

UMOWA

**o współpracy w zakresie zasilania centralnej ewidencji kierowców w drodze
teletransmisji za pośrednictwem Portalu Internetowego CEPiK, danymi osób,
którym wydano zaświadczenie ADR przewidziane w przepisach o przewozie
towarów niebezpiecznych**

zawarta dnia w Warszawie pomiędzy:

Skarbem Państwa - Ministrem Spraw Wewnętrznych,

w imieniu i na rzecz którego działa :

.....
.....

zwanym dalej „MSW”

a

**Województwem Mazowieckim reprezentowanym przez Zarząd Województwa
Mazowieckiego, w którego imieniu – na podstawie posiadanego upoważnienia – działają:**

1. Katarzyna Wieczorek - Dyrektor Departamentu Nieruchomości i Infrastruktury Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie oraz
2. Jan Bartosz – Zastępcą Dyrektora Departamentu Nieruchomości i Infrastruktury Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie,

zwanym dalej: „Województwem”,

wspólnie zwanymi „Stronami”:

§ 1.

Umowa określa zasady i tryb współpracy umawiających się Stron w zakresie przekazywania przez Marszałka do centralnej ewidencji kierowców za pośrednictwem Portalu Internetowego CEPiK danych osób, które ukończyły kurs przewidziany ustawą z dnia 19 sierpnia 2011 r. o przewozie towarów niebezpiecznych (Dz. U. z 2011 r., Nr 227, poz. 1367).

§ 2.

Dane, o których mowa w § 1 obejmują:

- 1) imię i nazwisko,

- 2) datę i miejsce urodzenia,
- 3) numer PESEL – o ile został nadany, lub rodzaj i numer innego dokumentu potwierdzającego tożsamość,
- 4) zakres i numer wydanego zaświadczenia ADR,
- 5) okres ważności zaświadczenia ADR,
- 6) adres zamieszkania osoby, której wydano zaświadczenie ADR – do dnia 30 czerwca 2012 r.

§ 3.

Minister SW oświadcza, że:

1. do przekazywania, za pośrednictwem aplikacji MWADR, danych określonych w §2 do centralnej ewidencji kierowców w trybie teletransmisji, wykorzystywane jest standardowe oprogramowanie, dostępne na stronach internetowych producentów lub dostarczane z zestawem kryptograficznym, określone w „Wymaganiach sprzętu i oprogramowania” stanowiącym Załącznik Nr 1 do Umowy,
2. na Portalu Internetowym CEPiK dostępny jest przykładowy zestaw instalacyjny (zawierający instalator oprogramowania standardowego, komponenty darmowego oprogramowania standardowego, instrukcje instalacji i podręczniki użytkownika), zwany dalej: „zestawem MWADR”, umożliwiający przekazywanie danych określonych w §2 do centralnej ewidencji kierowców, w trybie teletransmisji, za pośrednictwem aplikacji MWADR udostępnionej na Portalu Internetowym CEPiK.

§ 4.

Minister SW zobowiązuje się do:

1. udostępnienia Marszałkowi danych dotyczących aktualizacji zestawu MWADR w każdym przypadku wprowadzenia przez Ministra SW zmian do tej aplikacji,
2. usuwania ujawnionych i zgłoszonych przez Marszałka błędów w udostępnianej aplikacji MWADR,
3. wygenerowania certyfikatu kryptograficznego umożliwiającego Marszałkowi eksploatację aplikacji MWADR,
4. realizacji zobowiązań Centrum Certyfikacji i Generacji Kluczy wynikających z „Polityki certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną” opublikowanej na portalu www.cepik.gov.pl.

§ 5.

W celu realizacji Umowy Marszałek zobowiązuje się do:

- 1) zapewnienia we własnym zakresie niezbędnego sprzętu określonego w „Wymaganiach sprzętu i oprogramowania” stanowiącym Załącznik Nr 1 do Umowy,
- 2) zapewnienia łącza internetowego w swojej siedzibie, o parametrach określonych w Załączniku Nr 1 do Umowy,
- 3) przeprowadzenia we własnym zakresie instalacji zestawu MWADR,
- 4) korzystania z aplikacji MWADR tylko w pomieszczeniach, o których mowa w pkt 7 lit. b,
- 5) prowadzenia ewidencji użytkowania wydanych certyfikatów, w sposób umożliwiający, na żądanie Gestora Systemu Informacyjnego Centralnej Ewidencji Pojazdów i Kierowców (SI CEPiK) lub innego podmiotu uprawnionego na mocy prawa, jednoznaczne i niezaprzeczalne wskazanie osoby wprowadzającej dane do SI CEPiK,
- 6) przestrzegania zasad uregulowanych w obowiązującej wersji „Polityki certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną”,
- 7) przed przystąpieniem do realizacji postanowień Umowy zapewnienia rozwiązań techniczno-organizacyjnych i proceduralnych w szczególności:
 - a) zabezpieczających odpowiednią ochronę nośników kryptograficznych i haseł umożliwiających dostęp do SI CEPiK i zapewniających niezaprzeczalność przekazywanych danych oraz zabezpieczających przed możliwością ich wykorzystania przez nieuprawnioną osobę/system/urządzenie,
 - b) zapewniających odpowiedni poziom ochrony fizycznej sprzętu i pomieszczeń, w których dane będą wprowadzane do SI CEPiK, zabezpieczający przed dostępem do nich osób nieuprawnionych oraz przed ewentualną ich kradzieżą zgodnie ze „Specyfikacją ochrony fizycznej sprzętu i pomieszczeń” stanowiącą Załącznik Nr 2 do Umowy,
- 8) Marszałek ponosi odpowiedzialność za prawidłowość i zgodność ze stanem faktycznym danych, o których mowa w § 2, przekazywanych do SI CEPiK,
- 9) na żądanie Ministra SW Marszałek zobowiązany jest do udostępnienia niezbędnych dokumentów oraz złożenia wyjaśnień dotyczących danych wprowadzonych przez niego do SI CEPiK,
- 10) przekazania Ministrowi SW danych dotyczących podmiotów prowadzących kursy ADR na obszarze pozostającym w gestii Marszałka, w celu umożliwienia Ministrowi SW utworzenia słownika, zawierającego dane o podmiotach, wykorzystywanego w aplikacji MWADR,

- 11)** Przekazanie danych o których mowa w pkt. 10, w zakresie obejmującym nazwę i adres podmiotu prowadzącego kursy ADR, numer REGON, NIP, klasy uprawnień, datę wpisania do rejestru podmiotów prowadzących kursy lub wydanej decyzji o zakazie prowadzenia przez podmiot kursów, nastąpiło do dnia 15 grudnia 2011. Przekazanie danych dotyczących podmiotów, które wpisano do rejestru podmiotów prowadzących kursy po podpisaniu Umowy nastąpi w terminie 7 dni od daty dokonania wpisu,
- 12)** W każdym przypadku wystąpienia jakichkolwiek zmian, skutkujących koniecznością wprowadzenia nowych danych, dotyczących danego Ośrodka ADR lub zakończenia jego działalności, Marszałek zobowiązuje się do przekazywania tych danych, w terminie 7 dni od daty wystąpienia okoliczności stanowiącej podstawę zmiany,
- 13)** Przekazywanie danych o których mowa w pkt.10-12 będzie następowało w formie elektronicznej, zgodnie ze wzorem stanowiącym załącznik nr 3, drogą mailową na adres wskazany w § 10.

§ 6.

Marszałek oświadcza, że sprzęt i oprogramowanie, o których mowa w § 5 pkt 1, spełniają wymagania, określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 7.

Przed przystąpieniem do realizacji postanowień Umowy Minister SW na podstawie złożonego przez Marszałka wniosku wygeneruje certyfikaty na mikroprocesorowych kartach kryptograficznych, zwanych dalej certyfikatami, umożliwiające dostęp do SI CEPiK.

§ 8.

1. Pomiędzy komunikacyjną stacją dostępową Marszałka, a warstwą centralną SI CEPiK będą wykorzystane mechanizmy zabezpieczeń transmisji danych, wykorzystujące obustronne uwierzytelnienie, przy użyciu kryptografii z kluczem prywatnym i publicznym.
2. Jakakolwiek zmiana danych stanowiących podstawę wydania Marszałkowi przez Ministra SW certyfikatów będzie wymuszała pisemne powiadomienie Ministra SW i może spowodować konieczność wymiany przydzielonych Marszałkowi certyfikatów, służących do jego uwierzytelnienia.

§ 9.

Każda ze Stron ponosi odpowiedzialność za naruszenie przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), a w szczególności za udostępnienie danych osobom nieupoważnionym, zabranie danych przez osobę nieuprawnioną oraz przetwarzanie danych osobowych z naruszeniem ustawy, w zakresie w jakim przyczyniła się do ich naruszenia.

§ 10.

1. Do bezpośrednich kontaktów przy realizacji zadań wynikających z Umowy, w tym do wymiany danych o ośrodkach ADR, Strony wyznaczają swoich przedstawicieli:

- 1) ze strony Ministra SW – Ewelina Kosecka tel: 22/6028210
mail: Ewelina.Kosecka@msw.gov.pl
- 2) ze strony Województwa –Tel, mail.....
.....

2. Zmiana powyższych danych nie wymaga zmiany Umowy, a jedynie pisemnego powiadomienia.

§ 11.

Strony Umowy, każda we własnym zakresie ponoszą koszty związane z jej realizacją.

§ 12.

Wszelkie zmiany postanowień Umowy wymagają formy pisemnej pod rygorem nieważności.

§ 13

1. Integralną część Umowy stanowią następujące załączniki:

- 1) Załącznik Nr 1 – „Wymagania sprzętu i oprogramowania”,
- 2) Załącznik Nr 2 – „Specyfikacja ochrony fizycznej sprzętu i pomieszczeń”,
- 3) Załącznik Nr 3 – Szablon spisu Ośrodków ADR podległych danemu Marszałkowi w wersji elektronicznej.

2. Zmiana treści Załączników nie wymaga zmiany Umowy, a jedynie pisemnego powiadomienia oraz przekazania ich nowych wersji.

§ 14.

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

2. Umowę Strony zawierają na czas nieokreślony.

§ 15.

Umowa wchodzi w życie z dniem podpisania.

MINISTER SPRAW WEWNĘTRZNYCH

ZARZĄD WOJEWÓDZTWA
MAZOWIECKIEGO

.....

.....

WYMAGANIA SPRZĘTU I OPROGRAMOWANIA

W celu poprawnego działania aplikacji stanowiska komputerowe powinny spełniać poniższe wymagania sprzętowe. Jest to minimalna konfiguracja stacji roboczej Użytkownika.

1. Minimalna konfiguracja sprzętu komputerowego:

- komputer z dostępem do Internetu;
- procesor min. 1GHz;
- pamięć RAM min 512MB;
- dysk twardy HDD z min. 500MB wolnego miejsca
- min. 1 wolny port USB 1.1 lub 2.0;
- system operacyjny: Windows XP z Service Pack 2 (lub wyższym) lub Windows Vista z Service Pack 1 (lub wyższym), Windows 7.
- łącze internetowe powinno mieć minimalną przepustowość 512 kb/s w obie strony i możliwością nawiązywania połączeń z serwerem www.cepik.gov.pl poprzez porty 443 i 444.

2. Czytnik i karta kryptograficzna - Zestaw kryptograficzny wymagania:

Czytnik kart kryptograficznych:

- zgodny z PC/SC,
- sterowniki umożliwiające poprawną pracę czytnika w środowisku wybranego systemu operacyjnego.

Karta kryptograficzna:

- 32kB pamięci EPROM na certyfikaty, klucze kryptograficzne oraz kody PIN,
- operacje na kluczach asymetrycznych RSA o długości do 1024 bitów,
- algorytmy symetryczne DES, Triple-DES,
- funkcja skrótu SHA-1,
- zgodność z czytnikami PC/SC,
- zgodność ze standardami: ISO 7816-3, 7816-4, 7816-5, 7816-6, 7816-8,
- zgodność ze standardem PKCS#11,
- certyfikacja do poziomu ITSEC E3 High, zgodnie z wymogami Ustawy o Podpisie Elektronicznym,
- oprogramowanie umożliwiające zarządzanie kartą kryptograficzną, w szczególności wygenerowanie pary kluczy na karcie i stworzenie CSR-a w formacie PKCS#10.

3. Oprogramowanie standardowe:

- Przeglądarka internetowa - Firefox – Mozilla Foundation – www.mozilla-europe.org
- Java Runtime Environment – Sun Microsystems, Inc <http://www.java.com>
- Moduł do zarządzania kartą dostarczany przez producenta karty
- Sterowniki czytnika kart dostarczany przez producenta urządzenia

SPECYFIKACJA OCHRONY FIZYCZNEJ SPRZĘTU I POMIESZCZEŃ

Poziom ochrony fizycznej sprzętu i pomieszczeń, w których będą przetwarzane dane SI CEPiK, powinien być dostosowany do wymogów ustawy o ochronie danych osobowych, a w szczególności:

- a)** pomieszczenia, w których zlokalizowane są stacje robocze przeznaczone do współpracy z SI CEPiK, wyposażone m.in. w czytniki mikroprocesorowych kart kryptograficznych i drukarki oraz gdzie przetwarzane i przechowywane są informacje pobrane z bazy danych CEPiK (zwane dalej Pomieszczeniami), nie mogą być pomieszczeniami przechodnimi;
- b)** należy zapewnić kontrolę dostępu do Pomieszczeń poprzez automatyczne systemy kontroli dostępu (urządzenia kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony) lub poprzez wdrożenie metod organizacyjno-proceduralnych;
- c)** Pomieszczenia powinny być zlokalizowane w miejscach nie stwarzających zagrożenia ich zatopienia lub zalania;
- d)** Pomieszczenia, w których mają znajdować się stacje komputerowe powinny być wyposażone w drzwi o zwiększonej odporności na włamanie;
- e)** otwory okienne Pomieszczeń zlokalizowanych poniżej pierwszego piętra winny być okratowane lub zabezpieczone w inny równoważny sposób;
- f)** sprzęt informatyczny (komputery i urządzenia sieciowe) musi być zabezpieczony przed utratą danych na skutek zaniku napięcia zasilającego;
- g)** karty kryptograficzne służące do nawiązywania szyfrowanego połączenia TLS, dokumenty i nośniki informacji zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym, np. w metalowej szafie;
- h)** wdrożyć ewidencję użycia kart kryptograficznych;
- i)** do likwidacji wydruków roboczych powinno się stosować niszcarki dokumentów.

Odpowiedzialność za narażenie bezpieczeństwa danych osobowych ponosi osoba, która była zalogowana w czasie, gdy trwała wymiana komunikatów z SI CEPiK. Personalną odpowiedzialność ustala się na podstawie prowadzonej w jednostce ewidencji wykorzystania mikroprocesorowych kart kryptograficznych uprawniających do dostępu do SI CEPiK.