

Polityka Bezpieczeństwa Systemu UpRes

1. Synkom sp. z o.o. stosuje odpowiednie środki techniczne oraz organizacyjne gwarantujące ochronę danych osobowych Użytkowników.
2. Dane Użytkowników przetwarzane są zgodnie z obowiązującymi przepisami prawa.
3. Dostęp do rady wierzycieli oraz zgromadzenia wierzycieli przydzielany jest wyłącznie osobom uprawnionym do zasiadania w nich. Każdy użytkownik otrzymuje login oraz hasło pozwalające na dostęp do systemu.
4. Hasła przechowywane są w bazie danych w postaci zaszyfrowanej, uniemożliwiającej odczytanie ich osobom trzecim
5. Po dokonaniu rejestracji użytkownika (założeniu konta) i pierwszym jego zalogowaniu, podczas którego akceptuje on regulamin serwisu, podane w systemie dane będą wykorzystywane przez Spółkę m.in. do:
 - a) Przesyłania Użytkownikowi na podany adres e-mail linku z informacjami na temat przyszłych posiedzeń rady oraz zgromadzenia, a także podsumowań odbytych posiedzeń
 - b) Kontaktowania się Administratora z Użytkownikiem w sprawach związanych z obsługą systemu;8.
 - c) Wystawiania Faktur VAT.
6. Użytkownik poprzez rejestrację (utworzenie konta) i pierwszym zalogowaniu w systemie, podczas którego akceptuje on regulamin serwisu, wyraża zgodę na przetwarzanie podanego przez niego adresu e-mail w celach informacyjnych, w tym w szczególności zgodę na otrzymywanie komunikatów lub informacji Administratora lub innych podmiotów (za wiedzą i wyraźnym przyzwoleniem Administratora). Cofnięcie takiej zgody przez Użytkownika jest równoznaczne z żądaniem usunięcia konta Użytkownika wraz z całą jego zawartością. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają wyłącznie pracownicy firmy Synkom sp. z o.o., którzy uzyskali pisemne upoważnienie wydane przez Doradcę Restrukturyzacyjnego
7. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwa się niezwłocznie po ustaniu ich użyteczności
8. Dostęp do serwisu możliwy jest wyłącznie za pośrednictwem szyfrowanego protokołu https.
9. Transmisja audio video realizowana za pośrednictwem modułu obsługi rad wierzycieli jest szyfrowana po stronie systemu.
10. Wszystkie wprowadzane do serwisu dane są walidowane i filtrowane po stronie front-endu i back-endu
11. Środowisko działania aplikacji jest stale monitorowane pod kątem aktualności stosowanego oprogramowania i zapobiegania nieuprawnionemu dostępowi.
12. Dane każdego postępowania przechowywane są w osobnej bazie danych niezależnej od innych postępowań.