Regulamin Asseco Medical Cloud Backup (Regulamin AMCB)

Wydany w dniu 11.05.2018 przez Operatora Systemu Asseco Medical Cloud Backup

Postanowienia ogólne

§ 1

1. Regulamin Asseco Medical Cloud Backup określa warunki zakładania i prowadzenia Konta Asseco Medical Cloud Backup oraz świadczenie usługi Asseco Cloud Medical Backup, obowiązuje w oparciu o art. 8 ust. 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług droga elektroniczną (Dz. U.Dz.U.2016. 1030) i art. 384 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U.2016.380).
2. Operator Systemu Asseco Medical Cloud Backup udostępnia aplikację i klucz aktywacyjny do utworzenia konta Asseco Medical Cloud Backup umożliwiających korzystanie z usług przechowywania zaszyfrowanych kopii baz danych z wykorzystaniem repozytorium danych w chmurze.
3. Regulamin wchodzi w życie z dniem 25.05.2018

§ 2

1. Użyte w Regulaminie AMBS określenia należy rozumieć w następujący sposób:

a) **Operator Systemu Asseco Medical Cloud Backup(Operator AMCB)** - Designed.ly Sp. z o.o. z siedziba w Szczecinie ul. Chobolańska 27/5, 71-023 Szczecin, zarejestrowana w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy Szczecin-Centrum w Szczecinie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000463921, REGON: 321383478, NIP 8522603061, wysokość kapitału zakładowego 140.000 zł.

b) **Strona internetowa Dystrybutora Systemu AMCB:**

c) **Asseco Medical Cloud Backup**- jest aplikacją przeznaczoną do obsługi bezpiecznie przechowywanych, zaszyfrowanych kopii baz danych, nie stanowiących danych osobowych, o których mowa w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE- zwanego dalej „ Rozporządzenie”. Do jej funkcjonalności należą w szczególności:

- archiwizacja bazy danych „na żądanie”- tj. w dowolnym momencie, w którym użytkownik ręcznie wywoła wykonanie archiwizacji bazy danych,
- przechowywanie zaszyfrowanych kopii bazy danych w zdalnym repozytorium danych,
- automatyczne rotowanie kopii w ramach podstawowego planu przechowywania danych w repozytorium: 7 ostatnich kopii dziennych, 52 ostatnie kopie tygodniowe,
- automatyczna archiwizacja bazy danych wg zadanego harmonogramu,
- automatyczne odtworzenie bazy danych, *z zastrzeżeniem, że część silników baz danych może wymagać podstawowej wiedzy z zakresu administracji systemem bazodanowym związanej z przygotowaniem środowiska, w którym możliwe jest odtworzenie bazy danych;*

d) **usługi Asseco Medical Cloud Backup**– usługi w modelu Software as a Service, codzienne wykonywanie kopii bazy danych Użytkownika Konta Asseco Medical Cloud Backup według harmonogramu ustalonego przez Użytkownika w ustawieniach konta Asseco Medical Cloud Backup, szyfrowanie utworzonych kopii przy pomocy wygenerowanego w Asseco Medical Cloud Backup klucza publicznego, a następnie przesyłanie zaszyfrowanych kopii bazy danych w celu archiwizacji do repozytorium danych w chmurze, odtworzenie bazy danych i odszyfrowanie danych przy pomocy wygenerowanego przez Użytkownika w Asseco Medical Cloud Backup klucza prywatnego. Operator Systemu Asseco Medical Cloud Backup udostępnia narzędzia pozwalające na wykonanie lokalnie, na sprzęcie Użytkownika Konta Asseco Medical Cloud Backup:
    - aktywacji konta w zdalnym repozytorium z wykorzystaniem jednorazowego Klucza Aktywacyjnego wysyłanego przez Operatora Systemu Asseco Medical Cloud Backup,
    - konfiguracji kluczy prywatnego i publicznego oraz ustalenie hasła do ww. kluczy (niezbędnych do szyfrowania i odszyfrowywania danych),
    - konfiguracji dostępu do bazy danych, z której mają być realizowane kopie oraz określenie zakresu archiwizowanych danych (zakres archiwizowanych danych można konfigurować w przypadku wybranych motorów baz danych),
    - konfiguracji harmonogramu kopii zapasowych,
    - wykonanie kopii zapasowej bazy danych „na żądanie", zaszyfrowanie kopii z wykorzystaniem klucza publicznego klienta i przesłanie zaszyfrowanej kopii danych do zdalnego repozytorium danych,
    - wykonanie kopii zapasowej wg ustalonego przez Użytkownika harmonogramu, zaszyfrowanie kopii z wykorzystaniem klucza publicznego klienta i przesłanie kopii do zdalnego repozytorium danych,
    - odtworzenie wybranej kopii (z przechowywanych w zdalnym repozytorium danych) poprzez pobranie kopii ze zdalnego repozytorium danych, odszyfrowanie z wykorzystaniem klucza prywatnego oraz hasła (przechowywanych przez klienta) oraz odtworzenie do wskazanego przez klienta motoru bazy danych;
e) **„Użytkownik konta Asseco Medical Cloud Backup" (Użytkownik Konta AMCB) (Użytkownik)** – przedsiębiorca, który zawarł umowę z Dystrybutorem Systemu Asseco Medical Cloud Backup na świadczenie usług w ramach funkcjonalności Asseco Medical Cloud Backup;
f) **konto Asseco Medical Cloud Backup (Konto AMCB)**- zaszyfrowany identyfikator i hasło użytkownika usługi umożliwiający korzystanie z usługi Asseco Medical Cloud Backup, a w szczególności zapis zaszyfrowanej kopii bazy danych i jej pobranie poprzez dostęp do zdalnego repozytorium danych;
g) **umowa konta Asseco Medical Cloud Backup**– umowa zawarta pomiędzy Dystrybutorem Systemu Asseco Medical Cloud Backup, a Użytkownikiem konta Asseco Medical Cloud Backup, regulująca zasady świadczenia usługi Asseco Medical Cloud Backup i korzystania z konta Asseco Medical Cloud Backup na warunkach Regulaminu Asseco Medical Cloud Backup;
h) **Formularz zamówienia Asseco Medical Cloud Backup–** formularz stanowiący załącznik nr 2 do Regulaminu;
i) **Regulamin Asseco Medical Cloud Backup–** regulamin przewidujący warunki świadczenia usługi Asseco Medical Cloud Backup oraz ogólne warunki umowy konta Asseco Medical Cloud Backup;
j) **opłata –** wynagrodzenie Dystrybutora Systemu Asseco Medical Cloud Backup za świadczenie Usługi Asseco Medical Cloud Backup za dostęp do Konta Asseco Medical Cloud Backup,

k) **opłata roczna –** opłata uiszczana jednorazowo z góry za aktywację lub prolongatę aktywacji, w wysokości zgodnej z Cennikiem aktualnym w dniu przesłania Formularza Zamówienia Asseco Medical Cloud Backup,
l) **Aktywacja**– prawo korzystania z Usług Asseco Medical Cloud Backup przez pierwszy okres na jaki zostały zamówione od dnia realizacji zamówienia konta Asseco Medical Cloud Backup System;
m) **Prolongata Aktywacji** – prawo korzystania z Usługi Asseco Medical Cloud Backup przez kolejny okres od dnia zapłaty Opłaty zgodnie z Regulaminem i Cennikiem Asseco Medical Backup System;
n) **Cennik Asseco Medical Cloud Backup–** załącznik nr 3 do Regulaminu zawierający opłaty za poszczególne wersje Asseco Medical Cloud Backup z uwzględnieniem systemu płatności rocznej.
o) **dzień roboczy –** każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy;
p) **Dystrybutor Asseco Medical Cloud Backup(Dystrybutor AMCB) –** Asseco Poland S.A., który na podstawie umowy zawartej z Operatorem Systemu sprzedaje Aktywację lub Prolongatę Aktywacji;
q) **adres email Użytkownika** – email wskazany przez Użytkownika w Formularzu zamówienia Asseco Medical Cloud Backup, na który wysyłane są cotygodniowe raporty z wynikami przeprowadzonych przez tydzień archiwizacji, jak również klucz aktywacyjny oraz informacje dotyczące obsługi konta, w tym faktury, informacje dotyczące płatności, a także możliwości prolongaty aktywacji.
r) **adres email administratora** - email wskazany przez Użytkownika w Formularzu zamówienia Asseco Medical Cloud Backup, na który wysyłane są codzienne raporty z wynikami przeprowadzonych codziennie archiwizacji,
s) **klucz aktywacyjny –** ciąg znaków wysyłany Użytkownikowi przez Operatora Systemu, niezbędny do poprawnej konfiguracji usługi Asseco Medical Cloud Backup oraz aktywacji Konta Asseco Medical Cloud Backup,
t) **klucz prywatny –** klucz wykorzystywany do odszyfrowania informacji,
u) **hasło Użytkownika –** hasło zabezpieczające Klucz Prywatny, odpowiadające wymogom formalno-prawnym, przewidzianym w powszechnie obowiązujących przepisach,
v) **klucz publiczny –** klucz wykorzystywany do zaszyfrowania informacji,
w) **plik ratunkowy** – unikalny, zaszyfrowany plik, zabezpieczony Hasłem Użytkownika generowany przez aplikację, niezbędny do odzyskania danych z repozytorium danych, zawierający klucz prywatny oraz dane logowania niezbędne do dostępu do repozytorium danych, musi być przechowywany przez Użytkownika w bezpiecznym miejscu, niedostępnym dla osób postronnych,
x) **repozytorium danych** – centrum danych zgodnych z wymaganiami Tier 3, z certyfikacją ISO 9001:2008, ISO/IEC 27001:2013, AQAP 2110:2016, PN-N 19001:2006 (WSK), na serwerach zlokalizowanych w serwerowniach Asseco Data Systems w Szczecinie,
y) **kopia dzienna –** kopia wykonywana codziennie, według harmonogramu ustalonego przez Użytkownika,
z) **kopia tygodniowa –** ostatnia dostępna dzienna kopia z danego tygodnia,
aa) **archiwa -** zaszyfrowane kopie danych klienta, przechowywane w „repozytorium danych";

Zawarcie umowy konta Asseco Medical Cloud Backup

§ 3

1. Konto Asseco Medical Cloud Backup utworzone zostaje dla Użytkownika Konta Asseco Medical Cloud Backup po zawarciu przez Dystrybutora Asseco Medical Cloud Backup umowy konta Asseco

Medical Cloud Backup z Użytkownikiem Konta Asseco Medical Cloud Backup i, po zaakceptowaniu przez Użytkownika Regulaminu Asseco Medical Cloud Backup za pomocą podpisania i przesłania formularza – Formularza Zamówienia Asseco Medical Cloud Backup.

2. Po podpisaniu i przesłaniu do Dystrybutora Formularza Zamówienia Asseco Medical Cloud Backup, generowane jest dla Użytkownika konto Asseco Medical Cloud Backup, oraz wysyłany na adres mailowy Użytkownika klucz aktywacyjny, link do aplikacji Asseco Medical Cloud Backup, oraz faktura z terminem zapłaty 14 dni.
3. Konto Asseco Medical Cloud Backup jest aktywne po:

a) zainstalowaniu przez Użytkownika aplikacji Asseco Medical Cloud Backup,
b) Podpisaniu a tym samym zaakceptowaniu przez Użytkownika konta Regulaminu AMBC, co oznacza, że:
    - zapoznał się z Regulaminem konta Asseco Medical Cloud Backupi zobowiązuje się do jego przestrzegania,
    - wszelkie dane, udostępnia Operatorowi AMBS dobrowolnie i ze świadomością, że dostęp do tych danych może mieć Operator Systemu Asseco Medical Cloud Backup na warunkach przewidzianych w Regulaminie Asseco Medical Cloud Backup,
c) aktywowaniu konta przy pomocy klucza aktywacyjnego.

4. Od momentu aktywacji konta do czasu jego usunięcia Operator Systemu Asseco Medical Cloud Backup świadczy na rzecz Użytkownika usługi Asseco Medical Cloud Backup.
5. W przypadku nieuiszczenia przez Użytkownika Asseco Medical Cloud Backup kwoty, na którą została wystawiona faktura w terminie 14 dni od aktywacji konta, konto wraz z przechowywanymi danymi jest usuwane, o czym Użytkownik Konta Asseco Medical Cloud Backup zostanie zawiadomiony na adres mail użytkownika.

Licencja

§ 4

Z chwilą aktywacji Konta Asseco Medical Cloud Backup Operator Systemu Asseco Medical Cloud Backup udziela Użytkownikowi odwołalnej, niewyłącznej, i niezbywalnej licencji na korzystanie z aplikacji Asseco Medical Cloud Backup, o której mowa w § 3 ust. 2. Użytkownik uprawniony jest do instalacji wskazanej aplikacji oraz korzystania z niej zgodnie z przeznaczeniem w miejscu i czasie przez siebie wybranym przez okres za jaki została uiszczona Opłata.

Warunki świadczenia usług

§ 5

1. W celu korzystania z usługi Asseco Medical Cloud Backup niezbędne jest by Użytkownik posiadał :
    a) Dostęp do Internetu o przepustowości łącza wystarczającej do transmisji danych klienta z zastrzeżeniem ust. 2.
    b) Aktywny adres email (w przypadku zatrudnienia / współpracy z administratorem systemu informatycznego również jego adres email na potrzeby raportowania),
    c) Komputer z jednym z niżej wskazanych systemów operacyjnych:
        - Windows Vista,
        - Windows 7,
        - Windows 8/8.1,
        - Windows 10,

- Windows Server 2008/2012,
- Oracle Linux,
- Red Hat Linux,
- Ubuntu Linux.

d) jeden z niżej wskazanych silników bazodanowych z bazą nie przekraczającą 2TB wielkości:
   - Firebird 2.0, 2.5, 3.0
   - Oracle XE, 10g, 11g (SE, SE One, Enterprise) 12c (SE2, Enterprise).

2. W przypadku łącza internetowego o ograniczonej przepustowości może wystąpić sytuacja, w której dzienna kopia nie zdąży zostać przesłana do zdalnego repozytorium danych przed kolejną dzienną kopią zaplanowaną w harmonogramie. Operator systemu na dodatkowe zlecenie Użytkownika może przed aktywacją Konta Asseco Medical Cloud Backup lub w terminie 14 dni po jego aktywacji wykonać analizę, której wynikiem będzie ocena ryzyka wystąpienia ww. sytuacji. Wykonanie analizy jest możliwe po udzieleniu informacji dotyczących przepustowości łącza internetowego.
3. Operator Systemu Asseco Medical Cloud Backup nie ponosi odpowiedzialności za nieprawidłowe działanie Asseco Medical Cloud Backup ze względu na zaistnienie okoliczności o których mowa w ust. 2.

Bezpieczeństwo danych zapisanych na koncie

§ 6

1. Operator systemu zapewnia ochronę danych wprowadzonych do Asseco Medical Cloud Backup przed dostępem osób trzecich.
2. Bezpieczeństwo danych zapewnione jest poprzez:
   - szyfrowanie pliku ratunkowego i pliku konfiguracji w standardzie AES-128 z SHA-512 po stronie Użytkownika,
   - szyfrowanie kopii bazy danych w standardzie AES-256 po stronie Użytkownika,
   - transmisja danych z wykorzystaniem protokołu SSL/TLS,
   - weryfikację integralności deponowanych w repozytorium zaszyfrowanych kopii baz w oparciu o skrót MD5;

   Nadto zaszyfrowane dane przed potwierdzeniem transmisji są przechowywane w redundantnych urządzeniach.
3. Dane wprowadzone do Asseco Medical Cloud Backup są przechowywane w repozytorium danych dopiero po ich zaszyfrowaniu przez Użytkownika kluczem publicznym. Do odszyfrowania archiwum niezbędny jest plik ratunkowy (zawierający klucz prywatny i dane dostępowe do zdalnego repozytorium) i hasło, które generowane są przez Użytkownika i są w jego wyłącznym posiadaniu.
4. Zarówno Dystrybutor jak i Operator Systemu Asseco Medical Cloud Backup nie ma dostępu do pliku ratunkowego, jego zawartości i hasła Użytkownika, nie ma też żadnej inne faktycznej możliwości odszyfrowania przechowywanych danych.
5. Użytkownik ponosi wyłączną odpowiedzialność za bezpieczeństwo pliku ratunkowego, hasła oraz wszelkie przypadki korzystania z jego Konta Asseco Medical Cloud Backup przy użyciu pliku ratunkowego i hasła;
6. Użytkownik ponosi wyłączną odpowiedzialność za utratę pliku ratunkowego, klucza prywatnego i hasła.
7. W przypadku utraty pliku ratunkowego, klucza prywatnego, hasła bądź ich skompromitowania, Użytkownik:
   a) nie będzie miał możliwości odszyfrowania kopii przechowywanych w zdalnym repozytorium,
   b) powinien jak najszybciej wygenerować z poziomu bezpłatnego narzędzia (aplikacji) udostępnianego przez Operatora Systemu Asseco Medical Cloud Backup nowy plik ratunkowy

wraz z nowym hasłem. Tylko kopie zaszyfrowane przez posiadaną przez Użytkownika parę kluczy oraz hasłem będzie można nimi odszyfrować.

8. Operator Systemu Asseco Medical Cloud Backup nie ma możliwości odtworzenia utraconych plików ratunkowych, kluczy i hasła.
9. Operator Systemu Asseco Medical Cloud Backup nie ma dostępu do danych zapisywanych na Koncie Użytkownika. Część administratorów Operatora Systemu Asseco Medical Cloud Backup może w wyjątkowych sytuacjach, wymagających administracji zdalnym repozytorium danych, mieć dostęp do zaszyfrowanych kopii danych klientów, jednak nigdy Operator Systemu Asseco Medical Cloud Backup, jego pracownicy i osoby z nim współpracujące nie mają dostępu do wnętrza zaszyfrowanych archiwów, gdyż do odszyfrowania archiwum (kopii danych klienta) niezbędny jest plik ratunkowy (klucz prywatny) i hasło, które generowane są przez Użytkownika i są w jego wyłącznym posiadaniu.

Prawa i obowiązki stron

§7

1. Użytkownik ponosi wyłączną odpowiedzialność za treść danych rejestrowanych na koncie Asseco Medical Cloud Backup.
2. Użytkownik może wykorzystać konto Asseco Medical Cloud Backup tylko do celów zgodnych z prawem.
3. Użytkownik zobowiązuje się do niepodejmowania ani nieumożliwiania innych osobom przeprowadzania modyfikacji, tworzenia elementów pochodnych, tłumaczenia, dekompilacji, demontażu lub łamania kodu Asseco Medical Cloud Backup. Zabronione jest również przekazywanie praw udzielonych Użytkownikowi innym osobom.
4. Użytkownik nie jest uprawniony do:
   a) usuwania, dokonywania jakichkolwiek zmian treści przesyłanych w ramach Asseco Medical Cloud Backup,
   b) wprowadzania wirusów, robaków, programów internetowych oraz innych kodów lub instrukcji w celu spowodowania awarii, usunięcia, uszkodzenia lub dezasemblacji Asseco Medical Cloud Backup lub wywołujących taki skutek.
5. Użytkownik nie jest upoważniony do przenoszenia praw wynikających z Umowy Konta Asseco Medical Cloud Backup w tym licencji na inne osoby.

§ 8

1. Operator Systemu Asseco Medical Cloud Backup nie ponosi odpowiedzialności za dostęp do danych wprowadzonych do Asseco Medical Cloud Backup przez osoby nieupoważnione, jeżeli osoby te uzyskał dostęp do tych danych wskutek świadomych lub nieświadomych działań Użytkownika.
2. Operator Systemu Asseco Medical Cloud Backup nie odpowiada za szkody powstałe w wyniku wadliwego działania Asseco Medical Cloud Backup oraz Konta Asseco Medical Cloud Backup niezawinionego przez Operatora Systemu Asseco Medical Cloud Backup, w tym z przyczyn leżących po stronie operatorów telekomunikacyjnych, awarii sprzętu Użytkownika.
3. Operator Systemu Asseco Medical Cloud Backup nie ponosi odpowiedzialności za treści zamieszczane na Koncie Asseco Medical Cloud Backup.
4. Operator Systemu Asseco Medical Cloud Backup nie ponosi odpowiedzialności za utratę danych spowodowaną awarią sprzętu Użytkownika, systemów informatycznych oraz innymi okolicznościami niezależnymi od Operatora Systemu Asseco Medical Cloud Backup.

5. Odpowiedzialność odszkodowawcza Operatora Systemu za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy konta Asseco Medical Cloud Backup i świadczenia usług Asseco Medical Cloud Backup jest limitowana do wartości ostatnio uiszczonej przez Użytkownika opłat za aktywację lub prolongatę aktywacji Konta.
6. Operator Systemu Asseco Medical Cloud Backup może w każdym momencie bez konieczności informowania Użytkownika rozbudować Asseco Medical Cloud Backup o dodatkowe elementy i funkcje oraz naprawić błędy, aktualizować i modyfikować Asseco Medical Cloud Backup.
7. Operator Systemu Asseco Medical Cloud Backup zastrzega sobie prawo do:
   a) okresowego wyłączania dostępności Asseco Medical Cloud Backup w celu rozbudowy lub konserwacji,
   b) sporadycznych, krótkich przerw w dostępie do Asseco Medical Cloud Backup i Konta Asseco Medical Cloud Backup bez podania przyczyn zgodnych z SLA usługi stanowiącego załącznik do regulaminu,
   c) natychmiastowego zaprzestania świadczenia Usługi Asseco Medical Cloud Backup w przypadku, gdy Użytkownik naruszy postanowienia Regulaminu Konta Asseco Medical Cloud Backup lub prawa autorskie Operatora Systemu Asseco Medical Cloud Backup, o czym Użytkownik zostanie powiadomiony na adres email użytkownika.
8. Dostępność usług repozytorium danych jest gwarantowana zgodnie z SLA repozytorium danych, stanowiącego załącznik nr 1 do regulaminu.

Okres obowiązywania umowy i płatności

§ 9

1. Użytkownik Asseco Medical Cloud Backup wypełniając Formularz Zamówienia Asseco Medical Cloud Backup wybiera wersję produktu, do którego przypisana jest cena za okres zamówienia.
2. Aktualny cennik stanowi załącznik nr 3 do regulaminu.
3. Wersja dla baz Oracle obsługująca bazy danych do wielkości 2TB.
4. Umowa konta Asseco Medical Cloud Backup zawierana jest na czas nieokreślony, z zastrzeżeniem, że po upływie pierwszego okresu - Aktywacji, Użytkownik wykupi prolongatę aktywacji na kolejny okres.
5. W przypadku upływu okresu Aktywacji i braku Prolongaty Aktywacji lub braku kolejnej prolongaty aktywacji po upływie poprzedniej, umowa wygasa, konto jest bezpowrotnie usuwane wraz z archiwami Użytkownika.
6. Opłatę wnosi się jednorazowo z góry za okres zamówienia według wyboru Użytkownika dokonanego na Formularzu zamówienia Asseco Claoud Medical Backup.
7. W przypadku gdy Użytkownik korzystał z aktywacji uiszczając opłatę jednorazowo, na 1 miesiąc przed końcem okresu Aktywacji lub Prolongaty Aktywacji Dystrybutor Systemu Asseco Medical Cloud Backup przypomni o zbliżającym się upływie okresu Aktywacji lub Prolongaty wysyłając odpowiednią informację na adres email użytkownika oraz fakturę wystawioną na opłatę za prolongatę aktywacji na kolejne 12 miesięcy z terminem zapłaty 14 dni. W przypadku braku zapłaty opłaty w tym terminie Dystrybutor Systemu Asseco Medical Cloud Backup wysyła na adres email Użytkownika ponowienie uprzednio wysyłanego przypomnienia z dodatkową informacją, że konto Asseco Medical Cloud Backup prowadzone dla Użytkownika zostanie za 14 dni zablokowane. Jeśli w ostatnim dniu aktywacji na konto bankowe wskazane na fakturze

Dystrybutora Asseco Medical Cloud Backup nie wpłynie opłata, konto zostaje zablokowane, na adres email Użytkownika wysyłany jest mail, że konto zostało zablokowane.

8. W przypadku braku zapłaty za prolongatę aktywacji w ciągu kolejnych 14 dni od zablokowania konta zgodnie z ust. 7, Dystrybutor Systemu Asseco Medical Cloud Backup wysyła na adres email użytkownika informację, że jeśli w ciągu 14 kolejnych dni nie zapłaci opłaty za prolongatę aktywacji, to po 14 dniach wszystkie archiwa Użytkownika zostaną bezpowrotnie usunięte (bez możliwości odzyskania).

Postępowanie reklamacyjne

§ 10

1. Użytkownik Konta Asseco Medical Cloud Backup może zgłosić skutecznie reklamacje dotyczące niewykonywania lub nienależytego wykonywania umowy konta Asseco Medical Cloud Backup i świadczenia usług Asseco Medical Cloud Backup sporządzając ją w formie pisemnej, wysyłając na adres Dystrybutora Sytemu Asseco Medical Cloud Backup i zamieszczając w niej następującą treść:
   a) dane Użytkownika Konta umożliwiające kontakt z nim oraz identyfikację,
   b) opis nieprawidłowości, okoliczności uzasadniające zasadność reklamacji.
2. Dystrybutor Systemu Asseco Medical Cloud Backup zobowiązany jest udzielić odpowiedzi na reklamację, w terminie 14 dni od daty jej doręczenia z zastrzeżeniem, że jeśli konieczne będzie uzupełnienie treści reklamacji, pozyskanie dodatkowych informacji lub wyjaśnień, termin ten będzie biegł od udzielenia powyższych uzupełnień, informacji, wyjaśnień. Dystrybutor Systemu Asseco Medical Cloud Backup powinien w terminie 14 dni od zgłoszenia reklamacji wezwać do uzupełnienia reklamacji, udzielenia dodatkowych informacji lub wyjaśnień.

Zmiana postanowień Regulaminu Konta Asseco Medical Cloud Backup

§ 11

1. Zmiany Regulaminu Konta Asseco Medical Cloud Backup dokonywane w czasie obowiązywania Umowy Konta Asseco Medical Cloud Backup oraz termin ich wprowadzenia zamieszczane są na stronie internetowej Dystrybutora Systemu Asseco Medical Cloud Backup oraz wysyłane na email Użytkownika.
2. W terminie 14 dni od dnia zamieszczenia Zmian Regulaminu Konta Asseco Medical Cloud Backup na stronie internetowej Dystrybutora Systemu Asseco Medical Cloud Backup i wysłania ich na email Użytkownika, Użytkownik może złożyć pisemne oświadczenie o wypowiedzeniu Umowy Konta Asseco Medical Cloud Backup. Po upływie terminu 14 dni strony wiąże Umowa Konta Asseco Medical Cloud Backupo treści wynikającej ze zmienionego Regulaminu Konta Asseco Medical Cloud Backup.

§ 12

1. W przypadku rozwiązania Umowy lub jej wygaśnięcia ze względu na nieuiszczenie opłaty za Prolongatę Aktywacji Operator Systemu Asseco Medical Cloud Backup niezwłocznie usuwa wszelkie dane zapisane na Koncie Asseco Medical Cloud Backup Użytkownika.
2. W przypadku wypowiedzenia lub odstąpienia od Umowy przez Użytkownika, uiszczone opłaty nie są zwracane.

3. Jeżeli jakiekolwiek postanowienia niniejszego Regulaminy AMBS okażą się nieważne, nie uchybia to ważności pozostałych.
4. W sprawach nieuregulowanych w Regulaminie AMBS stosujemy przepisy prawa polskiego.

Ochrona danych osobowych

§ 13

1. Administratorem danych osobowych Użytkownika konta Asseco Medical Cloud Backup jest Designed.ly Sp. z o.o. z siedzibą w Szczecinie ul. Chobolańska 27/5, 71-023 Szczecin, zarejestrowana w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy Szczecin-Centrum w Szczecinie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000463921, REGON: 321383478, NIP 8522603061, wysokość kapitału zakładowego 140.000 zł.
2. Z Administratorem można się kontaktować:
   a) listownie, na adres: ul. Chobolańska 27/5, 71-023 Szczecin,
   b) mailowo, na adres: ado@designed.ly
3. Administrator powołał Inspektora Ochrony Danych Osobowych, z którym można się kontaktować:
   a) listownie, na adres: ul. Wojska Polskiego 42/5, 70-475 Szczecin
   b) mailowo, na adres: iod@designed.ly
4. Dane osobowe Użytkownika konta AMCB, podane w Formularzu zamówienia Asseco Medical Cloud Backup przetwarzane są na podstawie art. 6 ust. 1 lit. b) Rozporządzenia tj. przetwarzanie jest niezbędne do wykonania umowy konta AMCB, której stroną jest umowa, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy.
5. Administrator wdrożył odpowiednie środki techniczne i organizacyjne, o których mowa w art. 32 Rozporządzenia,
6. Dane osobowe Użytkownika konta AMCB mogą być udostępniane przez Administratora:
   a) pracownikom i współpracownikom Designed.ly Sp. z o.o. z siedziba w Szczecinie,
   b) podmiotom prowadzącym działalność pocztową lub kurierską.
7. Dane osobowe będą przetwarzane przez okres obowiązywania umowy konta AMCB.
8. Użytkownikowi konta AMCB przysługuje prawo do żądania dostępu do jego danych osobowych, ich, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
9. Użytkownik konta AMCB ma prawo do wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych.
10. Użytkownikowi konta AMCB przysługuje prawo do wniesienia sprzeciwu wobec przetwarzania jego danych:
    a) gdy zaistnieją przyczyny związane ze szczególną sytuacją Użytkownika konta AMCB, a przetwarzane danych oparte jest na podstawie niezbędności dla celów wynikających z prawnie uzasadnionych interesów Administratora lub
    b) w dowolnym momencie, gdy dane przetwarzane są na potrzeby marketingu bezpośredniego, w tym profilowania, przy czym po wniesieniu sprzeciwu wobec przetwarzania danych dla celów marketingowych nie wolno już przetwarzać danych do takich celów.
11. Użytkownik konta AMCB może realizować uprawnienia wymienione w ust. 8 i 10 poprzez przekazanie pisemnego oświadczenia na adres Administratora wskazany w ust. 2.

12. Administrator ma obowiązek udzielenia Użytkownikowi konta AMCB informacji o działaniach podjętych w związku z żądaniami, o których mowa w ust. 8 bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania. W razie potrzeby termin, o którym mowa w zdaniu poprzedzającym, może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje Użytkownika konta AMCB o takim przedłużeniu terminu z podaniem przyczyny opóźnienia.
13. Jeżeli Administrator nie podejmie działań w związku z żądaniem Użytkownika konta AMCB o których mowa w ust. 8, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje Użytkownika konta AMCB o powodach nie podjęcia działań oraz o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, oraz skorzystania ze środków ochrony prawnej przed Sądem.
14. Podanie danych osobowych jest warunkiem zawarcia umowy konta AMCB.

……

Załącznik nr 1 do Regulaminu AMCB – warunki SLA repozytorium danych

1. Repozytorium danych zobowiązuje się do zapewnienia minimalnego poziomu dostępności Usługi wynoszącego 95,5% w skali danego miesiąca kalendarzowego obowiązywania Umowy.
2. Repozytorium danych zobowiązuje się podjąć wszelkie działania mające na celu zapewnienie prawidłowego funkcjonowania infrastruktury informatycznej będącej Przedmiotem Umowy.
3. Z zastrzeżeniem zasad ustalonych w pkt 5 Okna Serwisowe oraz Przerwy Konserwacyjne nie będą uwzględniane w wyliczaniu poziomu dostępności Usług.
4. Brak dostępności Usługi niezawiniony przez Repozytorium Danych, nie wpływa na obniżenie całkowitego czasu dostępności Usługi.
5. Przerwa Konserwacyjna (Okno Serwisowe) może wystąpić maksymalnie 2 razy w miesiącu, za każdym razem poza Godzinami Roboczymi. Maksymalna długość okna serwisowego może trwać łącznie 12h.
6. Podczas Okna Serwisowego będzie mógł wystąpić brak dostępu do Usług.
7. Repozytorium danych nie jest zobowiązane do uzyskania zgody na Przerwę Konserwacyjną.
8. Podczas Okna Serwisowego Repozytorium Danych może wykonywać wszystkie niezbędne prace techniczne.

Załącznik nr 2 do Regulaminu AMCB – formularz zamówienia

ZAMÓWIENIE

ZAMAWIAJĄCY/UŻYTKOWNIK/PŁATNIK:	
Nazwa:	
Imię i nazwisko osoby reprezentującej:	
Adres:	
e-mail, tel./faks	
Dane do faktury (NIP):	
Opiekun handlowy/Partner	

PRZEDMIOT ZAMÓWIENIA:

USŁUGA						
Planowany termin realizacji:						
Lp	**Opis**	**Ilość**	**Wartość netto**	**Podatek VAT**	**Wartość brutto**	**Okres zamówienia (lata)**
1	Asseco MCB – instancja medyczna	1		23%		1 / 2 / 3
2	Asseco MCB – instancja laboratoryjna	1		23%		1 / 2 / 3
3	Asseco MCB – instancja administracyjna	1		23%		1 / 2 / 3
	ŁĄCZNIE:			**23%**		

Płatność:	
Termin płatności:	14 dni od daty wystawienia faktury

…….

Załącznik nr 3 do Regulaminu AMCB – Cennik

ASSECO MEDICAL CLOUD BACKUP			
Opłata roczna	Instancja medyczna (AMMS/Infomedica – Oracle)	Instancja laboratoryjna (Infomedica – Oracle)	Instancja Administracyjna (Infomedica – Oracle)
	7 499,00 zł netto	**1 999,00 zł netto**	**1 999,00 zł netto**
Archiwizacja „ na żądanie”	√	√	√
Archiwizacja zgodnie z harmonogramem	√	√	√
Szyfrowanie danych	AES-256	AES-256	AES-256
Odtwarzanie kopii	√	√	√
Przechowywanie kopii w bezpiecznym repozytorium	√	√	√
Transfer	Bez limitu	Bez limitu	Bez limitu
Szyfrowana transmisja danych	SSL/TLS	SSL/TLS	SSL/TLS
Automatyczne rotowanie kopii * zgodnie ze schematem 7 ostatnich dziennych 52 ostatnie tygodniowe	√	√	√
Szyfrowanie pliku ratunkowego	AES-128 z SHA-512	AES-128 z SHA-512	AES-128 z SHA-512
Szyfrowanie pliku konfiguracji	AES-128 z SHA-512	AES-128 z SHA-512	AES-128 z SHA-512
Dzienne raporty dla administratora	√	√	√
Tygodniowe raporty dla ADO	√	√	√
Poziom bezpieczeństwa data center	Zgodne z wymaganiami Tier 3, z certyfikacją ISO 9001:2008, ISO/IEC 27001:2013, AQAP 2110:2016, PN-N 19001:2006 (WSK)	Zgodne z wymaganiami Tier 3, z certyfikacją ISO 9001:2008, ISO/IEC 27001:2013, AQAP 2110:2016, PN-N 19001:2006 (WSK)	Zgodne z wymaganiami Tier 3, z certyfikacją ISO 9001:2008, ISO/IEC 27001:2013, AQAP 2110:2016, PN-N 19001:2006 (WSK)