ŚRODKI TECHNICZNE I ORGANIZACYJNE

RespoTime

Załącznik bezpieczeństwa do umowy powierzenia przetwarzania danych osobowych

Obszar	Opis środka / status
Usługodawca / podmiot przetwarzający	Market Reklamy Dominika Bieleń
Adres	ul. Jana Pawła II 16, 39-460 Nowa Dęba
Dane rejestrowe	NIP: 8141685116, REGON: 360477826
Kontakt	kontakt@respotime.pl
Wersja dokumentu	1.0
Data dokumentu	2026-06-02
System	RespoTime - system rezerwacji online dla różnych branż

Dokument opisuje środki techniczne i organizacyjne stosowane lub planowane w systemie RespoTime w celu ochrony danych osobowych przetwarzanych w ramach usługi. Dokument ma charakter informacyjny i dowodowy dla klientów korzystających z RespoTime jako administratorów danych.

Dokument nie jest certyfikatem zgodności ani gwarancją braku incydentu. Ma służyć wykazaniu, że RespoTime stosuje rozsądne, adekwatne do etapu MVP i rozwijane środki ochrony danych.

1. Cel dokumentu

Celem dokumentu jest opisanie środków technicznych i organizacyjnych, które mają zapewnić poufność, integralność, dostępność i odporność systemu RespoTime oraz danych przetwarzanych w systemie.

Dokument może być udostępniany klientom RespoTime jako załącznik do umowy powierzenia przetwarzania danych osobowych, odpowiedź na pytanie o gwarancje bezpieczeństwa albo element dokumentacji RODO.

2. Zakres systemu RespoTime

RespoTime jest systemem SaaS do obsługi rezerwacji i zapytań rezerwacyjnych dla różnych branż, w szczególności usług lokalnych, obiektów, atrakcji, noclegów, konsultacji, salonów, gabinetów, łowisk, warsztatów, edukacji, sportu i rekreacji.

System może przetwarzać dane klientów końcowych firm korzystających z RespoTime, dane użytkowników panelu oraz dane techniczne niezbędne do działania usługi.

- W aktualnym MVP funkcje AI, odczytywanie screenów i automatyczne przetwarzanie wiadomości przez zewnętrzne modele AI są wyłączone.
- Publiczny embed kalendarza pokazuje dostępność i zajętość terminów, bez danych osobowych klientów końcowych.
- Dane klientów końcowych są widoczne wyłącznie w panelu uprawnionego administratora/firmy.

3. Role w przetwarzaniu danych

Klient RespoTime, np. firma, obiekt, salon, gabinet, łowisko lub inny usługodawca, jest co do zasady administratorem danych swoich klientów końcowych.

RespoTime działa jako podmiot przetwarzający w zakresie, w jakim udostępnia system i technicznie przetwarza dane w imieniu klienta.

Market Reklamy Dominika Bieleń jest administratorem danych w zakresie danych własnych klientów B2B, kont użytkowników, kontaktu handlowego, rozliczeń i obsługi relacji z klientem RespoTime.

4. Podstawa przyjętego modelu bezpieczeństwa

Model bezpieczeństwa opiera się na zasadzie adekwatności środków do ryzyka, charakteru, zakresu i celów przetwarzania. Środki są rozwijane wraz z rozwojem systemu i wzrostem skali przetwarzania.

W praktyce RespoTime koncentruje się na ograniczaniu dostępu do danych, separacji danych firm, bezpiecznej konfiguracji produkcyjnej, kontroli dostępu do serwera i bazy oraz minimalizacji danych widocznych publicznie.

5. Środki organizacyjne

Obszar	Opis środka / status
Zakres odpowiedzialności	Określono role administratora i podmiotu przetwarzającego w umowie powierzenia danych. Klient odpowiada za własną podstawę prawną przetwarzania danych i obowiązek informacyjny wobec klientów końcowych.
Dokumentacja	Przygotowano umowę powierzenia danych, regulamin świadczenia usług RespoTime oraz roadmapę bezpieczeństwa i zgodności MVP.
Dostęp do danych	Dostęp do danych produkcyjnych powinien być ograniczony do osób, które faktycznie muszą go posiadać w celu utrzymania systemu, obsługi awarii lub wsparcia klienta.
Poufność	Osoby posiadające dostęp do danych powinny być zobowiązane do poufności. Dostęp nie powinien być udostępniany osobom nieupoważnionym.
Minimalizacja	Publiczne widoki nie powinny pokazywać danych osobowych

	klientów końcowych. Dane powinny być przetwarzane tylko w zakresie niezbędnym do obsługi rezerwacji i działania systemu.
Zmiany w systemie	Zmiany w kodzie powinny być wykonywane ostrożnie, z kopią pliku, kontrolą składni, czyszczeniem cache i testem działania po wdrożeniu.

6. Środki techniczne - aplikacja

Obszar	Opis środka / status
Tryb produkcyjny	Aplikacja działa w trybie APP_ENV=production.
Wyłączony debug	APP_DEBUG=false, co ogranicza ryzyko ujawnienia technicznych informacji w błędach publicznych.
HTTPS	System działa pod adresem HTTPS. Sesje i ciasteczka są skonfigurowane pod bezpieczne połączenie.
Szyfrowanie sesji	SESSION_ENCRYPT=true. Dane sesyjne są szyfrowane przez aplikację.
Secure cookie	SESSION_SECURE_COOKIE=true. Ciasteczka sesyjne są wysyłane wyłącznie przez HTTPS.
HTTP only	SESSION_HTTP_ONLY=true. Ciasteczko sesyjne nie powinno być dostępne dla JavaScript.
SameSite	SESSION_SAME_SITE=lax, co ogranicza część ryzyk związanych z cross-site request contexts.
Rate limit logowania	Logowanie ma limit błędnych prób: 5 błędnych prób na 60 sekund dla kombinacji e-mail + IP.
Hashowanie haseł	Hasła użytkowników są hashowane przez mechanizmy Laravel i nie są przechowywane w postaci jawnej.
Autoryzacja tenantowa	Dane rezerwacji, zapytań, stanowisk i statystyk są ograniczane przez fishery_id / identyfikator firmy lub publiczny slug aktywnego podmiotu.
Publiczny embed	Publiczny embed pobiera tylko pola potrzebne do pokazania dostępności: id, identyfikator firmy/obiektu, identyfikator zasobu, status i daty. Nie pobiera danych klienta końcowego.

7. Środki techniczne - baza danych

Obszar	Opis środka / status
Lokalny dostęp	Aplikacja łączy się z bazą danych przez 127.0.0.1.
Brak publicznej ekspozycji portu	MariaDB słucha na 127.0.0.1:3306, a nie na publicznym adresie 0.0.0.0.
Użytkownik bazy	Aplikacja korzysta z użytkownika respotime_user@localhost.
Zakres uprawnień	Użytkownik aplikacji ma uprawnienia do bazy respotime, bez globalnych uprawnień ALL ON *.*.
Separacja danych	Kluczowe tabele biznesowe zawierają fishery_id / identyfikator podmiotu i są filtrowane na poziomie aplikacji.
Klucze obce i indeksy	Tabele rezerwacji, zapytań, stanowisk i czasowych wyłączeń mają klucze obce i indeksy wspierające integralność i kontrolę dostępu.
Dane produkcyjne	Dostęp do danych produkcyjnych powinien być ograniczony do potrzeb utrzymaniowych, diagnostycznych i wsparciowych.

8. Środki techniczne - serwer i konfiguracja

Obszar	Opis środka / status
Serwer aplikacji	Aplikacja działa na serwerze VPS z systemem Ubuntu.
Nginx	Root aplikacji jest ustawiony na katalog public, co ogranicza dostęp do plików aplikacji spoza katalogu publicznego.

Blokada plików ukrytych	Konfiguracja Nginx blokuje dostęp do plików ukrytych, z wyjątkiem katalogu .well-known potrzebnego dla certyfikatów.
Certyfikat SSL	Domena systemu korzysta z certyfikatu SSL obsługiwanego przez Certbot.
Plik .env	Uprawnienia do pliku .env zostały ograniczone do 640. Plik nie powinien być publicznie dostępny ani udostępniany osobom nieuprawnionym.
Backupy kodu	Robocze pliki .bak zostały przeniesione poza katalog kontrolerów aplikacji do storage/app/code-backups/controllers.
Sekrety	Hasła, klucze i tokeny nie powinny być przesyłane w wiadomościach, dokumentach ani publicznych repozytoriach.

9. Minimalizacja danych publicznych

Jedną z kluczowych zasad RespoTime jest rozdzielenie panelu właściciela firmy od publicznego widoku dostępności.

- W panelu właściciela mogą być widoczne dane klienta potrzebne do obsługi rezerwacji.
- W publicznym embedzie widoczna jest wyłącznie informacja o dostępności lub zajętości terminu.
- Publiczny embed nie powinien ujawniać imion, nazwisk, telefonów, e-maili, liczby osób, notatek ani statusów płatności.

10. Obsługa branż regulowanych i danych szczególnych kategorii

RespoTime jest systemem uniwersalnym dla różnych branż. Niektóre branże mogą przetwarzać dane o większym ryzyku, w tym dane dotyczące zdrowia, konsultacji specjalistycznych, usług okołomedycznych lub innych informacji wrażliwych.

Klient korzystający z RespoTime w branży regulowanej albo przetwarzający szczególne kategorie danych jest zobowiązany samodzielnie ocenić podstawę prawną, zakres danych, obowiązki informacyjne, wymogi branżowe oraz potrzebę dodatkowych zabezpieczeń.

- RespoTime nie powinien być używany do przechowywania danych szczególnych kategorii, jeżeli klient nie ma właściwej podstawy prawnej i nie uzgodni dodatkowych wymogów bezpieczeństwa.
- W notatkach i wiadomościach nie należy wpisywać danych nadmiarowych ani danych wrażliwych, jeżeli nie są niezbędne do obsługi rezerwacji.

11. Backup, dostępność i odtwarzanie

System powinien posiadać kopie zapasowe adekwatne do skali i ryzyka przetwarzania. Szczegóły częstotliwości, lokalizacji i czasu przechowywania kopii mogą być opisane w osobnej procedurze backupu.

Obszar	Opis środka / status
Cel backupu	Ochrona przed utratą danych w wyniku awarii, błędu technicznego lub incydentu.
Zakres backupu	Baza danych, pliki aplikacji, konfiguracje niezbędne do odtworzenia usługi, z wyłączeniem niepotrzebnych danych roboczych.
Dostęp do backupu	Dostęp do kopii zapasowych powinny mieć wyłącznie osoby upoważnione.
Odtwarzanie	Możliwość odtworzenia danych powinna być testowana okresowo lub po istotnych zmianach infrastruktury.
Rozwój procedury	Szczegółowa procedura backupu i odtwarzania powinna zostać dopisana jako osobny dokument operacyjny.

12. Reagowanie na incydenty

W przypadku podejrzenia naruszenia ochrony danych RespoTime powinien niezwłocznie przeprowadzić analizę techniczną, zabezpieczyć logi, ograniczyć skutki incydentu i poinformować właściwego administratora danych zgodnie z umową powierzenia.

- Przykłady incydentów: nieuprawniony dostęp do panelu, wyciek danych, błędna konfiguracja publicznego widoku, utrata danych, kompromitacja konta użytkownika, ujawnienie sekretów lub błędna wysyłka danych.
- Administrator danych odpowiada za ocenę, czy incydent wymaga zgłoszenia do UODO lub zawiadomienia osób, których dane dotyczą, chyba że przepisy prawa stanowią inaczej.
- Procedura incydentowa powinna być rozwinięta jako osobny dokument operacyjny.

13. Audyt i informacje dla klientów

Zamiast udostępniać klientom dostęp do serwera lub kodu, RespoTime może przekazywać dokumentację bezpieczeństwa, opis środków, listę podprocesorów oraz odpowiedzi na uzasadnione pytania audytowe.

Audyt klienta powinien odbywać się w sposób, który nie narusza bezpieczeństwa systemu, danych innych klientów, tajemnicy przedsiębiorstwa ani ciągłości działania usługi.

14. Aktualny status zabezpieczeń

Obszar	Opis środka / status
APP_ENV	production - potwierdzone
APP_DEBUG	false - potwierdzone
APP_URL	https://kalendarz.respotime.pl - potwierdzone dla aktualnej instancji
SESSION_ENCRYPT	true - potwierdzone
SESSION_SECURE_COOKIE	true - potwierdzone
DB_HOST	127.0.0.1 - potwierdzone
MariaDB bind-address	127.0.0.1 - potwierdzone
Użytkownik bazy	respotime_user@localhost - potwierdzone
Uprawnienia bazy	ALL PRIVILEGES tylko na bazie respotime.* - potwierdzone
Publiczny embed	ograniczony do pól technicznych dostępności - wykonane
Rate limit logowania	wdrożony - wykonane
Backupy kodu .bak	przeniesione poza katalog kontrolerów - wykonane

15. Ograniczenia i działania planowane

Poniższe elementy są rekomendowane do dalszego rozwoju systemu i dokumentacji. Nie oznaczają one braku obecnych zabezpieczeń, lecz wskazują kierunek profesjonalizacji usługi wraz ze wzrostem liczby klientów.

- Polityka prywatności RespoTime dla klientów B2B i użytkowników panelu.
- Lista podprocesorów RespoTime.
- Procedura naruszeń ochrony danych.
- Procedura backupu i odtwarzania.
- Dodatkowe logi audytowe operacji w panelu.
- Formalna tabela akceptacji dokumentów prawnych przez firmy.
- Opcjonalne 2FA dla użytkowników panelu.
- Dalsza analiza nagłówków bezpieczeństwa Nginx z uwzględnieniem embeda iframe.

16. Podsumowanie

Na dzień sporządzenia dokumentu RespoTime posiada podstawowy, realnie wdrożony zestaw zabezpieczeń technicznych i organizacyjnych adekwatny do etapu MVP oraz przetwarzania danych w systemie rezerwacyjnym.

Zabezpieczenia obejmują między innymi separację danych klientów systemu, lokalny dostęp do bazy, brak publicznej ekspozycji portu bazy danych, tryb produkcyjny aplikacji, wyłączony debug, szyfrowane sesje, bezpieczne ciasteczka, rate limit logowania oraz minimalizację danych widocznych publicznie.

Dokument powinien być aktualizowany po istotnych zmianach systemu, infrastruktury, listy podprocesorów, zakresu danych albo funkcji wysokiego ryzyka.