



STOWARZYSZENIE INICJATYWA OBYWATELSKA

PRO CIVIUM

Niezależny nadzór nad ochroną danych osobowych

OCHRONA
DANYCH**DECYZJA INSPEKTORA OCHRONY DANYCH****Nr I/D/IOD/26/1**
z dnia 6 września 2026 r.**w sprawie zasad ochrony danych osobowych w
Systemie BazaWiedzy Pro Civium****oraz zasad współpracy Głównego Administratora Systemu z Inspektorem
Ochrony Danych**

STATUS	WERSJA	ORGAN WYDAJĄCY	OBSZAR
Obowiązuje	1.0	Inspektor Ochrony Danych	BazaWiedzy Pro Civium

Na podstawie § 21 pkt 4 i 5 Regulaminu Stowarzyszenia Inicjatywa Obywatelska Pro Civium, postanowień Zintegrowanego Systemu Zarządzania, art. 5 ust. 1 lit. c, d i f oraz ust. 2, art. 24, art. 32-34 i art. 37-39 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), a także w związku z Zarządzeniem Prezesa Zarządu nr X/Za/Pr/26/1 z dnia 30 sierpnia 2026 r. w sprawie ustanowienia funkcji Głównego Administratora Systemu BazaWiedzy Pro Civium, działając w granicach kompetencji Inspektora Ochrony Danych, wydaje się następującą decyzję:

§ 1 Cel, zakres i podstawowe pojęcia

- Decyzja określa wiążące zasady ochrony danych osobowych przy projektowaniu, wdrażaniu, utrzymaniu, rozwijaniu i korzystaniu z Systemu BazaWiedzy Pro Civium.
- Decyzję stosuje się do członków Stowarzyszenia, kadry zarządzającej, pracowników, współpracowników, wolontariuszy, praktykantów oraz innych osób, którym przyznano dostęp do Systemu lub jego zasobów.
- Administratorem danych osobowych w rozumieniu RODO jest Stowarzyszenie Inicjatywa Obywatelska Pro Civium. Określenie „Główny Administrator Systemu” oznacza funkcję organizacyjną i nie może być utożsamiane z administratorem danych.
- Ilekczo w Decyzji jest mowa o „Administratorze Systemu”, należy przez to rozumieć Głównego Administratora Systemu BazaWiedzy Pro Civium ustanowionego Zarządzeniem nr X/Za/Pr/26/1.

§ 2 Zasady ochrony danych w BazaWiedzy

- Legalność, rzetelność i przejrzystość - każdy proces przetwarzania musi mieć określony cel, podstawę prawną i czytelną informację dla osoby, której dane dotyczą.

- Minimalizacja danych - formularze, rejestry i narzędzia mogą zbierać wyłącznie dane adekwatne i niezbędne do wskazanego celu.
- Ograniczenie celu i przechowywania - danych nie wykorzystuje się do celów niezgodnych z celem pierwotnym ani nie przechowuje dłużej, niż wynika to z prawa, dokumentacji projektu lub przyjętych okresów retencji.
- Prawidłowość - dane wymagają aktualizacji, a stwierdzone nieścisłości usuwa się albo koryguje bez zbędnej zwłoki.
- Integralność i poufność - dane chroni się przed nieuprawnionym dostępem, utratą, zmianą, ujawnieniem lub zniszczeniem.
- Wiedza konieczna i najmniejsze uprawnienia - użytkownik otrzymuje wyłącznie taki dostęp, jaki jest niezbędny do jego aktualnych zadań.
- Rozliczalność - decyzje o dostępie, istotne zmiany oraz zdarzenia bezpieczeństwa muszą pozostawiać możliwości do odtworzenia ślad organizacyjny.

§ 3 Dostęp do danych i kont użytkowników

1. Dostęp do modułu zawierającego dane osobowe przyznaje się na podstawie udokumentowanej decyzji lub upoważnienia administratora danych albo osoby umocowanej do działania w jego imieniu.
2. Administrator Systemu wdraża, odwzorowuje i kontroluje zakres dostępu w Systemie, lecz nie nadaje samodzielnie upoważnień do przetwarzania danych osobowych, jeżeli nie posiada do tego odrębnego umocowania.
3. Konta są indywidualne. Zabrania się udostępniania haseł, korzystania z kont innej osoby oraz utrzymywania dostępu po ustaniu funkcji, współpracy albo potrzeby wykonywania zadań.
4. Właściciel procesu zgłasza niezwłocznie potrzebę nadania, zmiany lub odebrania dostępu. Dostęp zbędny albo budzący uzasadnione wątpliwości podlega czasowemu ograniczeniu do czasu wyjaśnienia.
5. Przegląd osób i zakresów dostępu prowadzi się nie rzadziej niż raz na kwartał oraz każdorazowo po istotnej zmianie struktury, funkcji lub zakresu zadań.

§ 4 Obowiązki Głównego Administratora Systemu

W obszarze ochrony danych Administrator Systemu:

- porównuje rzeczywiste dostępy z aktualnymi upoważnieniami i zakresem obowiązków;
- prowadzi albo współprowadzi ewidencję dostępow i wyników ich przeglądów;
- przed wdrożeniem nowego formularza lub modułu sprawdza, czy określono cel, zakres danych, odbiorców, okres przechowywania i właściwą klauzulę informacyjną;
- kieruje do IOD do zaopiniowania zmiany wpływające na zakres, sposób lub ryzyko przetwarzania danych;
- zgłasza właścicielowi procesu dane nieaktualne, nadmiarowe albo przechowywane bez widocznej potrzeby;
- dba, aby zgłoszenia błędów i zrzuty ekranu nie ujawniały danych osób trzecich ponad zakres konieczny do obsługi zgłoszenia;
- rejestruje i natychmiast przekazuje incydenty bezpieczeństwa IOD oraz Prezesowi Zarządu;



- dokumentuje wykonane działania ograniczające ryzyko oraz monitoruje zamknięcie zgłoszenia.

§ 5 Zakazy i bezpieczne posługiwanie się danymi

1. Zabrania się kopiowania danych z BazaWiedzy na prywatne dyski, prywatne konta chmurowe, prywatne skrzynki pocztowe albo do komunikatorów niezatwierdzonych do obsługi danego procesu.
2. Eksport zestawienia danych jest dopuszczalny wyłącznie wtedy, gdy wynika z zadania służbowego lub projektowego, został ograniczony do niezbędnego zakresu oraz jest przechowywany w zatwierdzonym miejscu przez niezbędny okres.
3. Nie wolno ujawniać danych osobowych w nazwach publicznie dostępnych plików, adresach odnośników, komentarzach, zgłoszeniach technicznych ani materiałach szkoleniowych, jeżeli nie jest to konieczne i prawnie uzasadnione.
4. Każdy użytkownik jest zobowiązany zabezpieczać urządzenie, blokować ekran, stosować aktualne mechanizmy uwierzytelniania i natychmiast zgłaszać utratę urządzenia, danych dostępowych albo podejrzenie przejęcia konta.

§ 6 Podział ról i granice odpowiedzialności

ROLA	ODPOWIEDZIALNOŚĆ	GRANICE
Stowarzyszenie - administrator danych	Ustala cele i sposoby przetwarzania, zatwierdza rozwiązania organizacyjne, upoważnienia i działania wymagane przepisami.	Nie przenosi swojej odpowiedzialności na IOD ani Administratora Systemu.
Inspektor Ochrony Danych	Informuje, doradza, opiniuje, monitoruje zgodność, prowadzi działania kontrolne i współpracuje z organem nadzorczym.	Działa niezależnie; nie zarządza operacyjnie Systemem i nie przejmuje decyzji administratora danych.
Główny Administrator Systemu	Kontroluje zgodność dostępów z upoważnieniami, testuje procesy, dokumentuje problemy i uruchamia właściwe osoby.	Nie jest administratorem danych, nie zastępuje IOD i nie zmienia samodzielnie klauzul ani zasad prawnych.
Właściciele procesów	Odpowiadają za cel, zakres, prawidłowość, aktualność i terminowe usuwanie danych w swoim obszarze.	Nie przekazują dostępu osobom trzecim i nie rozszerzają zakresu danych bez wymaganej decyzji lub konsultacji.

§ 7 Reagowanie na naruszenia i zdarzenia bezpieczeństwa

1. Każdy użytkownik, który stwierdzi lub podejrzewa nieuprawniony dostęp, ujawnienie, utratę, błędne skierowanie, zmianę albo niedostępność danych, powiadamia natychmiast Administratora Systemu i IOD, nie prowadząc samodzielnego postępowania wyjaśniającego.
2. Zgłoszenie otrzymuje priorytet KRYTYCZNY. Administrator Systemu odnotowuje czas, miejsce, zakres i źródło zdarzenia, zabezpiecza dostępne informacje oraz - w granicach uprawnień - rekomenduje lub wdraża czasowe ograniczenie dostępu do wadliwego modułu.

3. IOD dokonuje wstępnej oceny ryzyka i przekazuje administratorowi danych zalecenia dotyczące dalszego postępowania. Decyzję o zgłoszeniu naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz o zawiadomieniu osób, których dane dotyczą, podejmuje administrator danych zgodnie z art. 33 i 34 RODO.
4. Jeżeli naruszenie podlega zgłoszeniu organowi nadzorczemu, działania organizuje się tak, aby umożliwić zgłoszenie bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia.
5. Każde zdarzenie i sposób jego zakończenia dokumentuje się w rejestrze naruszeń lub rejestrze zdarzeń bezpieczeństwa, również wtedy, gdy po ocenie nie zachodzi obowiązek zgłoszenia do organu nadzorczego.

§ 8 Kontrola zgodności i wdrożenie

1. Administrator Systemu, właściciele procesów i osoby zarządzające modułami współpracują z IOD, udzielają informacji i przedstawiają dokumentację niezbędną do przeprowadzenia kontroli lub oceny ryzyka.
2. W terminie 30 dni od wejścia w życie Decyzji Administrator Systemu dokonuje przeglądu dostępu do modułów zawierających dane osobowe i przedstawia IOD krótką informację o wyniku oraz wykrytych niezgodnościach.
3. Nowy moduł albo istotna zmiana sposobu przetwarzania danych nie mogą zostać udostępnione produkcyjnie przed sprawdzeniem wymagań określonych w niniejszej Decyzji i uzyskaniem opinii IOD, jeżeli zmiana może wpływać na prawa lub wolności osób fizycznych.

§ 9 Postanowienia końcowe

1. Decyzja wchodzi w życie z dniem podpisania.
2. Decyzja podlega rejestracji w Repozytorium Aktów Wewnętrznych Pro Civium oraz udostępnieniu wszystkim użytkownikom BazaWiedzy.
3. Nadzór nad zgodnością stosowania Decyzji z przepisami o ochronie danych sprawuje Inspektor Ochrony Danych, a za wykonanie działań organizacyjnych i systemowych odpowiadają, w granicach swoich kompetencji, Główny Administrator Systemu oraz właściciele procesów.
4. Decyzję stosuje się łącznie z Polityką RODO, instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, Polityką Digitalizacji i Archiwizacji Dokumentacji oraz Zarządzeniem nr X/Za/Pr/26/1.

Ochrona danych w BazaWiedzy jest wspólnym obowiązkiem. Każdy dostęp musi mieć cel, właściciela, podstawę i możliwy do odtworzenia ślad.

Poznań, 6 września 2026 r.

Anna Pasierb-Wojciechowska
Inspektor Ochrony Danych Osobowych
Stowarzyszenie Inicjatywa Obywatelska Pro Civium

Anna Pasierb-Wojciechowska
podpis