REGULAMIN I WARUNKI PROCESU WIDEOIDENTYFIKACJI

ORAZ WYDAWANIA CERTYFIKATÓW KRÓTKOTERMINOWYCH

QES ONCE

SIGNICAT, S.L.U. (Wcześniej nazywana Electronic Identification, S.L.) z siedzibą pod adresem Avenida Ciudad de Barcelona 81, 4ª Planta, zarejestrowana w Rejestrze Handlowym w Madrycie dnia 13 marca 2013 r. pod numerem CIF B86681533, (zwana dalej „SIGNICAT SLU"), jest Kwalifikowanym Dostawcą Zaufanych Usług, które działają zgodnie z przepisami Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 910/2014 z dnia 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w zakresie transakcji elektronicznych we wnętrzu rynku oraz uchylenia dyrektywy 1999/93/ CE, a także normy techniczne ETSI mające zastosowanie do wydawania i zarządzania certyfikatami kwalifikowanymi, głównie EN 319 411-1 i EN 319 411-2, w celu ułatwienia zgodności z wymaganiami prawnymi i międzynarodowego uznania jej usług.

Z drugiej strony UŻYTKOWNIK lub WNIOSKODAWCA, których dane identyfikacyjne dla celów niniejszej Umowy są zawarte w używanym Dokumencie Identyfikacyjnym oraz, w filmie wideo, wygenerowanym w wyniku procesu identyfikacji wideo i wydawania certyfikatu.

1. PODMIOT

Celem niniejszego dokumentu jest poinformowanie Wnioskodawcy/Użytkownika w jasnej i zrozumiałej formie o aktualnym *„Regulaminie procesu identyfikacji wideo i wydawania certyfikatów krótkoterminowych"* oraz uregulowaniu usług według ustalonych warunków w niniejszym dokumencie, *Kodeks Postępowania Certyfikacyjnego, Rozporządzenie eIDAS* oraz *przepisy lokalne, które mogą być zastosowane*.

Ten powyżej wskazany proces identyfikacji jest niezbędny do akredytacji tożsamości Wnioskodawcy/Użytkownika, który wnioskuje o SIGNICAT SLU o wydanie kwalifikowanego certyfikatu podpisu elektronicznego osoby fizycznej o krótkim czasie trwania („Usługi Certyfikacyjne"), certyfikatu podlegającego warunkom Certyfikacji Elektronicznej, usługi świadczonej przez SIGNICAT SLU jako kwalifikowanego dostawcę usług zaufania opisana poniżej.

UŻYTKOWNIK przyjmuje do wiadomości i zaświadcza, że przeczytanie i zaakceptowanie niniejszego dokumentu poprzez zaznaczenie pól wyboru będzie uważane za zwykły podpis.

2. DEFINIJCE

- **URZĄD CERTYFIKACYJNY (CA):** zaufany podmiot nadawcy i odbiorcy wiadomości. To zaufanie obu stron do „zaufanej strony trzeciej" zezwala każdemu z nich zaufać dokumentom podpisanym przez Urząd Certyfikacji, w szczególności tym, które identyfikują każdy klucz publiczny z jego odpowiednim właścicielem i są nazwane certyfikatami. W ramach świadczenia Usługi zleconej przez Użytkownika SIGNICAT SLU będzie pełnił rolę Urzędu Certyfikacji, związanego z wydaniem Certyfikatu przypisującego określony klucz publiczny do konkretnego użytkownika.

- **ORGAN REJESTRACYJNY (RA):** podmiot, który między innymi bezbłędnie identyfikuje wnioskodawcę certyfikatu oraz w podobnych przypadkach inne okoliczności związane z certyfikatem zgodnie z postanowieniami sekcji 1.3.2. Urzędy Rejestracyjne CPS należące do SIGNICAT SLU. Urząd Rejestracji dostarcza Urzędowi Certyfikacji zweryfikowane dane wnioskodawcy, aby Urząd Certyfikacji mógł wydać odpowiedni certyfikat. Wszystkie lub każdą z funkcji RA może przejąć albo bezpośrednio SIGNICAT SLU, albo dowolny podmiot upoważniony przez SIGNICAT SLU.

- **CERTYFIKAT PODPISU ELEKTRONICZNEGO:** elektroniczne oświadczenie, które łączy dane weryfikujące podpis z osobą fizyczną i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

- **KWALIFIKOWANY CERTYFIKAT PODPISU ELEKTRONICZNEGO:** certyfikat podpisu elektronicznego, który został wystawiony przez kwalifikowanego dostawcę usług zaufania i spełnia wymagania określone w załączniku I Rozporządzenia UE 910/2014 z dnia 23 lipca 2014 r. (Rozporządzenie eIDAS), dający najwyższe gwarancje prawne dotyczące identyfikacji osoby podpisującej i jego powiązania z firmą w unikalny sposób, integralności i niezaprzeczalności danych, o ile są one powiązane z firmą.

- **OŚWIADCZENIE O PRAKTYKACH CERTYFIKACYJNYCH („CPS**"): jest to dokument przygotowany przez Urząd Certyfikacji, który zbiera lub reguluje świadczenie usług certyfikacyjnych przez dany Urząd Certyfikacji w charakterze Dostawcy Usług Certyfikacyjnych, w tym przypadku SIGNICAT SLU. Reguluje m.in. rozporządzanie danymi dotyczącymi tworzenia i weryfikacji podpisu oraz Certyfikatami, warunkami dotyczącymi wniosku, wystawianiem, używaniem, zawieszeniem i zakończeniem ważności Certyfikatów.

- **KWALIFIKOWANY PODPIS ELEKTRONICZNY:** zaawansowany podpis elektroniczny składany za pomocą kwalifikowanego urządzenia do tworzenia podpisu elektronicznego, oparty na kwalifikowanym certyfikacie podpisu elektronicznego. Ważność podpisu jest iuris tantum, ponieważ jest to podpis kwalifikowany, ciężar dowodu spoczywa na osobie, która odrzuca podpis jako ważny.

- **KWALIFIKOWANY DOSTAWCA USŁUG ZAUFANIA**: dostawca usług zaufania, który świadczy przynajmniej jedną usługę zaufania kwalifikowaną, i któremu organ nadzorczy przyznał kwalifikację.

- **UŻYTKOWNIK LUB WNIOSKODAWCA**: jest osobą fizyczną wskazaną w tytule zlecającą usługi certyfikacji SIGNICAT SLU, która przed wydaniem certyfikatu kwalifikowanego zażądała i poprawnie zrealizowała Proces Wideo Identyfikacji SIGNICAT SLU.

3. REGULAMIN I WARUNKI PROCESU WIDEOIDENTYFIKACJI

Proces Identyfikacji Wnioskodawcy Usług Identyfikacyjnych świadczonych przez SIGNICAT SLU w celu wydawania certyfikatów elektronicznych będzie realizowany w jeden z następujących sposobów, zgodnie z art. 24 ust. 1 eIDAS:

a) z udziałem osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, dla której Wnioskodawca musi stawić się w biurach SIGNICAT SLU z adresem Av. de la Ciudad de Barcelona, 81, 4, 28007 Madryt, Hiszpania, ze względu na brak Urzędów Rejestrów delegowanych.

b) Zdalnie, za pomocą środków identyfikacji elektronicznej, dla których przed wydaniem kwalifikowanego certyfikatu zapewniono obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej oraz zgodnie z procesem wideo identyfikacji, o którym mowa

w niniejszym dokumencie i Kodeksem Postępowania Certyfikacyjnego, który jest dostępny w następującym linku:
https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wystawionej zgodnie z lit. a) lub b).

d) stosując inne ze sposobów identyfikacji uznane na szczeblu krajowym, które zapewniają bezpieczeństwo równorzędne pod względem niezawodności fizycznej obecności. Bezpieczeństwo równorzędne zostanie potwierdzone przez jednostkę oceniającą zgodność.

3.1. WALIDACJA TOŻSAMOŚCI ZA POMOCĄ ŚRODKÓW ELEKTRONICZNYCH I OPIS PROCESU IDENTYFIKACJI WIDEO

Proces identyfikacji obrazu wideo (zwany dalej „Procesem identyfikacji obrazu wideo" lub „Procesem") jest metodą zdalnej weryfikacji tożsamości obrazu wideo, która jest świadczona za pośrednictwem autorskiego pakietu bibliotek oprogramowania, interfejsów aplikacji REST i aplikacji internetowych („Aplikacja"), która realizuje, wspiera i rejestruje cały proces rejestracji osoby oraz umożliwia zdalne sprawdzanie poprawności dokumentów tożsamości poprzez nagrywanie wideo. Ten film To wideo rejestruje i potwierdza dokument tożsamości w czasie rzeczywistym i automatycznie. Automatycznie (około 10-20 sekund), co jest realizowane przez SIGNICAT SLU za pośrednictwem wykwalifikowanych agentów ludzkich, którzy jako operatorzy weryfikacji działający jako urząd rejestracyjny odpowiadają za potwierdzanie tożsamości.

3.1.1. Generalne informacje o procesie identyfikacji wideo

Wnioskodawca wchodzi do Aplikacji i interfejsu i przed przystąpieniem do czynności mających na celu weryfikację tożsamości proszony jest o zapoznanie się z regulaminem wyrażenie zgody na niniejszy dokument oraz o dobrowolne wyrażenie zgody na przetwarzanie danych biometrycznych niezbędnych do realizacji wideo- identyfikacji. W tym celu SIGNICAT SLU uprzednio przekazuje wnioskodawcy Politykę Prywatności zawierającą przetwarzanie danych osobowych w ramach Procesu zgodnie z Przepisami o Ochronie Danych.

W przypadku, gdy Wnioskodawca nie wyraża takiej zgody, Proces nie może być kontynuowany, i Wnioskodawca musi skorzystać z jednej z alternatywnych metod identyfikacji wskazanych w punkcie Pierwszej Klauzuli niniejszego dokumentu zgodnie z postanowieniami art. 24 ust. 1 Rozporządzenia eIDAS .

Po zapoznaniu się przez Wnioskodawcę z polityką prywatności i dobrowolnym wyrażeniu zgody, proces będzie kontynuowany.

Przez cały proces identyfikacji wideo wnioskodawca jest kierowany audio i tekstem, a za pośrednictwem Aplikacji dokonywana jest automatyczna kontrola elementów otoczenia (warunki oświetlenia, sieć, jakość kamer), które pozwalają uzyskać optymalny zapis identyfikacji wideo i jej dowody. W taki sposób etapy procesu poprzedzające do wydania

certyfikatu kwalifikowanego są następujące:

Pierwszy etap Procesu wskazuje Wnioskodawcy, że musi pokazać dokument tożsamości, którego będzie używał w celu porównania obrazów z oryginalnymi dokumentami za pomocą technologii patternmatchingu w celu weryfikacji autentyczności dokumentu i przeprowadzenia ekstrakcji danych (OCR) MRZ lub innych części dokumentu oraz możliwość wywoływania poświadczeń w czasie rzeczywistym.

Wtedy zostanie uchwycona przednia część dokumentu tożsamości używanego przez wnioskodawcę podczas tego procesu. Żeby tego dokonać Wnioskodawca zostanie poproszony o pokazanie przedniej części dokumentu i dopasowanie go do pokazanego pola.

Po zakończeniu przechwytywania wyświetlony będzie komunikat o zgodności oraz nastąpi kolejny etap.

Następnym krokiem jest przechwycenie tylnej części dokumentu. Wnioskodawca zostanie poproszony o pokazanie tyłu dokumentu i dopasowanie obrazu do pokazanego pola. Po zakończeniu przechwytywania wyświetlany jest komunikat o zgodności oraz nastąpi kolejny etap.

Kolejno zbierane są dane biometryczne Wnioskodawcy w celu dokonania porównania w czasie rzeczywistym z wizerunkiem dokumentu tożsamości dla procesu rozpoznawania twarzy opartego na automatycznej punktacji biometrycznej. Żeby tego dokonać Wnioskodawca zostanie poproszony o pokazanie twarzy i dopasowanie jej do pokazanego pola.

Po zebraniu danych biometrycznych Wnioskodawca proszony jest o wykonanie ruchu twarzy do kamery jako dowód życia, jeśli wszystko jest w porządku, wyświetlony zostanie komunikat o zgodności i kontynuowana jest kolejna część procesu.

Jeżeli cały Proces przebiega prawidłowo, Wnioskodawca zostaje poinformowany, że Proces identyfikacji wideo został zakończony, a dowody wygenerowane w trakcie Procesu zostaną sprawdzone i zweryfikowane za pomocą Narzędzia Weryfikacyjnego Punktu Rejestracji w celu dokonania przeglądu Procesu przez wykwalifikowaną osobę, która została wcześniej przeszkolona poprzez specjalne szkolenie.

W tym momencie Aplikacja łączy się z wykwalifikowanym ludzkim Agentem odpowiedzialnym za weryfikację tożsamości Wnioskodawcy Procesu i żąda asynchronicznego przeglądu nagranego wideo, a także pozostałych dowodów i elementów uzyskanych podczas Procesu. Średni czas weryfikacji agenta wynosi zwykle około trzech minut.

Następnie użytkownik zostanie poproszony o podanie numeru telefonu w celu wysłania

mu OTP. Za pomocą niniejszego OTP użytkownik, oprócz zatwierdzenia niniejszych warunków, będzie wyrażał zgodę na wydanie Certyfikatu, w tym w tym samym czasie dane uzyskane z procesu identyfikacji wideo zgodnie z punktem 3.3.5 niniejszego dokumentu.

3.1.2. Elementy bezpieczeństwa procesu identyfikacji wideo i zatwierdzenie przez wykwalifikowanego agenta ludzkiego

W przypadku przeglądu asynchronicznego przez Kwalifikowanego Przedstawiciela istnieje protokół bezpieczeństwa oparty na dobrych praktykach UE, który jest wspierany przez narzędzie oferowane Kwalifikowanej Przedstawicielowi, w którym przedstawiane są dowody uzyskane podczas procesu, a także flagi lub powiadomienia tych nieuzyskanych.

Nagranie wideo, prośba o weryfikację wideo-identyfikacji, oraz opinia Wykwalifikowanego Agenta są śledzone w Aplikacji, a do każdego śladu nanoszony jest znacznik czasu, aby zapewnić jego spójność i integralność.

W związku z tym Proces zapewnia łańcuch nadzoru weryfikacji od dowodów zebranych przez Proces do śladów łączących identyfikację z wykwalifikowanym ludzkim Agentem Punktu Rejestracji. W taki sposób wynikiem jest zweryfikowana tożsamość z technicznym zabezpieczeniem równowartościowym przeprowadzonej w fizycznej obecności Wnioskodawcy.

Po pozytywnej weryfikacji tożsamości przez wykwalifikowanego agenta ludzkiego tożsamość wnioskodawcy zostanie akredytowana i będzie on mógł konturować w Elektronicznej Usłudze Certyfikacji SIGNICAT SLU, która umożliwia kontynuację procesu wydawania certyfikatu osoby kwalifikowanej oraz podpisywania dokumentów elektronicznych.

W przypadku negatywnego wyniku Procesu kontynuowanie Procesu Wydawania Certyfikatu Kwalifikowanego nie będzie możliwe, a Wnioskodawca musi fizycznie udać się do biur SIGNICAT SLU w celu przeprowadzenia bezpośredniej weryfikacji swojej tożsamości.

3.2. OBOWIĄZKI WNIOSKODAWCY W ZWIĄZKU Z PROCESEM WIDEO IDENTYFIKACJI

Wnioskodawca przez cały Proces zobowiązuje się do:

- Korzystania z Usługi zgodnie z postanowieniami niniejszego dokumentu, Kodeksu, w szczególnych warunkach, które mogą mieć zastosowanie, oraz z wszelkimi innymi instrukcjami lub procedurą dostarczoną przez SIGNICAT SLU.

  Dokument tożsamości użyty w Procesie jest dokumentem autentycznym, prawnie ważnym oraz że dodatkowo:

- Nie jest to kserokopia ani drukowana karta:
- Nie jest w formacie cyfrowym (telefon komórkowy, tablet lub komputer).
- Nie jest w pokrowcu.
- Nie jest uszkodzony i jest kompletny, ze wszystkimi zabezpieczeniami w dokumencie.

- Że podczas procesu i przechwytywania wideo, aby nie zostało odrzucone:

  - Warunki oświetleniowe w filmie muszą umożliwiać dobrą widoczność twarzy zidentyfikowanej osoby i dokumentu.
  - Wideo musi mieć stały przepływ, bez cięć i opóźnień.
  - Żyjąca osoba musi okazać dowód tożsamości.
  - Jeżeli inna osoba, niż osoba, która ma zostać zidentyfikowana, przeprowadza cały Proces, identyfikacja zostanie odrzucona.
  - Jeśli podczas wideo rozmowy jest obecna inna osoba, ale wyraźnie nie zmusza tej osoby do identyfikacji, identyfikacja może być ważna, tak jak w przypadku, gdy dana osoba pomaga osobie niepełnosprawnej w dokonaniu identyfikacji.
  - Muszą być wyraźnie widoczne wszystkie części uchwyconego dokumentu, przodu, tyłu i twarzy osoby.
  - Użytkownik nie może spać ani wykazywać oznak, które mogłyby zostać zinterpretowane jako stan nietrzeźwości bądź odurzenia.

3.3. WYDANIE, DOSTAWA I AKCEPTACJA CERTYFIKATU

3.3.1. WNIOSEK O CERTYFIKACJĘ I GENEROWANIE KLUCZY PRZEZ SIGNICAT SLU W IMIENIU UŻYTKOWNIKA

Po zakończeniu procesu identyfikacji wideo UŻYTKOWNIK upoważnia SIGNICAT SLU do generowania i zarządzania kluczami publicznymi i prywatnymi w jego imieniu, umożliwiając SIGNICAT SLU przystąpienie do wydawania kwalifikowanego krótkoterminowego certyfikatu osoby fizycznej i podpisanie nim/ w jego imieniu dokumentów elektronicznych udostępnianych za pośrednictwem SIGNICAT SLU lub osób trzecich o charakterze publicznym lub prywatnym, z którymi SIGNICAT SLU utrzymuje określone porozumienia umowne.

3.3.2. WIARYGODNOŚĆ INFORMACJI

UŻYTKOWNIK będzie odpowiedzialny za wszystkie informacje, które przekaże do SIGNICAT SLU, bezpośrednio lub za pośrednictwem dokumentu tożsamości używanego podczas procesu wydawania certyfikatu. Muszą być dokładne,

kompletne do celów certyfikatu i stale aktualizowane, aby zagwarantować użycie ważnego i zgodnego z prawem dokumentu tożsamości, który nie został zmieniony i/lub zmodyfikowany przez UŻYTKOWNIKA lub przez osoby trzecie.

3.3.3. WYDANIE CERTYFIKATU

W celu wydania zaświadczenia SIGNICAT SLU będzie wykorzystywał dane z dokumentu tożsamości przekazanego przez UŻYTKOWNIKApodczas procesu wideoidentyfikacji. Informacje te zostaną wyodrębnione za pomocą SIGNICAT SLU i bezpośrednio włączone do certyfikatu elektronicznego w celu powiązania tożsamości UŻYTKOWNIKA z certyfikatem elektronicznym.

3.3.4. DOSTAWA CERTYFIKATU

W procesie wydawania certyfikatu krótkoterminowego nie następuje konkretne dostarczenie certyfikatu UŻYTKOWNIKOWI. SIGNICAT SLU będzie nim zarządzać jako Kwalifikowany Dostawca Usług Zaufania, tak aby UŻYTKOWNIK mógł go używać do elektronicznego podpisu dokumentów.

3.3.5. AKCEPTACJA WYDANIA CERTYFIKATU I ZATWIETRDENIE NINIEJSZYCH WARUNKÓW

ABONENT, podając swój numer telefonu i potwierdzając OTP zgodnie z punktem 3.1.1, będzie zazwalał na wydanie certyfikatu, w tym danych pochodzących z procesu identyfikacji wideo i potwierdzeń niniejszych Warunków.

3.4. USŁUGA PODPISU SERWERA

Po zakończeniu procesu identyfikacji, wprowadzeniu hasła jednorazowego (OTP) i potwierdzeniu tożsamości przez agenta weryfikującego, tożsamość osoby podpisującej zostanie zagwarantowana, a UŻYTKOWNIKOWI zostaną wyraźnie przedstawione następujące dokumenty w celu kontynuowania elektronicznego podpisu:

- o Odbiorca umowy do podpisania
- o Wezwanie do działania w celu zaakceptowania tego dokumentu
- o Opcja pobierania umożliwiająca użytkownikowi zapisanie dokumentu.

Aby kontynuować proces, UŻYTWKONIK powinien przejrzeć i zaakceptować dokument, w przeciwnym razie musi zostać poinformowany, że proces nie może być kontynuowany.

W celu akceptacji dokumentu UŻYTKOWNIK jest informowany, że zostanie wysłany drugi SMS z nowym OTP (6 cyfr) wymaganym do uzupełnienia podpisu,

dla którego UŻYTKOWNIK upoważni SIGNICAT SLU jako kwalifikowany zaufany dostawca usług do zastosowania danych tworzenia podpisu, zapewniających jego wyłączną kontrolę.

Aplikacja zweryfikuje te informacje i jeśli są poprawne, przystąpi do wystawienia certyfikatu i podpisania dokumentu. Certyfikat jest ważny 1 dzień i służy wyłącznie do podpisania zaakceptowanego dokumentu.

SIGNICAT SLU udziela UŻYTKOWNIK, na zasadzie niewyłącznej i nieprzekazywalnej, licencji na używanie kopii oprogramowania bezpiecznego urządzenia kryptograficznego SIGNICAT SLU do obsługi urządzenia do podpisu, w stosownych przypadkach, a także do produkcji podpisu elektronicznego, certyfikatu oraz pozostałe usługi kryptograficzne przez osoby podpisujące.

UŻYTKOWNIK może wykonywać kopie oprogramowania wyłącznie do celów archiwizacji lub tworzenia kopii zapasowych.

W przypadku, gdy ktokolwiek inny niż SIGNICAT SLU dokona modyfikacji dostarczonego oprogramowania, wszelkie gwarancje dotyczące oprogramowania zostaną natychmiast anulowane.

4. OGÓLNE WARUNKI USŁUGI ZAUFANIA

4.1. OGÓLNE WARUNKI USŁUGI WIDEO IDENTYFIKACJI

- Okres Przechowywania Informacji

Wszelkie informacje związane z procesem wideo identyfikacji dla wydania certyfikatów elektronicznych dla osób fizycznych, w tym informacja biometryczna, będą przechowywane przez SIGNICAT SLU przez umówiony okres, chyba że ich usunięcie będzie wymagane. Także w okresie przedawnienia kiedy mogą powstać czynności prawne lub roszczenia, które mogą otrzymać organy urzędowe.

W tym sensie maksymalny okres przechowywania odpowiednich informacji w związku z procesem wideo identyfikacji i wydawania kwalifikowanych certyfikatów, czyli kopii nagrania wideo, zdjęć lub zrzutów ekranu Wnioskodawcy oraz użytego dokumentu tożsamości, automatyczny wynik weryfikacji przeprowadzonej przez Aplikację SIGNICAT SLU, jak również ocena i obserwacje przeprowadzone przez wykwalifikowanych agentów weryfikacji tożsamości ludzi, wraz z ich decyzją o zatwierdzeniu lub odrzuceniu identyfikacji, będą miały 15 lat liczonych od daty wydanie zaświadczenia, chyba że prawo stanowi inaczej. Po zakończeniu relacji dane użytkownika zostaną należycie zablokowane, zgodnie z postanowieniami obowiązującego regulaminu.

Ponadto zgłasza się, że wszystkie dowody niekompletnych procesów identyfikacji, które nie zostały ukończone z powodu podejrzenia próby oszustwa, będą przechowywane przez okres 5 lat od wykonania procesu, z wyszczególnieniem przyczyny ich

niedokończenia. Zgodnie z ustanowioną w tym celu polityką.

- Ograniczenie Odpowiedzialności w Zakresie Procesu Wideoidentyfikacji

O jakości procesu: SIGNICAT SLU gwarantuje odpowiednie wykonanie Usług Wideo Identyfikacji opisanych w niniejszym dokumencie pod warunkiem właściwego wykorzystania środków udostępnionych UŻYTKOWNIKOWI zgodnie z instrukcjami SIGNICAT SLU.

Dostęp i korzystanie z usług identyfikacji wideo nie oznacza zobowiązania ze strony SIGNICAT SLU do kontrolowania braku wirusów, robaków lub innych szkodliwych elementów komputera. Wnioskodawca, jako użytkownik, w każdym przypadku jest odpowiedzialny za dostępność odpowiednich narzędzi do wykrywania i dezynfekcji szkodliwych programów komputerowych. SIGNICAT SLU nie ponosi odpowiedzialności za jakiekolwiek uszkodzenia sprzętu komputerowego UŻYTKOWNIKA lub stron trzecich podczas Procesu Identyfikacji Wideo.

O dostępności Procesu: Działanie Procesu Wideo Identyfikacji może zależeć od poprawnej konfiguracji sprzętu, z którego użytkownik uzyskuje dostęp i rozpoczyna proces identyfikacji wideo, dlatego użytkownik musi postępować zgodnie z oferowane wskazania i we wszystkich przypadkach mają zawsze określone wymagania sprzętowe i programowe.

Również, aby przeprowadzić proces Identyfikacji Wideo, musi być dostępne łącze internetowe. Przebieg procesu może zależeć od odpowiedniej jakości i szybkości połączenia, za pośrednictwem którego UŻYTKOWNIK uzyskuje dostęp do aplikacji, i będzie on jedynym odpowiedzialnym za zapewnienie łączy telekomunikacyjnych, abonamentów lub połączeń internetowych lub wszelkich innych niezbędnych środków technicznych w celu uzyskania dostępu do swoich danych i korzystania z nich.

SIGNICAT SLU nie ponosi odpowiedzialności za jakiekolwiek szkody wynikające lub związane z niewykonaniem lub nienależytym wykonaniem zobowiązań wynikających z odpowiedzialności Wnioskodawcy, nieprawidłowe wykorzystanie wyników Procesu i kluczy lub jakiekolwiek szkody pośrednie, które mogą wyniknąć z korzystania z Procesu lub informacji dostarczonych przez SIGNICAT SLU.

SIGNICAT SLU nie ponosi odpowiedzialności za jakiekolwiek nieścisłości w identyfikacji Wnioskodawcy wynikające z informacji przekazanych przez Wnioskodawcę w trakcie Procesu.

SIGNICAT SLU nie ponosi odpowiedzialności za prawidłowe działanie z niezatwierdzonymi aplikacjami oraz za szkody powstałe w wyniku niemożności skorzystania z tych aplikacji przez Wnioskodawcę.

4.2. OGÓLNE WARUNKI USŁUGI WIDEO IDENTYFIKACJI

- **Ramy Prawne Świadczenia Usług**

Usługi certyfikacyjne SIGNICAT SLU są technicznie i operacyjnie regulowane przez Kodeks

Postępowania Certyfikacyjnego i Politykę Certyfikacji SIGNICAT SLU oraz ich następujące aktualizacje, jak również przez dokumentację uzupełniającą dostarczoną UŻYTKOWNIKOWI, który oświadcza, że zna w momencie podpisywania niniejszej Umowy. Tak więc, niniejsze ogólne warunki, Kodeks postępowania Certyfikacyjnego oraz Zasady Certyfikacji, tworzą ramy prawne obowiązujące podczas emisji certyfikatu, które będą regulować relacje między SIGNICAT SLU i UŻYTKOWNIKIEM, pomagać wewnętrznie przeciw osobom trzecim, bez zagrożenia temu co przedstawione w obowiązującym prawie.

Dlatego niniejszy dokument zawiera najistotniejsze elementy oraz wymogi praw i obowiązków stron.

Obowiązujący Kodeks Postępowania Certyfikacyjnego (CPS) i Szczególne Polityki Certyfikacji (CP) są włączone do niniejszego dokumentu przez odniesienie. Najnowsza zaktualizowana wersja CPS będzie dostępna przez cały czas i bezpłatnie w następujących językach za pośrednictwem linku podanego poniżej:

- **Hiszpański**: https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firma-electronica
- **Angielski**: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

W przypadku rozbieżności, znaczenie warunków zawartych w niniejszej dokument będzie nadrzędne w stosunku do postanowień CPS.

- **Okres Umowy**

Niniejsza Umowa będzie obowiązywać w terminie zbiegającym się z datami wydania i ważności wskazanymi w Certyfikacie Kwalifikowanym osoby fizycznej, o którą wnioskował i zlecił Użytkownik SIGNICAT SLU.

- **Zobowiązania do Właściwego Używania**

UŻYTKOWNIK musi korzystać z usług certyfikacyjnych świadczonych przez SIGNICAT SLU wyłącznie do dozwolonych zastosowań w CPS, które są znane i akceptowane przez UŻYTKOWNIKA poprzez przeczytanie i zaakceptowanie w polach wyboru zawartych w procesie.

UŻYTKOWNIK zobowiązuje się do korzystania z usługi certyfikacji cyfrowej i wszelkich innych elementów technicznych dostarczanych przez SIGNICAT SLU oraz certyfikatów zgodnie z niniejszymi warunkami CPS i CP i szczególnymi warunkami, które mogą mieć zastosowanie, oraz z innymi instrukcjami lub procedurami dostarczonymi przez SIGNICAT SLU UŻYTKOWNIKOWI zgodnie z przepisami obowiązującego prawa.

Zawarcie Usługi Certyfikacyjnej z SIGNICAT SLU dopuszcza wyłącznie korzystania z Certyfikatu w zakresie działalności UŻYTKOWNIKA, zgodnie z celem wnioskowanego rodzaju certyfikatu, tj. Kwalifikowanego Certyfikatu Krótkoterminowego podpisu elektronicznego osoby fizycznej. Po wydaniu certyfikatu UŻYTKOWNIK nie może, o ile nie uzgodniono inaczej między stronami, korzystać z certyfikatu w celach komercyjnych.

Komercyjne wykorzystanie z certyfikatu rozumiane jest jako wszelkie działanie, poprzez które UŻYTKOWNIK oferuje osobom trzecim niezwiązanym z niniejszą umową, odpłatnie lub nieodpłatnie, usługi wymagające użycia wydanego certyfikatu.

- **Transakcje Zabronione**

Usługi certyfikacji cyfrowej świadczone przez SIGNICAT SLU nie zostały zaprojektowane ani nie pozwalają na ich wykorzystanie lub odsprzedaż jako urządzenie kontrolne w sytuacjach niebezpiecznych lub do zastosowań wymagających działań zabezpieczających przed błędami takich jak operacje przy obiektach jądrowych, systemach nawigacyjnych lub łączności lotniczej czy systemy kontroli ruchu lotniczego lub systemy kontroli broni, w przypadku których błąd może bezpośrednio spowodować śmierć, uszkodzenie ciała lub poważne szkody dla środowiska.

- **Obowiązki i Odpowiedzialności SIGNICAT SLU**

a. W Zakresie Świadczenia Usługi Urzędu Rejestru

SIGNICAT SLU zobowiązuje się do zarejestrowania danych certyfikatu i jego późniejszego wydania UŻYTKOWNIKOWI, w celu przeprowadzenia kontroli, jakie uzna za stosowne, dotyczących tożsamości oraz innych danych osobowych i uzupełniających UŻYTKOWNIKÓW oraz w stosownych przypadkach, osób podpisujących.

Te kontrole muszą uwzględniać udokumentowane uzasadnienie dostarczone przez UŻYTKOWNIKA oraz, jeśli SIGNICAT SLU uzna to za konieczne, wszelkie inne istotne dokumenty i informacje dostarczone przez UŻYTKOWNIKA.

W przypadku gdy SIGNICAT SLU znajdzie błędy w danych, które muszą być zawarte w certyfikatach lub które uzasadniają te dane, może dokonać zmian, które uzna za konieczne przed wydaniem certyfikatu lub zawiesić proces wydawania i z UŻYTKOWNIKIEM zarządzać danym incydentem.

W przypadku, gdy SIGNICAT SLU poprawi dane bez uprzedniego zarządzania z UŻYTKOWNIKIEM danym incydentem, musi zgłosić UŻYTKOWNIKOWI dane ostatecznie poświadczone.

SIGNICAT SLU zastrzega sobie prawo do odmowy wydania certyfikatu, gdy przedstawione uzasadnienie dokumentowe jest niewystarczające do prawidłowej identyfikacji i uwierzytelnienia UŻYTKOWNIKA lub gdy proces identyfikacji wideo przeprowadzony przed wydaniem certyfikatu nie został potwierdzony przez SIGNICAT SLU.

Powyższe obowiązki zostaną zawieszone w przypadku, gdy UŻYTKOWNIK pełni funkcję rejestracji i posiada elementy techniczne odpowiadające generowaniu kluczy, wydawaniu certyfikatów, i nagrywanie urządzeń do podpisu firmowego.

b. Zakres Świadczenia Usługi Certyfikacji Cyfrowej

SIGNICAT SLU zobowiązuje się do przestrzegania obowiązków określonych w ustawie 6/2020 z dnia 11 listopada regulującej dane aspekty elektronicznych usług zaufania, a w szczególności do:

a) Wydawać, dostarczać, zarządzać, zawieszać, odwoływać i odnawiać certyfikaty, zgodnie z instrukcjami przekazanymi przez UŻYTKOWNIKA, w przypadkach i z przyczyn opisanych w CPS SIGNICAT SLU.

b) Wykonywać usługi odpowiednimi środkami technicznymi i mediami oraz personelem spełniającym warunki kwalifikacyjne i doświadczenie ustalone w CPS.

c) Przestrzegać poziomów jakości usług, zgodnie z ustaleniami CPS, w wymiarach technicznych, operacyjnych i bezpieczeństwa.

e) Przekazywać stronom trzecim, które o to proszą, status certyfikatów, zgodnie z ustaleniami CPS dla różnych usług weryfikacji certyfikatów.

f) O jakości procesu*:* SIGNICAT SLU gwarantuje odpowiednie wykonanie Usług Certyfikacyjnych opisanych w niniejszym dokumencie pod warunkiem właściwego wykorzystania środków udostępnionych UŻYTKOWNIKOWI zgodnie z instrukcjami SIGNICAT SLU.

Dostęp i korzystanie z Usług Certyfikacyjnych nie oznaczają zobowiązania ze strony SIGNICAT SLU do kontrolowania braku wirusów, robaków lub innych szkodliwych elementów komputerowych. Zależy od użytkownika, w każdym przypadku dostępność odpowiednich narzędzi do wykrywania i dezynfekcji szkodliwych programów komputerowych. SIGNICAT SLU nie ponosi odpowiedzialności za jakiekolwiek uszkodzenia sprzętu komputerowego UŻYTKOWNIKA lub stron trzecich podczas Procesu Identyfikacji Wideo.

g) O dostępności Procesu: Działanie Procesu Certyfikacji może zależeć od poprawnej konfiguracji sprzętu, z którego użytkownik uzyskuje dostęp i rozpoczyna proces identyfikacji wideo, dlatego użytkownik musi postępować zgodnie z oferowanymi wskazaniami i zawsze ma określone wymagania sprzętowe i programowe.

Podobnie, aby przeprowadzić proces certyfikacji, musi być dostępne łącze internetowe. Przebieg procesu może zależeć od odpowiedniej jakości i szybkości połączenia, za pośrednictwem którego UŻYTKOWNIK uzyskuje dostęp do aplikacji, i będzie on jedynym odpowiedzialnym za zapewnienie łączy telekomunikacyjnych, abonamentów lub połączeń internetowych lub wszelkich innych niezbędnych środków technicznych w celu uzyskania dostępu do swoich danych i korzystania z nich.

c. Jako Dostawca Usług Certyfikacyjnych

SIGNICAT SLU ma obowiązek:

a) Publikować prawdziwe informacje zgodne z ustawą 6/2020 z 11 listopada regulującą dane aspekty usług elektronicznych zaufania oraz rozporządzeniem (UE) 910/2014.

b) Nie przechowywać ani nie kopiować samodzielnie lub za pośrednictwem strony trzeciej, danych tworzenia podpisu z wyjątkiem zarządzania nimi w imieniu właściciela w celu zastosowania prywatnych kluczy tworzenia podpisu, poprzez wskazanie UŻYTKOWNIKA za pośrednictwem systemu OTP, który SIGNICAT SLU udostępnia UŻYTKOWNIKOWI do podpisywania dokumentów elektronicznych. W takim przypadku będą korzystać z niezawodnych systemów i produktów, w tym z bezpiecznych kanałów komunikacji elektronicznej, oraz stosować odpowiednie procedury i mechanizmy techniczne i organizacyjne, aby środowisko było zaufane i wykorzystywane pod wyłączną kontrolą posiadacza certyfikatu. Ponadto muszą strzec i chronić dane do tworzenia podpisu przed jakąkolwiek zmianą, zniszczeniem lub nieuprawnionym dostępem, a także gwarantować ich ciągłą dostępność.

c) Mieć publicznie dostępną usługę konsultacyjną dotyczącą stanu ważności lub cofnięcia wydanych certyfikatów.

d) Przestrzegać następujących dodatkowych obowiązków:

1. Okres przechowywania informacji związanych ze świadczonymi usługami zgodnie z art. 24 ust. 2 lit. h) Rozporządzenia (UE) 910/2014 wynosi 15 lat od wygaśnięcia certyfikatu lub zakończenia świadczonej usługi. W przypadku wydawania podmiotom prawnym kwalifikowanej pieczęci elektronicznej lub certyfikatów uwierzytelniania witryn internetowych, dostawcy usług zaufania będą też rejestrować informacje pozwalające ustalenie tożsamości osoby fizycznej, której dostarczono ww. certyfikaty, w celu ich identyfikacji w sądzie lub postępowaniu administracyjnym.

2. Stanowią ubezpieczenie od odpowiedzialności cywilnej na minimalną kwotę 1 500 000 euro, z wyjątkiem sytuacji, gdy usługodawca należy do sektora publicznego. Jeśli świadczy więcej niż jedną kwalifikowaną usługę spośród tych przewidzianych w Rozporządzeniu (UE) 910/2014, zostanie doliczone 500 000 euro więcej dla każdego rodzaju usługi. Powyższa gwarancja może być całkowicie lub częściowo zastąpiona gwarancją bankową lub gwarancją poręczającą, tak aby suma ubezpieczonych sum była zgodna z postanowieniami poprzedniego paragrafu. Kwoty i środki ubezpieczenia i gwarancji ustalone w dwóch poprzednich paragrafach mogą zostać zmienione przez dekret królewski.

3. W przypadku zaprzestania działalności jako Kwalifikowany Dostawca Usług Zaufania należy powiadomić klientów, na rzecz których są świadczone usługi, oraz organ nadzorczy z co najmniej dwumiesięcznym wyprzedzeniem o skutecznym zaprzestaniu działalności, w celu wykazania w miarę możliwości skutecznej dostawy i odbioru. Plan rozwiązania usługodawcy może obejmować przeniesienie klientów po wykazaniu braku sprzeciwu do innego kwalifikowanego usługodawcy, który może przechowywać w tym czasie informacje związane ze świadczonymi usługami. Również należy poinformować organ nadzorczy o wszelkich innych istotnych okolicznościach, które mogą uniemożliwić kontynuacje działalności. O wszczęciu postępowania upadłościowego należy poinformować natychmiastowo po podjęciu decyzji.

4. Przesłać raport oceny do Ministerstwa Gospodarki i Transformacji Cyfrowej na zasadach określonych w art. 20.1 Rozporządzenia (UE) 910/2014. Niedopełnienie tego obowiązku będzie skutkowało cofnięciem kwalifikacji usługodawcy i świadczonej

przez niego usługi oraz skreśleniem go z listy zaufanych, o której mowa w art. 22 ww. Rozporządzenia, po wezwaniu usługodawcy do zaprzestania ww. naruszenie.

e) SIGNICAT SLU przejmie pełną odpowiedzialność względem osób trzecich za działania innych osób lub innych dostawców, którym deleguje wykonywanie jednej lub więcej funkcji niezbędnych do świadczenia elektronicznych usług zaufania, w tym czynności weryfikacji tożsamości przed wydaniem kwalifikowanego certyfikatu.

- GWARANCJE USŁUG CERTYFIKACJI

Gwarancja SIGNICAT SLU na Usługi Certyfikacji Elektronicznej

SIGNICAT SLU gwarantuje, że klucz prywatny urzędu certyfikacji stosowany do wydawania certyfikatów nie został naruszony, chyba że poinformowano inaczej za pośrednictwem rejestru certyfikacji, zgodnie z CPS.

SIGNICAT SLU gwarantuje jedynie UŻYTKOWNIKOWI w momencie wydawania certyfikatu, że:

a) W należytych przypadkach certyfikaty są kwalifikowane na warunkach określonych w Ustawie 6/2020 z dnia 11 listopada regulującej dane aspekty elektronicznych usług zaufania.

b) SIGNICAT SLU nie tworzy ani nie wprowadza fałszywych lub błędnych oświadczeń w żadnych informacjach o certyfikacie, również nie zawiera niezbędnych informacji dostarczonych i zweryfikowanych przez UŻYTKOWNIKA.

c) Wszystkie certyfikaty spełniają wymagania formalne i merytoryczne określone w CPS i PC SIGNICAT SLU.

d) SIGNICAT SLU spełnia procedury określone w CPS.

SIGNICAT SLU dokłada wszelkich starań, aby zapewnić, że każdy produkt dostarczany w ramach świadczenia usług jest wolny od wirusów komputerowych, robaków i innych nielegalnych kodów i zobowiązuje się powiadomić UŻYTKOWNIKA o wszelkich wirusach, robakach lub innych nielegalnych kodach wykrytych w następnych produktach.

- WYŁĄCZENIA GWARANCJI

SIGNICAT SLU nie gwarantuje, żadnego oprogramowania używanego przez UŻYTKOWNIKA certyfikatów, podpisującego lub jakąkolwiek inną osobę do generowania, weryfikowania lub innego wykorzystywania podpisu cyfrowego lub jakiegokolwiek certyfikatu cyfrowego wydanego przez SIGNICAT SLU, z wyjątkiem przypadków, gdy SIGNICAT SLU ma pisemne przeciwne oświadczenie skierowane do SIGNICAT SLU.

- OGRANICZENIA ODPOWIEDZIALNOŚCI JAKO DOSTAWCY ZAUFANYCH USŁUG ELEKTRONICZNYCH

SIGNICAT SLU, w granicach określonych przez obowiązujące prawo, nie ponosi

odpowiedzialności za szkody wyrządzone osobie, na rzecz której świadczyła swoje usługi w dobrej wierze lub osobom trzecim, jeżeli osoba ta poniesie szkodę w którymkolwiek z przewidzianych założeń w rozporządzeniu (UE) 910/2014 lub w następującym:

a) Nieprzekazanie dostawcy usług zaufania prawdziwych, pełnych i dokładnych informacji do świadczenia usługi zaufania, szczególnie danych, które muszą być zawarte w certyfikacie elektronicznym lub które są niezbędne do jego wystawienia, do zakończenia lub zawieszenia jego ważności, gdy jego nieścisłość nie mogła zostać wykryta, działając z odpowiednio przez usługodawcę.

b) Brak przekazywania bez zbędnej zwłoki do SIGNICAT SLU jakiejkolwiek modyfikacji okoliczności mających wpływ na świadczenie usługi zaufania, zwłaszcza tych opisanych w certyfikacie elektronicznym.

c) Niedbałe przekazywanie danych dotyczących tworzenia podpisu, pieczęci lub danych uwierzytelniających witrynę internetową, w zapewnieniu ich poufności oraz w ochronie wszelkiego dostępu lub ujawnienia tych danych lub w przypadkach środków umożliwiających dostęp do nich.

d) Brak żądania zawieszenia lub unieważnienia certyfikatu elektronicznego w przypadku wątpliwości dotyczących zachowania poufności danych dotyczących składania podpisu, pieczęci lub uwierzytelniania witryny lub w przypadkach środków umożliwiających dostęp do nich.

e) Używanie tych danych do stworzenia podpisu, pieczęci lub uwierzytelnienia strony internetowej, gdy wygasł okres ważności certyfikatu elektronicznego lub dostawca usług zaufania powiadomi o wygaśnięciu lub zawieszeniu jego ważności.

SIGNICAT SLU nie ponosi również odpowiedzialności za szkody, jeśli działania odbiorcy są niedbałe.

Oznacza, że odbiorca postępuje niedbale, gdy nie bierze pod uwagę zawieszenia lub utraty ważności certyfikatu elektronicznego lub gdy nie weryfikuje podpisu elektronicznego lub pieczęci.

SIGNICAT SLU nie ponosi odpowiedzialności za szkody w przypadku niedokładności danych zawartych w certyfikacie elektronicznym, jeżeli zostały one potwierdzone za pomocą dokumentu publicznego lub urzędowego, zarejestrowanego w rejestrze publicznym, jeżeli jest to wymagane.

- **OBOWIĄZKI UŻYTKOWNIKA**

UŻYTKOWNIK musi odpowiedzieć każdej osobie za naruszenie swoich zobowiązań, a w szczególności czynności identyfikacyjnych lub w przypadku organu rejestracyjnego, zgodnie z warunkami niniejszego regulaminu.

UŻYTKOWNIK jest odpowiedzialny za wszelką komunikację elektroniczną uwierzytelnioną za pomocą podpisu cyfrowego wygenerowanego przy pomocy jego klucza prywatnego,

gdy certyfikat został zweryfikowany za pomocą mechanizmów i warunków ustanowionych przez SIGNICAT SLU.

Dopóki nie nastąpi powiadomienie, o którym mowa w punkcie 5 niniejszego dokumentu, odpowiedzialność, która może wyniknąć z nieuprawnionego i/lub niewłaściwego użycia certyfikatów, ponosi w każdym przypadku UŻYTKOWNIK.

- ADEKWATNOŚĆ PRODUKTÓW WYKORZYSTUJĄCYCH IDENTYFIKACJĘ, PODPIS ELEKTRONICZNY LUB SZYFROWANIE

SIGNICAT SLU nie ponosi odpowiedzialności za adekwatność istniejących na rynku produktów i usług związanych z certyfikacją cyfrową, identyfikacją, podpisem elektronicznym lub szyfrowaniem, które są wykorzystywane w aplikacjach komputerowych UŻYTKOWNIKA, z wyjątkiem przypadków, gdy dostarcza je SIGNICAT SLU. W takim przypadku strony będą podlegały odpowiednim warunkom użytkowania.

- **WŁASNOŚĆ CERTYFIKATÓW I URZĄDZENIA PODPISUJĄCE**

Dostarczone certyfikaty pozostają własnością UŻYTKOWNIKA.

- **ROZWIĄZANIE**

Rozwiązanie nastąpi w następujących przypadkach:

a) Z powodu naruszenia przez drugą stronę któregokolwiek z jej zobowiązań, jeśli naruszenie to nie zostało rozwiązane:

b) W ciągu trzydziestu dni od otrzymania zawiadomienia dokonanego przez stronę, która nie uchybiła swoim zobowiązaniom.

c) Momentalnie, jeśli naruszenie zagraża bezpieczeństwu usług.

d) Ze względu na zbieżność wszelkich innych przyczyn wcześniejszego rozwiązania, określonych w obowiązujących przepisach, a zwłaszcza w obowiązujących przepisach dotyczących certyfikacji podpisu elektronicznego.

- **POLITYKA POUFNOŚCI**

SIGNICAT SLU nie może ujawniać ani być zmuszany do ujawnienia jakichkolwiek informacji poufnych dotyczących certyfikatów bez uprzedniego wyraźnego wniosku ze strony:

a) Osoby, wobec której SIGNICAT SLU ma obowiązek zachowania informacji w tajemnicy lub

b) Nakazu sądowego, administracyjnego lub innego przewidzianego w obowiązującym prawodawstwie.

Jednakże, jeśli użytkownik zgadza się, że określone informacje osobiste i innego rodzaju, podane we wniosku o wydanie certyfikatu, będą zawarte w jego certyfikatach oraz w

mechanizmie weryfikacji statusu certyfikatu oraz że wymienione informacje nie będą poufne z prawnego nakazu.

- **POLITYKA ZWROTÓW**

SIGNICAT SLU w żadnym wypadku nie zwraca kosztów usługi certyfikacyjnej.

- **OKRES PRZECHOWYWANIA INFORMACJI**

Wszelkie informacje związane z procesem wydawania kwalifikowanych certyfikatów elektronicznych dla osób fizycznych, w tym należycie sformalizowana przez UŻYTKOWNIKA umowa, generowane logi w trakcie wydania, będą przechowywane przez SIGNICAT SLU przez umówiony okres, chyba że ich usunięcie będzie wymagane. Także w okresie przedawnienia kiedy mogą powstać czynności prawne lub roszczenia, które mogą otrzymać organy urzędowe.

W związku z tym maksymalny okres przechowywania ważnych informacji w związku z Procesem wydawania certyfikatów kwalifikowanych będzie wynosił 15 lat od momentu wydania certyfikatu, chyba że przepisy prawa stanowią inaczej. Po zakończeniu relacji dane użytkownika zostaną należycie zablokowane, zgodnie z postanowieniami obowiązującego regulaminu.

5. POSTANOWIENIA OGÓLNE

5.1. MIEJSCE ŚWIADCZENIA DZIAŁALNOŚCI

Miejscem wykonania zobowiązań SIGNICAT SLU związanych z usługami certyfikacji cyfrowej oraz w danych przypadkach licencjami na użytkowanie oprogramowania jest siedziba SIGNICAT SLU.

5.2. ROZDZIELNOŚĆ REGULAMINU I WARUNKÓW

Klauzule niniejszego dokumentu są od siebie niezależne, dlatego jeśli jakakolwiek klauzula zostanie uznana za nieważną lub niemającą zastosowania, pozostałe klauzule będą nadal obowiązywać, chyba że strony wyraźnie uzgodnią inaczej.

5.3. OBOWIĄZUJĄCE PRZEPISY I WŁAŚCIWA KONTROLA PRAWNA

Relacje z SIGNICAT SLU będą regulowane przepisami rozporządzenia (UE) 910/2014 eIDAS, prawem hiszpańskim, a w szczególności wszystkimi tymi, które wynikają z jego polityki zgodności.

Właściwa kontrola prawna jest wskazana w ustawie 1/2000 z dnia 7 stycznia o postępowaniu cywilnym, z wyjątkiem sytuacji, gdy UŻYTKOWNIK jest uważany za konsumenta, w którego przypadku SIGNICAT SLU podda go kontroli, która z prawnego punktu widzenia go obejmuje.