

Bezpieczeństwo i ochrona danych w dataBAS

Opis techniczny dla administratora danych i inspektora ochrony danych (IOD)

System	dataBAS 2.1 — kreator aplikacji bazodanowych (PHP, MySQL/MariaDB lub SQLite)
Producent	Arnold Basiński · databas.pl
Model wdrożenia	instalacja na serwerze administratora danych (szkoła, gmina, firma) — oprogramowanie, nie usługa w chmurze
Lokalizacja danych	wyłącznie serwer i baza danych wskazane przez administratora
Dostęp producenta do danych	brak
Połączenia zewnętrzne	serwer licencji (klucz, domena, wersja programu); poczta i wtyczka WordPress — tylko jeśli zostaną włączone
Usługi zewnętrzne w interfejsie	brak (bez CDN, zewnętrznych czcionek, statystyk i reklam)

dataBAS instalujesz na własnym serwerze szkoły, gminy lub firmy. Dane uczniów, pracowników i klientów zostają u Ciebie — producent programu nie ma do nich dostępu. Poniżej opisujemy, co dokładnie dzieje się z danymi, jakie zabezpieczenia ma system i co warto ustawić po instalacji.

Gdzie są przechowywane dane

Wszystkie dane wprowadzane do dataBAS — rekordy, przesłane pliki, konta użytkowników, dziennik zmian — są zapisywane wyłącznie w bazie danych (MySQL / MariaDB albo plik SQLite) i w katalogu `uploads/` na serwerze, na którym zainstalowano program.

- dataBAS nie korzysta z chmury producenta ani z zewnętrznych usług: nie łąduje czcionek, skryptów ani statystyk z innych serwerów.
- Kody QR do logowania dwuetapowego są tworzone na Twoim serwerze.
- Wykresy i raporty są generowane na Twoim serwerze.

Jakie informacje opuszczają serwer

Są tylko trzy sytuacje, w których dataBAS łączy się z innym serwerem:

1. **Sprawdzanie licencji** — co kilka dni program wysyła do serwera licencji dataBAS: klucz licencyjny, nazwę domeny instalacji i numer wersji programu. Nie są wysyłane żadne dane z bazy ani dane użytkowników.
2. **Powiadomienia e-mail** — tylko jeśli je włączysz. Wiadomości wychodzą przez serwer poczty wskazany w ustawieniach (np. pocztę szkoły) i zawierają pola, które sam wybierzesz w szablonie.

3. **Wtyczka WordPress** — tylko jeśli ją zainstalujesz. Twoja strona WordPress pobiera dane z Twojej instalacji dataBAS przez zabezpieczone kluczem API, z tymi samymi uprawnieniami co w programie.

Kto ma dostęp do danych

- Dostęp mają tylko osoby, którym administrator założy konto. Uprawnienia ustawia się dla grup: przeglądanie, dodawanie, edycja, usuwanie i eksport — osobno dla każdej tabeli.
- Filtry wierszy pozwalają ograniczyć dane, np. wychowawca widzi tylko uczniów swojej klasy.
- Opcja „tylko własne rekordy” ogranicza użytkownika do wpisów, które sam utworzył.
- Wszystkie uprawnienia sprawdza serwer — ukrycie przycisku w interfejsie nie jest jedynym zabezpieczeniem.
- Producent dataBAS nie ma kont w Twojej instalacji ani dostępu do Twojego serwera.

Zabezpieczenia logowania

- Hasła są przechowywane wyłącznie jako skróty (funkcja `password_hash` PHP); nikt — także administrator — nie może ich odczytać.
- Logowanie dwuetapowe (2FA) z aplikacją w telefonie, z 10 jednorazowymi kodami zapasowymi. Administrator może wymagać 2FA od administratorów albo od wszystkich użytkowników.
- Blokada po 8 nieudanych próbach logowania w ciągu 15 minut z jednego adresu.
- Bezpieczne ciasteczko sesji (HttpOnly, SameSite, Secure przy HTTPS), wylogowanie po zmianie hasła lub zablokowaniu konta.

Ochrona przed atakami

- Zapytania do bazy wyłącznie w formie przygotowanej (PDO) — ochrona przed SQL injection.
- Token CSRF przy każdej zmianie danych.
- Przesyłane pliki: lista dozwolonych rozszerzeń (nigdy pliki wykonywalne), losowe nazwy, wydawanie wyłącznie po sprawdzeniu uprawnień.
- Nagłówki bezpieczeństwa przeglądarki (m.in. X-Frame-Options, X-Content-Type-Options, Referrer-Policy).
- Eksport CSV zabezpieczony przed wstrzykiwaniem formuł do Excela.

Rozliczalność: kto i co zmienił

Dziennik zmian zapisuje każde dodanie, zmianę i usunięcie rekordu: kto, kiedy, z jakiego adresu IP i jakie były wartości przed zmianą i po niej. Usunięty rekord można przywrócić. Dziennik włącza się dla całej aplikacji i dla poszczególnych tabel. Zawiera dane osobowe użytkowników (login, adres IP), dlatego dostęp do niego mają tylko administratorzy.

Dane osobowe w dziennikach technicznych

- **Dziennik zmian** — login użytkownika, adres IP, zmienione wartości. Okres przechowywania ustawia administrator (Kreator → Ustawienia: 30 dni, 90 dni, 6 miesięcy, 1, 2 lub 5 lat albo bez limitu); starsze wpisy są usuwane automatycznie raz na dobę.
- **Nieudane logowania** — adres IP i wpisany login; usuwane automatycznie po 15 minutach.

- **Wysłane powiadomienia** — adresy odbiorców i temat ostatnich 500 wiadomości (do diagnozowania poczty); starsze są usuwane automatycznie.

Rola producenta w rozumieniu RODO

W typowym wdrożeniu — program zainstalowany na serwerze szkoły lub firmy i obsługiwany przez jej pracowników — producent dataBAS nie przetwarza danych osobowych zapisanych w programie i nie ma do nich dostępu. Administratorem danych jest szkoła (firma), a dataBAS jest dla niej narzędziem, tak jak arkusz kalkulacyjny. W takim modelu umowa powierzenia przetwarzania danych z producentem zwykle nie jest potrzebna.

Umowa powierzenia będzie potrzebna, jeśli producent lub inna firma ma dostęp do danych — np. utrzymuje serwer albo pomaga przy wdrożeniu na prawdziwych danych. Ostateczną ocenę zawsze przeprowadza inspektor ochrony danych administratora.

Zalecenia po instalacji

1. Uruchom dataBAS wyłącznie przez **HTTPS**.
2. Włącz **logowanie dwuetapowe** co najmniej dla administratorów (Ustawienia → Bezpieczeństwo).
3. Nadaj użytkownikom **najmniejsze potrzebne uprawnienia** i używaj filtrów wierszy.
4. Rób **regularne kopie zapasowe** bazy danych i katalogu `uploads/`, przechowywane poza serwerem.
5. Trzymaj plik bazy SQLite **poza katalogiem publicznym** serwera (ustawienie w `config.php`).
6. Usuń plik `install.php` po instalacji i aktualizuj dataBAS do najnowszej wersji.
7. Uwzględnij dataBAS w **rejestrze czynności przetwarzania** i ustal okresy przechowywania danych.

Ten opis przedstawia techniczne działanie dataBAS. Nie stanowi porady prawnej — ocenę zgodności z RODO w konkretnej organizacji przeprowadza jej administrator danych i inspektor ochrony danych.

Do uzupełnienia przez administratora danych

Adres serwera / dostawca hostingu	
Lokalizacja serwera (kraj)	
Cel przetwarzania w dataBAS	
Kategorie osób i danych	
Osoby z kontem administratora	
Kopie zapasowe (gdzie, jak często)	
Okres przechowywania danych	
Logowanie dwuetapowe włączone dla	