

REGULAMIN KORZYSTANIA Z SYSTEMU TELEINFORMATYCZNEGO (SYSTEM S46)

wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa

Rozdział I: Postanowienia ogólne i definicje

§1. Umocowanie prawne

1. Niniejszy regulamin (dalej: „Regulamin”) określa zasady i warunki korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „Ustawa”), zwanego dalej „Systemem S46”.
2. Administratorem Systemu S46 jest minister właściwy do spraw informatyzacji (dalej: „Minister”), który zapewnia jego utrzymanie, rozwój oraz bezpieczeństwo.
3. System S46 służy realizacji zadań i obowiązków określonych w Ustawie, w szczególności w zakresie wymiany informacji o incydentach, zagrożeniach i podatnościach oraz rejestracji podmiotów kluczowych i ważnych w wykazie, o którym mowa w art. 7 ust. 1 Ustawy.
4. System S46 służy również do dokonywania zgłoszeń naruszeń ochrony danych osobowych, o których mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przez podmioty kluczowe lub podmioty ważne.

§2. Definicje

1. Osoba Użytkująca – osoba fizyczna upoważniona przez Podmiot Użytkujący do technicznej obsługi Systemu S46 w jego imieniu.
2. Podmiot Użytkujący – podmiot wymieniony w art. 4 Ustawy, m.in. podmiot kluczowy, podmiot ważny, organ właściwy do spraw cyberbezpieczeństwa, zespół CSIRT, którym Minister udostępnił dostęp do Systemu S46 lub inny podmiot na podstawie odrębnych przepisów za zgodą Ministra.
3. S46 Cyber Hub – aplikacja wchodząca w skład Systemu S46 wspierająca współpracę w ramach krajowego systemu cyberbezpieczeństwa w zakresie art. 46 ust. 1 Ustawy.
4. S46 Wykaz KSC – aplikacja wchodząca w skład Systemu S46, w której prowadzony jest Wykaz Podmiotów kluczowych i Podmiotów ważnych, o którym mowa w Art. 7 Ustawy.
5. MFA (Multi-Factor Authentication) – wieloskładnikowe uwierzytelnianie użytkownika wymagane przy logowaniu do Systemu S46.

Rozdział II: Funkcjonalności Systemu S46

§3. Zakres usług

Zgodnie z art. 46 ust. 1 Ustawy, System S46 zapewnia funkcjonalności umożliwiające:

1. W ramach aplikacji S46 Cyber Hub:
 - a) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;

- b) wymianę informacji, ostrzeżeń i zaleceń, o których mowa w art. 8h ust. 1 Ustawy, przez podmioty krajowego systemu cyberbezpieczeństwa;
 - c) przekazywanie organom właściwym informacji o wynikach audytów;
 - d) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
 - e) zgłaszanie i obsługę incydentów;
 - f) przekazywanie do CSIRT informacji o cyberzagrożeniach, wynikach szacowania ryzyka, podatnościach, potencjalnych zdarzeniach dla cyberbezpieczeństwa i wykorzystywanych technologiach;
 - g) szacowanie ryzyka na poziomie krajowym;
 - h) ostrzeganie o cyberzagrożeniach;
 - i) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;
 - j) dokonywanie zgłoszenia naruszenia ochrony danych osobowych przez podmioty kluczowe lub podmioty ważne;
 - k) wymianę informacji o aktach ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1 Ustawy;
 - l) realizację zadań CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Urzędu Ochrony Danych Osobowych wynikających z Ustawy.
2. W ramach aplikacji S46 Wykaz KSC - obsługę Wykazu Podmiotów Kluczowych i Podmiotów Ważnych, w tym składanie wniosków o wpis, uzupełnienie wpisu, aktualizację danych lub wykreślenie, o którym mowa w art. 46 ust. 1a Ustawy.

Rozdział III: Zasady dostępu i bezpieczeństwa

§4. Uzyskiwanie dostępu

1. Warunkiem uzyskania dostępu jest spełnianie wymogów uznania za podmiot, o którym mowa w art. 4. Ustawy, lub bycie podmiotem zobowiązanym do korzystania z systemu na podstawie odrębnych przepisów za zgodą Ministra.
2. Aktywacja konta w Systemie S46 dla podmiotu wpisanego do Wykazu następuje niezwłocznie, nie później niż w terminie 7 dni roboczych od dnia dokonania poprawnego wpisu lub aktualizacji danych w Wykazie.
3. Podmiot Użytkujący wyznacza Osoby Użytkujące i zapewnia ich odpowiednie umocowanie do działania w systemie.

§5. Bezpieczeństwo użytkownika

1. Dostęp do Systemu S46 realizowany jest za pośrednictwem przeglądarki internetowej przy wykorzystaniu bezpiecznego protokołu komunikacyjnego.
2. Obowiązkowe jest stosowanie MFA zgodnie z wytycznymi technicznymi udostępnionymi przez Ministra.
3. Osoba Użytkująca jest zobowiązana do zachowania poufności danych dostępowych. Udostępnianie konta osobom trzecim jest zabronione.

Rozdział IV: Prawa i obowiązki stron

§6. Obowiązki Podmiotu Użytkującego

1. Korzystanie z Systemu S46 wyłącznie w celach określonych w Ustawie i Regulaminie.
2. Niezwłoczna aktualizacja danych osób upoważnionych (Osób Użytkujących).
3. Przestrzeganie zasad cyberhigieny, w tym dbałość o bezpieczeństwo urządzeń końcowych, z których następuje logowanie.
4. Niezwłoczne zgłaszanie Administratorowi wszelkich błędów w działaniu Systemu lub podejrzeń naruszenia bezpieczeństwa (incydentów bezpieczeństwa Systemu S46).

§7. Odpowiedzialność Administratora

1. Minister dokłada wszelkich starań, aby System S46 działał w trybie ciągłym (24/7).
2. Administrator zastrzega sobie prawo do przerw technicznych w celu konserwacji lub aktualizacji systemu, o których użytkownicy będą informowani z wyprzedzeniem (chyba że charakter awarii wymaga natychmiastowej interwencji).
3. Administrator nie ponosi odpowiedzialności za treść informacji wprowadzanych do systemu przez Podmioty Użytkujące.

Rozdział V: Przetwarzanie danych osobowych (RODO)

§8. Ochrona danych osobowych

1. Administratorem danych osobowych przetwarzanych w celu obsługi kont użytkowników w Systemie S46 jest Minister właściwy do spraw informatyzacji.
2. Administratorem danych osobowych przetwarzanych w związku ze zgłaszaniem naruszeń ochrony danych osobowych za pomocą Systemu S46 jest Prezes Urzędu Ochrony Danych Osobowych.
3. W związku z porozumieniem zawartym pomiędzy Ministrem Cyfryzacji a Prezesem Urzędu Ochrony Danych Osobowych, w sprawie zasad współpracy przy zgłaszaniu naruszeń ochrony danych osobowych przy wykorzystaniu Systemu S46, Minister Cyfryzacji oraz Prezes UODO działają jako współadministratorzy. Podział obowiązków pomiędzy współadministratorami jest następujący:
 - 1) każdy ze współadministratorów jest zobowiązany do samodzielnego wypełniania obowiązków informacyjnych, o których mowa w art. 13 i art. 14 rozporządzenia 2016/679;
 - 2) każdy ze współadministratorów jest zobowiązany do samodzielnej realizacji

praw podmiotowych wskazanych w art. 15–22 rozporządzenia 2016/679 w stosunku do osób, których dane osobowe są przetwarzane;

- 3) każdy ze współadministratorów prowadzi rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 rozporządzenia 2016/679;
 - 4) każdy ze współadministratorów we własnym zakresie zobowiązany jest bez zbędnej zwłoki do samodzielnego wypełniania obowiązków wynikających z art. 33 oraz art. 34 rozporządzenia 2016/679.
4. Klauzule informacyjne dotyczące przetwarzania danych osobowych stanowią załączniki do niniejszego Regulaminu i są dostępne w Systemie S46.

Rozdział VI: Postanowienia końcowe

§9. Zmiany Regulaminu

1. Minister ma prawo do zmiany niniejszego Regulaminu. Zmiany wchodzi w życie w terminie wskazanym przez Administratora, nie wcześniej niż 7 dni od dnia udostępnienia nowej treści Regulaminu w Systemie S46.
2. Kontynuacja korzystania z Systemu S46 po wejściu w życie zmian wymaga akceptacji nowej treści Regulaminu Osobę Użytkującą.

§10. Wejście w życie

Niniejszy regulamin wchodzi w życie z dniem **13 kwietnia 2026 r.** i zastępuje dotychczasowe zasady korzystania z systemu.

Załącznik nr 1 do Regulaminu korzystania z systemu teleinformatycznego (System S46)

KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE S46

Niniejsza klauzula stanowi realizację obowiązku informacyjnego, o którym mowa w art. 13 i 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). System S46 przetwarza dane w dwóch obszarach: administracyjnym (obsługa kont) oraz funkcjonalnym (transmisja zgłoszeń do organów).

CZĘŚĆ I: Zarządzanie dostępem i obsługa Systemu S46

Dotyczy: Osób Użytkujących (użytkowników systemu)

1. Administrator Danych Administratorem danych osobowych Osób Użytkujących jest Minister właściwy do spraw informatyzacji (obecnie Minister Cyfryzacji), ul. Królewska 27, 00-060 Warszawa.

- Kontakt: sekretariat.dc@cyfra.gov.pl
- Inspektor Ochrony Danych (IOD): iod.mc@cyfra.gov.pl

2. Cele i podstawy prawne przetwarzania Dane przetwarzane są w celu:

1. Zapewnienia dostępu do Systemu S46: utworzenia konta, uwierzytelnienia (MFA) oraz technicznej obsługi Systemu.
2. Realizacji zadań ustawowych: prowadzenia Wykazu KSC oraz wymiany informacji o incydentach i zagrożeniach.
3. Komunikacji: informowania o szkoleniach, rekomendacjach Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zmianach w systemie.

Podstawa prawna: Art. 6 ust. 1 lit. c RODO (obowiązek prawny) w związku z art. 7, art. 8h, art. 39, art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa (KSC).

3. Okres przechowywania danych:

Dane przetwarzane są przez okres posiadania aktywnego konta w Systemie S46. Po dezaktywacji konta, dane są przechowywane przez okres 5 lat, zgodnie z wymogami art. 7f lub art. 39 Ustawy KSC.

4. Źródło pochodzenia danych Dane (imię, nazwisko, służbowy adres e-mail, numer telefonu) pochodzą z:

1. Wpisu w Wykazie KSC dokonanego przez podmiot reprezentujący.
2. Węzła Krajowego (w przypadku logowania środkami identyfikacji elektronicznej).

5. Odbiorcy danych

1. NASK-PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy) – jako podmiot technicznie utrzymujący system na zlecenie Ministra.
2. Organy właściwe ds. cyberbezpieczeństwa i zespoły CSIRT (w zakresie niezbędnym do obsługi incydentów i w zakresie prowadzenia Wykazu Podmiotów Kluczowych i Podmiotów Ważnych) zgodnie z art 39 Ustawy.
3. Zgodnie z Art. 7g ust 2. Minister udostępnia dane, o których mowa w art. 7 ust. 2 UKSC, na wniosek, następującym Instytucjom:
 - a) Agencji Bezpieczeństwa Wewnętrznego,
 - b) Agencji Wywiadu,
 - c) dyrektorowi Rządowego Centrum Bezpieczeństwa,
 - d) organom Krajowej Administracji Skarbowej,
 - e) Najwyższej Izbie Kontroli,
 - f) Policji,
 - g) Prezesowi Urzędu Lotnictwa Cywilnego,
 - h) Prezesowi Urzędu Ochrony Danych Osobowych,
 - i) Prezesowi Urzędu Transportu Kolejowego,
 - j) Prokuraturii Generalnej Rzeczypospolitej Polskiej,
 - k) prokuratorowi,
 - l) sądom,
 - m) Służbie Kontrwywiadu Wojskowego,
 - n) Służbie Ochrony Państwa,
 - o) Służbie Wywiadu Wojskowego,

- p) Straży Granicznej,
- q) Żandarmerii Wojskowej.

CZĘŚĆ II: Moduł zgłaszania naruszeń ochrony danych osobowych

Dotyczy: Danych zawartych w formularzach kierowanych do Prezesa UODO

Administrator danych osobowych.

Administratorem Państwa danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stanisława Moniuszki 1A, 00-014 Warszawa.

Mogą się Państwo z nim kontaktować w następujący sposób:

- a. listownie: ul. Stanisława Moniuszki 1A, 00-014 Warszawa,
- b. na adres do e-Doręczeń UODO AE:PL-67085-31860-RWFHC-35,
- c. przez elektroniczną skrzynkę podawczą /UODO/SkrytkaESP,
- d. za pośrednictwem adresu e-mail: kancelaria@uodo.gov.pl,
- e. telefonicznie: (22) 531 03 00.

Inspektor ochrony danych.

Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych::

- a. pod adresem email iod@uodo.gov.pl,
- b. listownie na adres: ul. Stanisława Moniuszki 1A, 00-014 Warszawa,
- c. na adres do e-Doręczeń UODO AE:PL-67085-31860-RWFHC-35,
- d. przez elektroniczną skrzynkę podawczą /UODO/SkrytkaESP.

Cele i podstawy przetwarzania.

Państwa dane osobowe będą przetwarzane w celu przyjmowania zgłoszeń naruszeń ochrony danych osobowych, ich analizy oraz podejmowania działań przewidzianych przepisami prawa. Podstawą prawną przetwarzania jest art. 6 ust. 1 lit. c RODO (a w przypadku danych szczególnych kategorii – także art. 9 ust. 2 lit. g RODO). Przetwarzanie jest niezbędne do wykonania:

- a. obowiązku przyjmowania i ewidencjonowania przez Prezesa UODO naruszeń ochrony danych osobowych zgłaszanych na podstawie art. 33 ust. 1, 3 i 4 RODO albo art. 44 ust. 1, 4 i 5 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,
- b. podejmowania przez Prezesa UODO działań określonych w art. 58 ust. 1 i 2 RODO, art. 34 ust. 4 RODO albo art. 45 ust. 5 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,
- c. obowiązków wynikających z art. 5 ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach w zakresie postępowania z dokumentacją.

Odbiorcy danych osobowych.

Odbiorcami Państwa danych osobowych mogą być:

- a. strony i inni uczestnicy postępowań administracyjnych, jeżeli wynika to z przepisów prawa,

- b. podmioty uprawnione do doręczania korespondencji,
- c. podmioty świadczące usługi serwisowe i utrzymaniowe systemów informatycznych wykorzystywanych w UODO, działające na podstawie umowy powierzenia przetwarzania danych,
- d. właściwe miejscowo archiwum państwowe, któremu przekazywana jest dokumentacja po ekspertyzie archiwalnej.

Okres przechowywania danych.

Będziemy przechowywać Państwa dane zgodnie z przepisami o archiwizacji dokumentów i obowiązującą w UODO Instrukcją Kancelaryjną - przez okres do 10 lat od 1 stycznia roku następnego od daty, w którym zakończono czynności w sprawie. Okres ten może zostać wydłużony do 25 lat, na podstawie ekspertyzy archiwalnej przeprowadzanej przez właściwe miejscowo archiwum państwowe.

Prawa osób, których dane dotyczą.

Zgodnie z RODO przysługuje Państwu:

- a. prawo dostępu do swoich danych oraz otrzymania ich kopii – mogą Państwo uzyskać informacje, jakie dane są przetwarzane,
- b. prawo do sprostowania swoich danych - jeżeli dane osobowe są nieprawidłowe lub niekompletne,
- c. prawo do ograniczenia przetwarzania danych osobowych – w przypadkach określonych w RODO,
- d. prawo do wniesienia skargi do Prezesa UODO, jeśli uznają Państwo, że przetwarzanie danych osobowych narusza przepisy prawa.

Informacja o wymogu podania danych.

Podanie przez Państwa danych osobowych jest obowiązkiem wynikającym z przepisów prawa, a ich niepodanie może stanowić naruszenie przepisów RODO.

CZĘŚĆ III: Uprawnienia osób, których dane dotyczą

Każdej osobie, której dane są przetwarzane w Systemie S46, przysługuje prawo do:

1. Dostępu do treści swoich danych.
2. Sprostowania (poprawienia) danych – jeśli są nieprawidłowe.
3. Ograniczenia przetwarzania – w sytuacjach określonych w RODO.
4. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Zautomatyzowane podejmowanie decyzji: Państwa dane nie będą podlegały profilowaniu ani zautomatyzowanemu podejmowaniu decyzji.

Podsumowanie dla Użytkownika

Korzystanie z Systemu S46 i podanie danych w celach określonych w Ustawie KSC jest obowiązkiem ustawowym. Brak podania danych uniemożliwi utworzenie konta i realizację obowiązków w ramach krajowego systemu cyberbezpieczeństwa.

Niniejsza klauzula wchodzi w życie z dniem **13 kwietnia 2026 r.** i zastępuje dotychczasowe klauzule w Systemie S46.