Przykładowe mogą być niezgodne ze środowiskiem programistycznym Klienta. Ponadto Klient

ponosi wyłączną odpowiedzialność za testowanie i wdrażanie Produktu Osadzanego w rozwiązaniu CIMA.

Dalsze postanowienia umieszczone w niniejszym paragrafie mają zastosowanie, jeśli Usługi Przetwarzania w Chmurze opisane w niniejszym dokumencie są świadczone przez podmiot inny niż International Business Machines Corporation, spółka zarejestrowana w Nowym Jorku (zwana dalej „IBM Corporation"). Prawa do pakietu SDK i Elementu Podlegającego Redystrybucji opisanych niniejszym dokumencie są udzielane przez IBM Corporation. W ramach niniejszej Umowy IBM występuje jako dystrybutor dostarczający pakiet SDK i Element Podlegający Redystrybucji i ponosi odpowiedzialność za egzekwowanie warunków oraz spełnianie wszelkich zobowiązań dotyczących takiego pakietu SDK i Elementu Podlegającego Redystrybucji, a niniejsza Umowa nie daje Klientowi żadnej podstawy roszczeniowej wobec IBM Corporation. Klient zrzeka się wszelkich roszczeń i podstaw roszczeniowych wobec IBM Corporation, a w odniesieniu do wszelkich praw, odszkodowań i zadośćuczynień związanych z pakietem SDK i Elementem Podlegającym Redystrybucji zobowiązuje się kontaktować wyłącznie z IBM.

2. Specyfikacje techniczne dotyczące przetwarzania i ochrony danych

Dodatek IBM dotyczący Przetwarzania Danych dostępny pod adresem http://ibm.com/dpa (dalej „DPD") oraz Specyfikacja Techniczna dotycząca Przetwarzania i Ochrony Danych (dalej „Specyfikacja Techniczna" lub „Załącznik Szczegółowy do DPD") dostępna za pośrednictwem zamieszczonych poniżej odsyłaczy zawierają dodatkowe informacje na temat ochrony danych dla Usług Przetwarzania w Chmurze oraz ich opcji. Informacje te precyzują, jakie rodzaje Zawartości mogą być przetwarzane przez daną Usługę, jakie czynności przetwarzania są realizowane, jakie są opcje ochrony danych, a także jakie są szczegółowe zasady przechowywania i zwrotu Zawartości. Jeśli do Zawartości stosuje się i) ogólne rozporządzenie o ochronie danych (RODO – UE/2016/679) lub ii) inne regulacje dotyczące ochrony danych osobowych określone pod adresem http://ibm.com/dpa/dpl, to w zakresie, w jakim przepisy te mają zastosowanie do danych osobowych uwzględnionych w Zawartości, obowiązuje DPD.

Dla uniknięcia wątpliwości wyjaśnia się, że w Specyfikacjach Technicznych wymienione są zwykle wszystkie lokalizacje, w których IBM (w tym ewentualni podwykonawcy IBM jako podmiotu przetwarzającego będący osobami trzecimi) udostępnia i przetwarza Dane Osobowe, niezależnie od centrum przetwarzania danych, z którego usługi są wdrażane. Lista lokalizacji udostępniających i przetwarzających Dane Osobowe, powiązanych z centrum przetwarzania danych, z którego usługi są wdrażane, znajduje się w paragrafie 5.1 (Informacje o dodatkowych miejscach przetwarzania).

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

3. Poziomy Usług i wsparcie techniczne

3.1 Umowa dotycząca Poziomu Usług

IBM udostępnia Klientowi przedstawioną poniżej Umowę dotyczącą Poziomu Usług („SLA"). IBM naliczy najwyższe obowiązujące wyrównanie na podstawie łącznej dostępności Usługi Przetwarzania w Chmurze, zgodnie z poniższą tabelą. Dostępność wyrażona procentowo jest równa ilorazowi łącznej liczby minut w danym miesiącu obowiązywania umowy, pomniejszonej o łączną liczbę minut Wyłączenia Usługi w tym miesiącu, oraz łącznej liczby minut w tym miesiącu. Definicja Wyłączenia Usługi, opis procesu zgłaszania reklamacji oraz opis sposobu kontaktowania się z IBM w sprawach związanych z dostępnością usług znajdują się w podręczniku wsparcia dla Usługi Przetwarzania w Chmurze IBM pod adresem https://www.ibm.com/software/support/saas_support_overview.html.

Dostępność	Uznanie (% miesięcznej opłaty za subskrypcję*)
Poniżej 99,9%	2%
Poniżej 99,0%	5%
Poniżej 95,0%	10%

* Opłata za subskrypcję oznacza cenę w miesiącu obowiązywania umowy, którego dotyczy reklamacja.

3.2 Wsparcie techniczne

Informacje o wsparciu technicznym dla Usługi Przetwarzania w Chmurze, w tym dane kontaktowe, poziomy istotności, godziny świadczenia usług, czasy reakcji oraz inne informacje i procesy, można znaleźć w podręczniku wsparcia IBM, dostępnym pod adresem https://www.ibm.com/support/home/pages/support-guide/ (należy wybrać odpowiednią Usługę Przetwarzania w Chmurze).

4. Opłaty

4.1 Opłaty rozliczeniowe

Opłaty rozliczeniowe za Usługę Przetwarzania w Chmurze są określone w Dokumencie Transakcyjnym.

Przy sprzedaży niniejszej Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie jednej z następujących miar:

- Uprawniony Uczestnik to osoba lub podmiot uprawniony do uczestnictwa w dowolnym programie świadczenia usługi zarządzanym lub monitorowanym za pomocą Usług Przetwarzania w Chmurze.
- Urządzenie Klienckie to urządzenie, które żąda komend wykonawczych, procedur lub aplikacji ze środowiska serwera uzyskującego dostęp do Usług Przetwarzania w Chmurze bądź otrzymuje takie komendy wykonawcze, procedury lub aplikacje.

5. Warunki dodatkowe

Dla Umów o Usługi Przetwarzania w Chmurze (lub podstawowych umów o usługi przetwarzania w chmurze będących ich odpowiednikami) zawartych przed 1 stycznia 2019 r. mają zastosowanie warunki zamieszczone pod adresem https://www.ibm.com/acs.

5.1 Informacje o dodatkowych miejscach przetwarzania

Udostępnianie i przetwarzanie Danych Osobowych, również przez ewentualnych podwykonawców podmiotu przetwarzającego będących osobami trzecimi, którzy zostali wyszczególnieni w Specyfikacji Technicznej, będzie się odbywać w całości w następujących miejscach:

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Niemcy, Izrael, Irlandia i Holandia.

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Japonii IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Japonia, Izrael i Irlandia.

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Stanach Zjednoczonych IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Stany Zjednoczone, Izrael, Irlandia, Singapur i Australia.

Oprócz powyższych lokalizacji dla wszystkich usług świadczonych przez centra przetwarzania danych w Niemczech, Japonii i Stanach Zjednoczonych dane dotyczące wsparcia mogą być udostępniane lub przetwarzane w Niemczech i Francji przez firmę Salesforce.Com będącą zewnętrznym podwykonawcą IBM jako podmiotu przetwarzającego.

Usługi wsparcia i serwisowania kont IBM Trusteer mogą być również udostępniane w razie potrzeby, w miarę dostępności odpowiedniego personelu IBM, lokalizacji Klienta oraz centrum przetwarzania danych, w którym przechowywane są odpowiednie dane.

5.2 Zintegrowane rozwiązania

Dla uniknięcia wątpliwości precyzuje się, że różne produkty oferowane w ramach marki Trusteer mogą stanowić zintegrowane rozwiązanie. W związku z tym, jeśli Klient przestanie korzystać z jednej z takich Usług Przetwarzania w Chmurze, IBM może zatrzymać Dane Klienta w celu świadczenia mu pozostałych Usług Przetwarzania w Chmurze zgodnie z niniejszym Opisem Usługi, a także innych usług Trusteer zgodnie z opisami mającymi do nich zastosowanie.

5.3 Weryfikacja

Klient będzie i) prowadzić i na żądanie dostarczać rekordy i dane wyjściowe narzędzi systemowych w zakresie niezbędnym dla IBM i jego niezależnych rewidentów w celu zweryfikowania, czy Klient

przestrzega Umowy, oraz ii) niezwłocznie zamawiać i opłacać wszelkie niezbędne uprawnienia według cen obowiązujących w danym czasie, a także uiszczać inne opłaty oraz spełniać inne zobowiązania stwierdzone w wyniku takiej weryfikacji, zgodnie z fakturą wystawioną przez IBM. Takie zobowiązania w zakresie weryfikacji zgodności pozostają w mocy przez cały okres świadczenia Usługi Przetwarzania w Chmurze i przez dwa lata po jego zakończeniu.

5.4 Dane gromadzone w związku z wdrażaniem usługi

Wdrożenie Usługi Przetwarzania w Chmurze może wymagać od Klienta przekazania IBM określonych danych. Wytyczne dotyczące danych, które Klient przekazuje IBM w związku z wdrożeniem usługi, znajdują się w „Wytycznych dotyczących wdrażania usługi Trusteer”, które zostaną udostępnione Klientowi.

6. Warunki unieważniające

6.1 Wykorzystanie danych

Następujące postanowienie ma znaczenie rozstrzygające w przypadku, gdy którekolwiek z postanowień paragrafu „Ochrona Zawartości i Danych” warunków podstawowych dotyczących Usługi Przetwarzania w Chmurze, które zostały uzgodnione między Stronami, jest z nim sprzeczne: IBM nie będzie wykorzystywać ani ujawniać rezultatów używania Usługi Przetwarzania w Chmurze przez Klienta, które występują wyłącznie w Zawartości (Rezultatach) Klienta lub w inny sposób umożliwiają jego identyfikację. IBM będzie jednak wykorzystywać Zawartość oraz inne oparte na niej informacje (z wyjątkiem Rezultatów) w ramach Usługi Przetwarzania w Chmurze w celu jej usprawnienia.IBM może również udostępniać identyfikatory zagrożeń i inne informacje dotyczące bezpieczeństwa osadzone w Zawartości na potrzeby wykrywania zagrożeń i ochrony przed nimi.