Przedsiębiorstwo Wielobranżowe FISKAS SERVICE
Wojciech Kańczurzewski
62-300 Września ul. Żwirki i Wigury 25

Września, 2018-05-25

ZMIANY W SEKAFI ZWIĄZANE Z RODO

Nasza firma dołożyła wszelkich starań aby sprostać wymaganiom, które postawiło przed nami Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 z dnia 27 kwietnia 2016 dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Odbyliśmy szereg konsultacji w tym zakresie, których celem było ustalenie ostatecznych zmian, które należałoby wprowadzić w systemach informatycznych dotyczących branży fiskalnej. W wyniku tych konsultacji zostały podjęte poniższe ustalenia.

Podmioty zajmujące się Produkcją Importem oraz Dystrybucją i Serwisem Urządzeń Fiskalnych, podlegają przede wszystkim Ustawom i Rozporządzeniom w tym zakresie. Ustawodawca (Ministerstwo Finansów) zobowiązuje i nakłada na te podmioty obowiązki przetwarzania tych danych przez cały cykl życia urządzeń fiskalnych, od momentu fiskalizacji, poprzez przeglądy, naprawy i inne czynności aż do odczytu zawartości pamięci fiskalnej.

Po dokonaniu odczytu zawartości pamięci fiskalnej obowiązuje nas Ustawa o Rachunkowości, która nakazuje przechowywanie tych dokumentów przez okres kolejnych pełnych 5 lat.

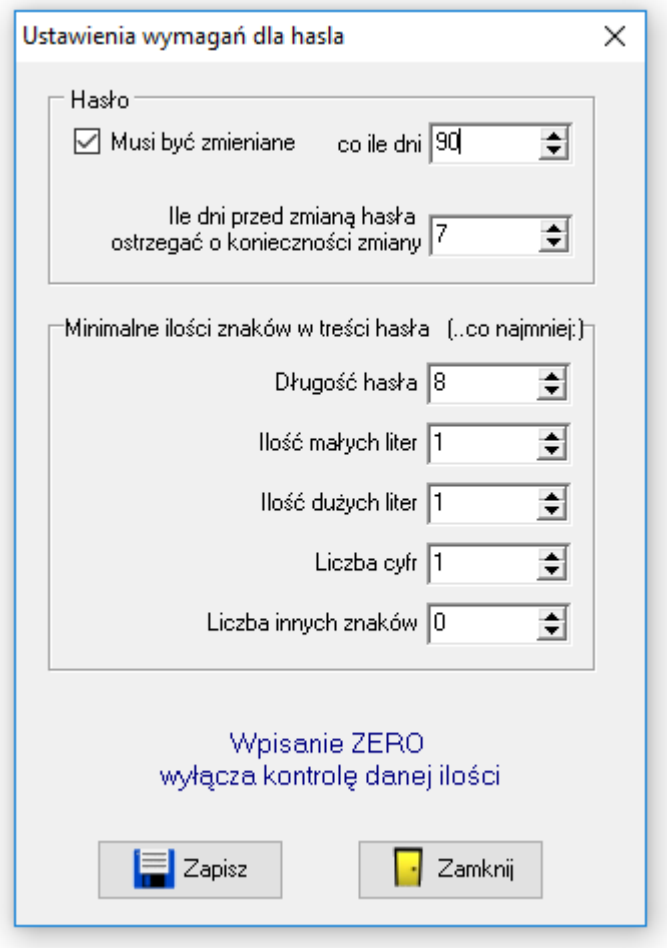
Przykład:
Byli pracownicy firmy zajmującej się serwisowaniem urządzeń fiskalnych, będą znajdować się w ewidencji na dokumentach (na protokołach) oraz w książkach serwisowych przez cały cykl życia urządzenia fiskalnego oraz pięć pełnych lat od ich odczytu.

Poza powyższymi zasadami – które są nadrzędne – wszystkie pozostałe obowiązki i zapisy RODO dotyczące bezpieczeństwa, integralności, informacji oraz czasu przetwarzania danych pozostają w mocy.

W związku z tym w Sekafi zostało wprowadzonych wiele zmian.

Dla naszych klientów opracowaliśmy dokument „**Zalecenia bezpieczeństwa Systemu SEKAFI3 SQL**”, w którym został umieszczony szereg uwag oraz informacji dotyczących bezpieczeństwa przetwarzania danych.

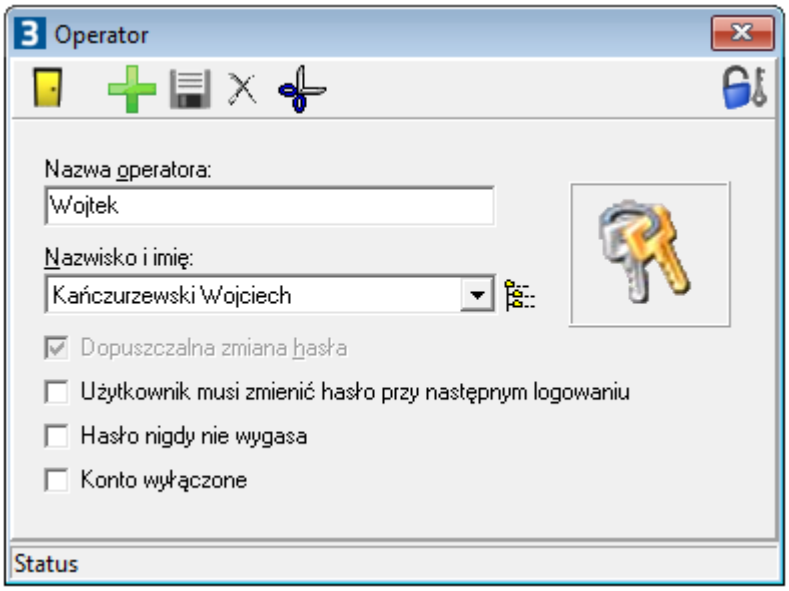
1. Nowy formularz parametryzacji wymogów haseł
   Administracja -> Uprawnienia -> Wymagania dla hasła operatora



W poprzednich wersjach program dawał pełną dowolność co do stosowania siły hasła oraz nie wymuszał częstotliwości dokonywania jego zmiany. Począwszy od teraz to ASI (Administrator Systemów Informatycznych) może ustawić takie zasady haseł, jakie zostały ustalone i zapisane w polityce bezpieczeństwa danej firmy. Użytkownik programu otrzymuje pełną możliwość ustalenia wszystkich możliwych parametrów związanych z polityką haseł, np. co ile czasu hasło ma być zmienione oraz ile dni przed terminem ma pojawiać się informacja o zbliżającym się czasie wygaśnięcia dotychczasowego hasła.

W pozostałych parametrach można określić siłę hasła, na co składa się: długość oraz zawartość hasła. Użytkownik sam dokona zmiany na nowe własne hasło, ale o takich parametrach jakie są wymagane przez politykę bezpieczeństwa.

2. Zmodyfikowany formularz kartoteki Operatora
   Administracja -> Uprawnienia -> Operatorzy

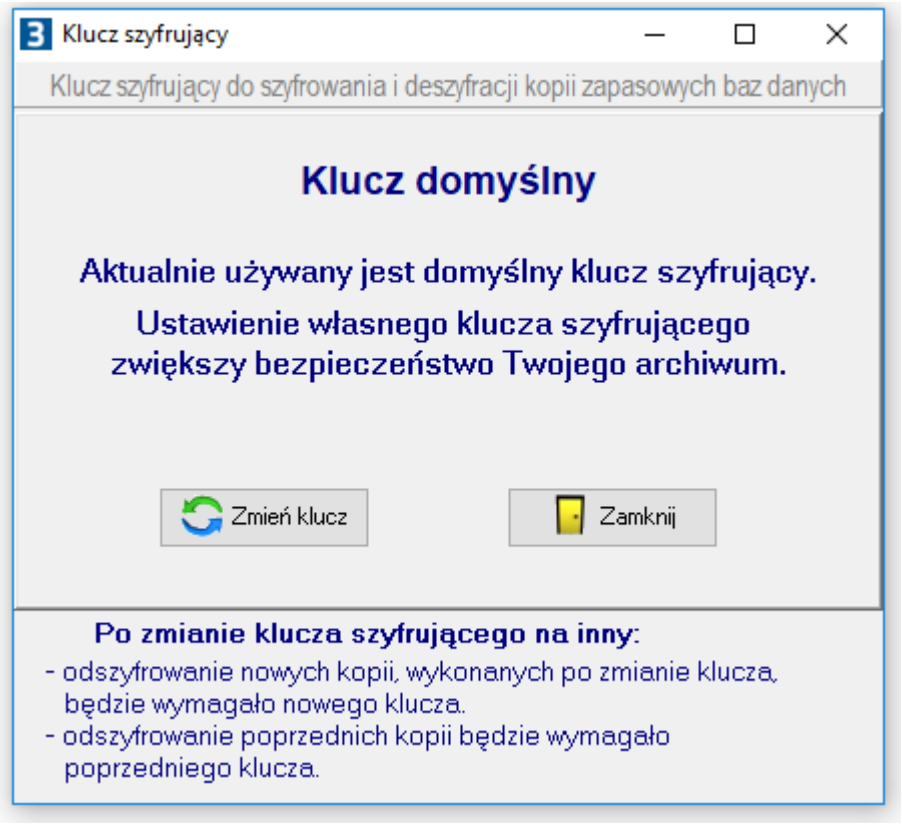


W oknie ustawień konta operatora, dotychczasowy parametr „Dopuszczalna zmiana hasła” został wyłączony z obsługi, gdyż od teraz każdy ma prawo do zmiany hasła, a dotychczasowe ustawienie tego parametru mogło to operatorowi uniemożliwić. Stary parametr pozostał na formularzu, ale jest nieaktywny – dostępny jest on teraz tylko do podglądu, aby sprawdzić wcześniejsze ustawienie (za jakiś czas zostanie usunięty z formularza).

Zostały dodane trzy nowe parametry, które pozwolą elastycznie zdefiniować ustawienia dla Pracowników obsługujących system:

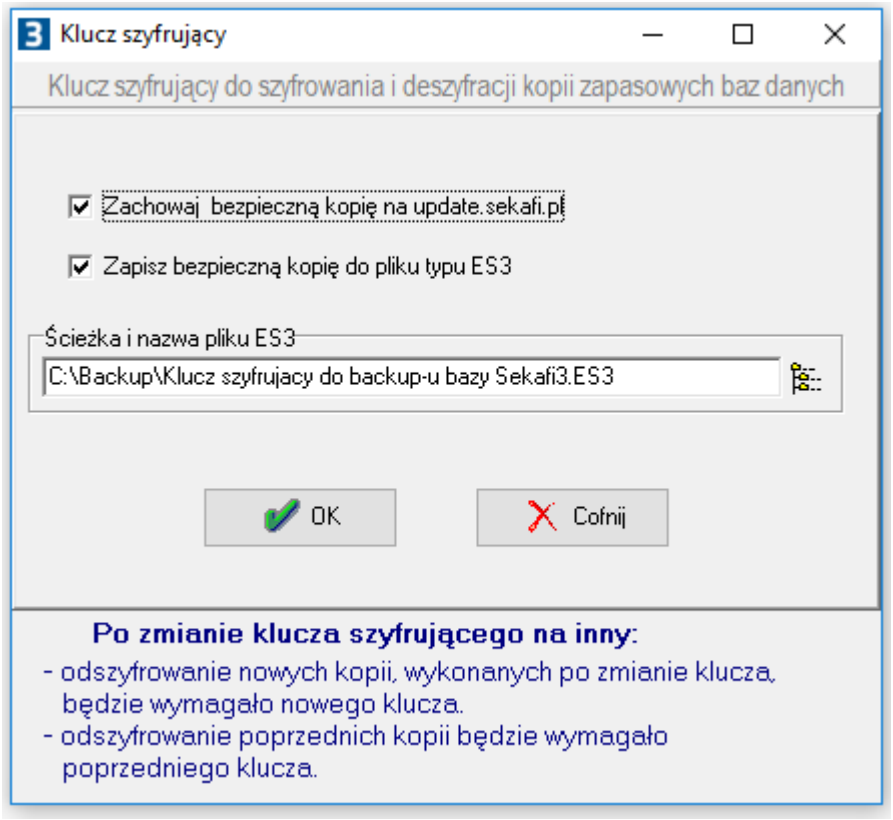
- „*Użytkownik musi zmienić hasło przy następnym logowaniu*” - zaznaczenie tego parametru wymusi jednorazową zmianę hasła na nowe (inne) przy następnym zalogowaniu prze tego użytkownika. Zmiana hasła spowoduje odznaczenie tego parametru i wyznaczenie nowego terminu zmiany, zgodnie z ustawionym harmonogramem.
- „*Hasło nigdy nie wygasa*” - zaznaczenie tego parametru jest przewidziane dla kont administratorów, na które logowanie następuje incydentalnie raz na kilka miesięcy. Wówczas przy zachowaniu wysokich standardów bezpieczeństwa ten parametr może być włączony. Nie zaleca się jednak ustawiania tego parametru dla operatorów regularnie obsługujących system.
- „*Konto wyłączone*” - opcję stosuje się w przypadku gdy dany operator utracił prawo do logowania w systemie. Aby uniknąć utraty dostępu do administracyjnych funkcji systemu, przypadkowe zaznaczenie tego parametru dla konta administratora nie spowoduje wyłączenia konta Administrator.

3. Nowa funkcjonalność: Szyfrowanie kopii bezpieczeństwa
   Administracja -> Baza danych -> Klucz Szyfrujący



Aby zapewnić maksymalną ochronę wykonywanych kopii bezpieczeństwa, została wprowadzona możliwość szyfrowania wykonanych kopii. Od teraz każdy z operatorów będzie mógł wykonać kopię bezpieczeństwa bez obawy, że archiwum może być użyte przez osoby nieuprawnione. Tak przygotowana kopia może znajdować się na stacji roboczej i jest bezpieczna, gdyż aby uzyskać dostęp do zawartych w niej danych, wymagane jest podanie klucza szyfrującego.

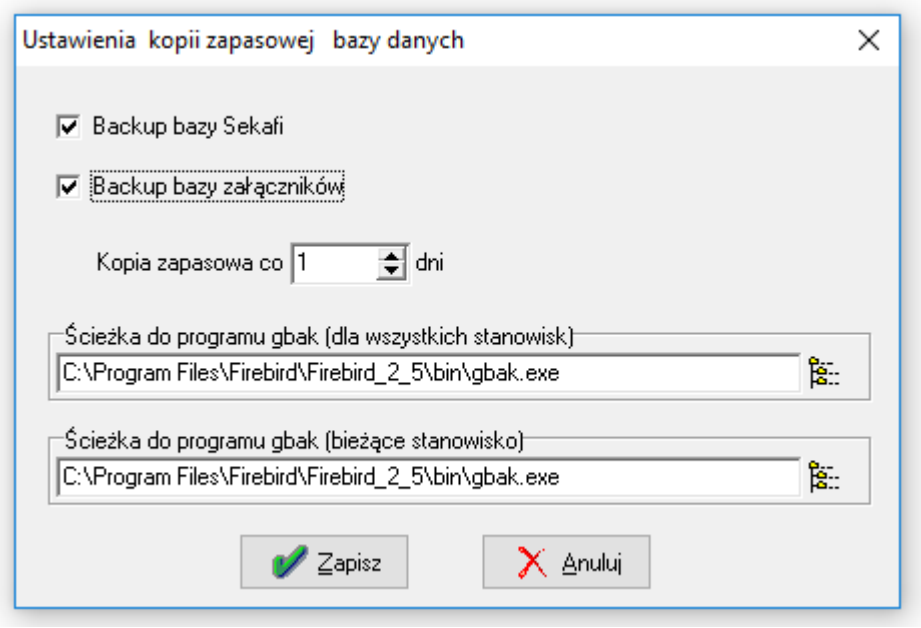
Dodatkowym mechanizmem zapewniającym ochronę jest możliwość umieszczania wykonywanych zaszyfrowanych kopii zapasowych w niepublicznej chmurze Sekafi Cloud. Na naszych serwerach została uruchomiona usługa cloud.sekafi.pl dedykowana dla użytkowników programu Sekafi, w której można przechowywać wykonywane kopie bezpieczeństwa. W przypadku utraty lub uszkodzenia komputera, na którym były przechowywane lokalne kopie zapasowe, użytkownik korzystający z cloud.sekafi.pl, będzie mógł zawsze przywrócić kopię swojej bazy, co bez przechowywania kopii w dodatkowym zewnętrznym miejscu byłoby niemożliwe.



Procedura nadania oraz zmiany klucza szyfrującego powinna odbyć się w przemyślany i rozważny sposób. Nierozważne ustawienie tego parametru i niezapamiętanie użytego klucza, a także nie zachowanie pliku z kluczem ES3, może skutecznie odebrać dostęp do wykonanych kopii archiwalnych. Zostały stworzone dwie metody, które pomogą zachować klucz szyfrujący użytkownika w bezpiecznej postaci:

- Zapisanie bezpiecznej kopii klucza do pliku o rozszerzeniu ES3 – w takim pliku klucz jest zaszyfrowany i niewidoczny dla osób nieuprawnionych, ale pozostawienie dostępu do tego pliku dla osób niepowołanych umożliwi im odszyfrowanie kopii bezpieczeństwa.
  Opis wykorzystania pliku ES3: Administrator (ASI) wprowadza bezpieczny klucz szyfrujący, który przechowywany jest w poufnym oraz bezpiecznym miejscu. Wygenerowany plik ES3 przekazuje wyznaczonemu pracownikowi, mającemu prawo do wykonania odtworzenia danych z kopii zapasowej, w celu przeprowadzenia testowego wypakowania i sprawdzenia poprawności kopii bezpieczeństwa.
- Przesłanie kopii klucza w postaci zaszyfrowanej przez bezpieczne połączenie (SSL) na serwer update.sekafi.pl. Klucz przesłany do update.sekafi.pl będzie mógł być odzyskany w sytuacji krytycznej jeśli zawiodą wszystkie inne metody, np. jeśli doszło do zaszyfrowania całego dysku wirusem, pożaru lub innej katastrofy, to zawsze można odzyskać klucz z bezpiecznej strefy update.sekafi.pl. Wysyłka do tej strefy wymaga zaznaczenia pola „Zachowaj bezpieczną kopie na update.sekafi.pl”, które domyślnie jest niezaznaczone – chcemy, aby była to świadoma decyzja użytkownika.

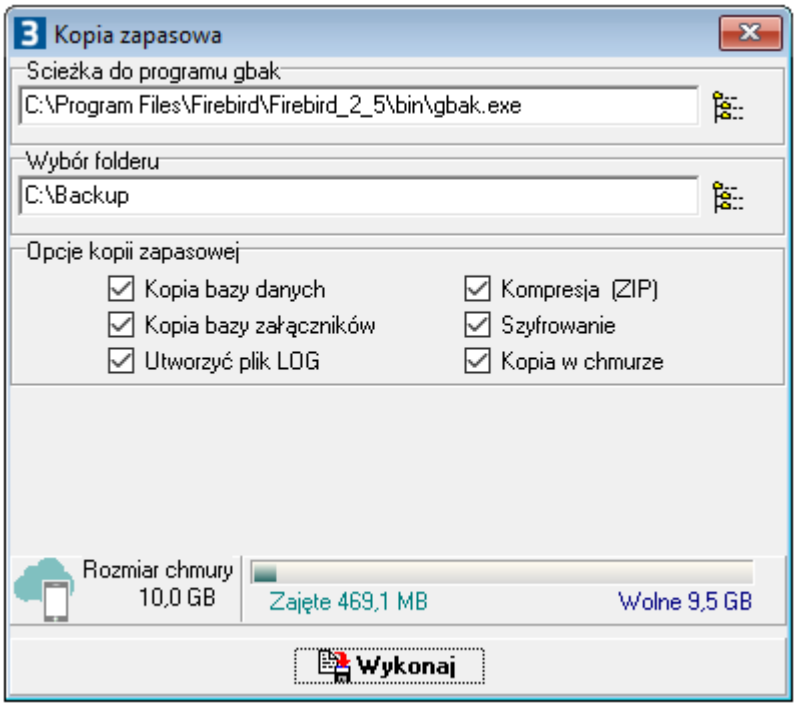
4. Nowy formularz ustawień automatycznych kopii zapasowych bazy danych
   Administracja -> Baza danych -> Ustawienia kopii zapasowej



W nowej wersji Sekafi, przy zamykaniu programu pojawia się okno z zapytaniem o chęć wykonania kopii zapasowej bazy danych. Tak wykonana kopia jest przesyłana na indywidualne konto użytkownika w prywatnej bezpiecznej chmurze cloud.sekafi.pl. Na powyższym formularzu można zdefiniować co ile dni program ma przypominać o wykonaniu kopii bezpieczeństwa, a także można wyłączyć wykonywanie okresowych kopii bazy dla wybranej bazy danych.

Należy zwrócić szczególną uwagę na to, aby na stacjach roboczych była zainstalowana właściwa wersja klienta bazy danych Firebird dla środowiska stacji roboczej. Jeśli na stacji 64-bitowej zostanie zainstalowany klient w wersji 32-bitowej lub jeśli została wskazana inna ścieżka podczas instalacji, to ścieżka do aplikacji wykonującej kopie na powyższym formularzu będzie inna niż domyślna. Instalacja na stanowisku klienta bazy danych w wersji: „Minimalna instalacja klienta” uniemożliwia wykonywanie kopii na takiej stacji. Jeśli na takim stanowisku powinna być możliwość wykonywana kopii i np. przesyłana jej do strefy cloud.sekafi.pl, wymagane jest, aby przeinstalować klienta do wersji umożliwiającej wykonanie tego procesu.

5. Zmodyfikowany formularz wykonywania kopii zapasowej bazy danych
Administracja -> Baza danych -> Kopia zapasowa

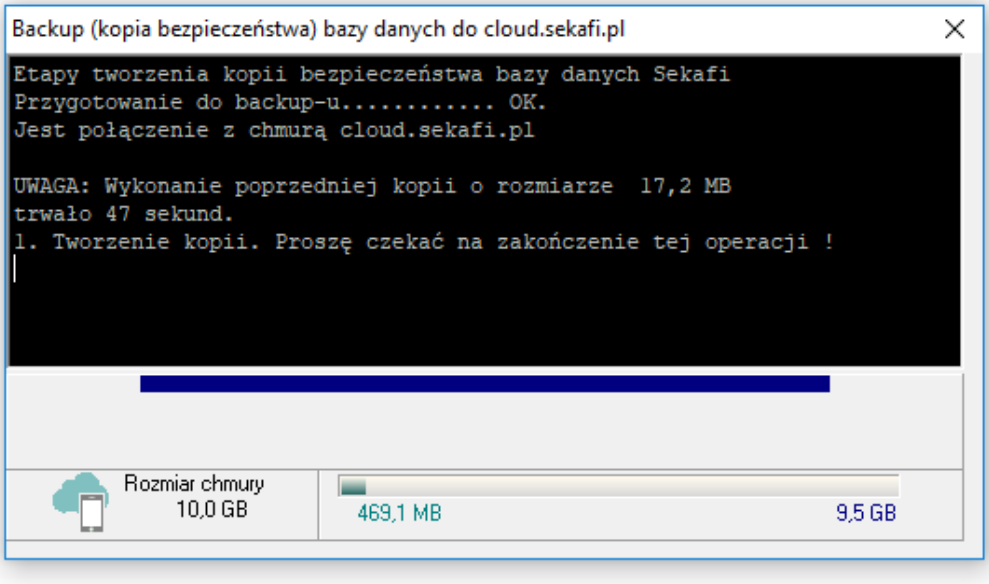


W oknie umożliwiającym wykonywanie kopii zapasowej bazy danych zostały dodane nowe funkcjonalności:
– tworzenie pliku LOG,
– szyfrowanie kopii.

Po zaznaczeniu pola „tworzenie pliku LOG”, oprócz tworzonej kopii bazy do wskazanego folderu zostanie zapisany plik LOG z wszystkimi informacji dotyczącymi poszczególnych etapów tworzenia pliku archiwum. Dzięki temu w dowolnym momencie użytkownik będzie mógł przejrzeć plik LOG i sprawdzić status wykonania kopii. Jeśli archiwum zawiera jakieś uszkodzone fragmenty, będzie można to zweryfikować na podstawie analizy tego pliku.

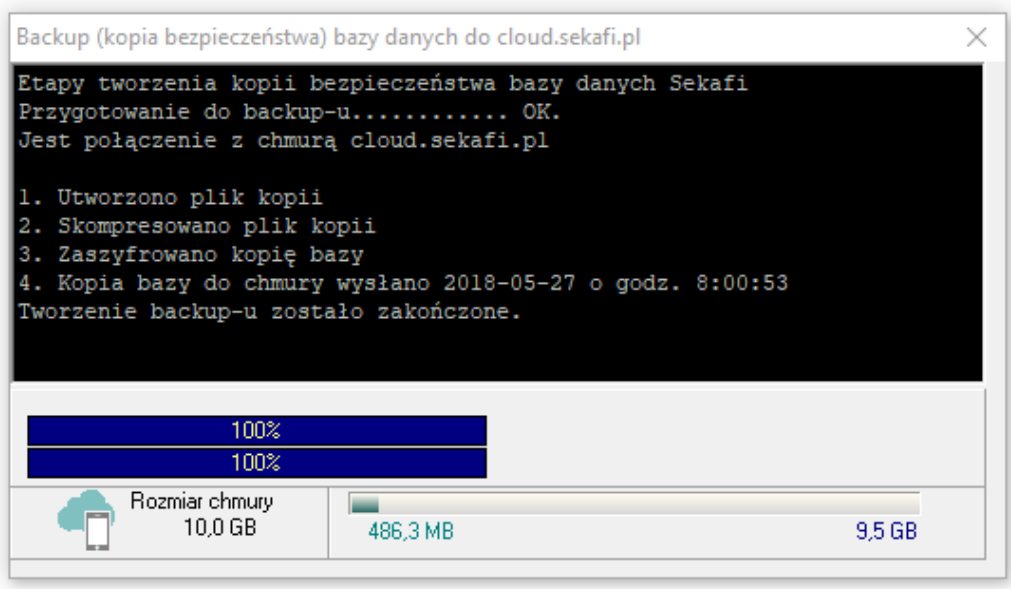
Po zaznaczeniu pola „Szyfrowanie”, wykonana kopia zapasowa zostanie zaszyfrowana do bezpiecznej postaci. Wypakowanie danych z utworzonej w ten sposób kopii zapasowej będzie możliwe tylko po podaniu klucza szyfrującego, który jest bardziej szczegółowo opisany w punkcie 3 powyżej.

6. Nowy formularz tworzenia kopii zapasowej do cloud.sekafi.pl
   Aplikacja -> Backup do cloud.sekafi.pl



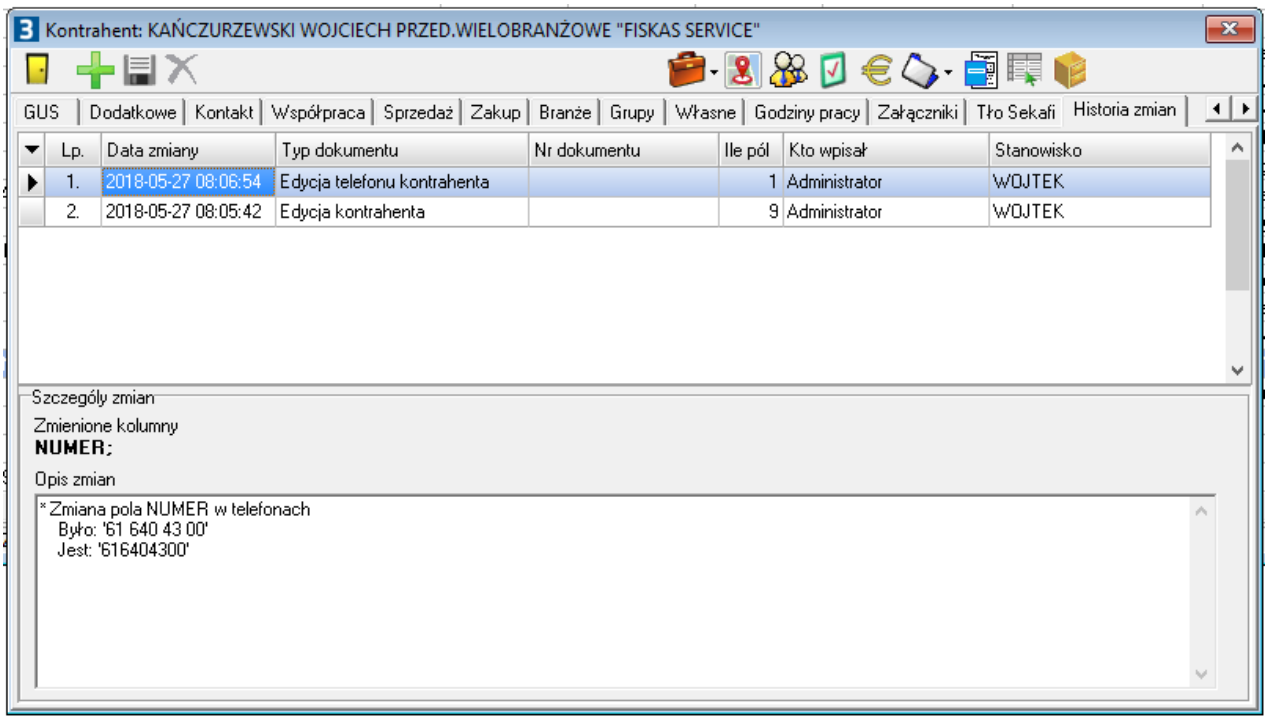
Tak jak zostało już wspomniane w punkcie 4. powyżej, została udostępniona nowa funkcjonalność przypominania o wykonaniu kopii zapasowej co określony czas podczas zamykania programu. Wykonywane w ten sposób kopie zapasowe są wysyłane na indywidualne konto użytkownika w bezpiecznej prywatnej chmurze cloud.sekafi.pl.

Oprócz automatycznego przypominania o wykonaniu kopii podczas zamykania programu, w dowolnym momencie można łatwo wywołać okno wykonania kopii do cloud.sekafi.pl. W tym celu wystarczy przejść do menu Aplikacja -> Backup do cloud.sekafi.pl. Po otwarciu okna, program sprawdza połączenie z chmurą, a następnie rozpoczyna wykonywanie kopii zapasowej.



Po wykonaniu kopii jest ona zawsze pakowana do archiwum zip, a następnie zaszyfrowana i wysłana do cloud.sekafi.pl. W dowolnym momencie można przejrzeć swoje pliki kopii znajdujące się w chmurze po zalogowaniu w Sekafi na konto Administratora i przejściu do menu Administracja -> Baza danych -> Cloud.sekafi.pl -> Pliki w chmurze.

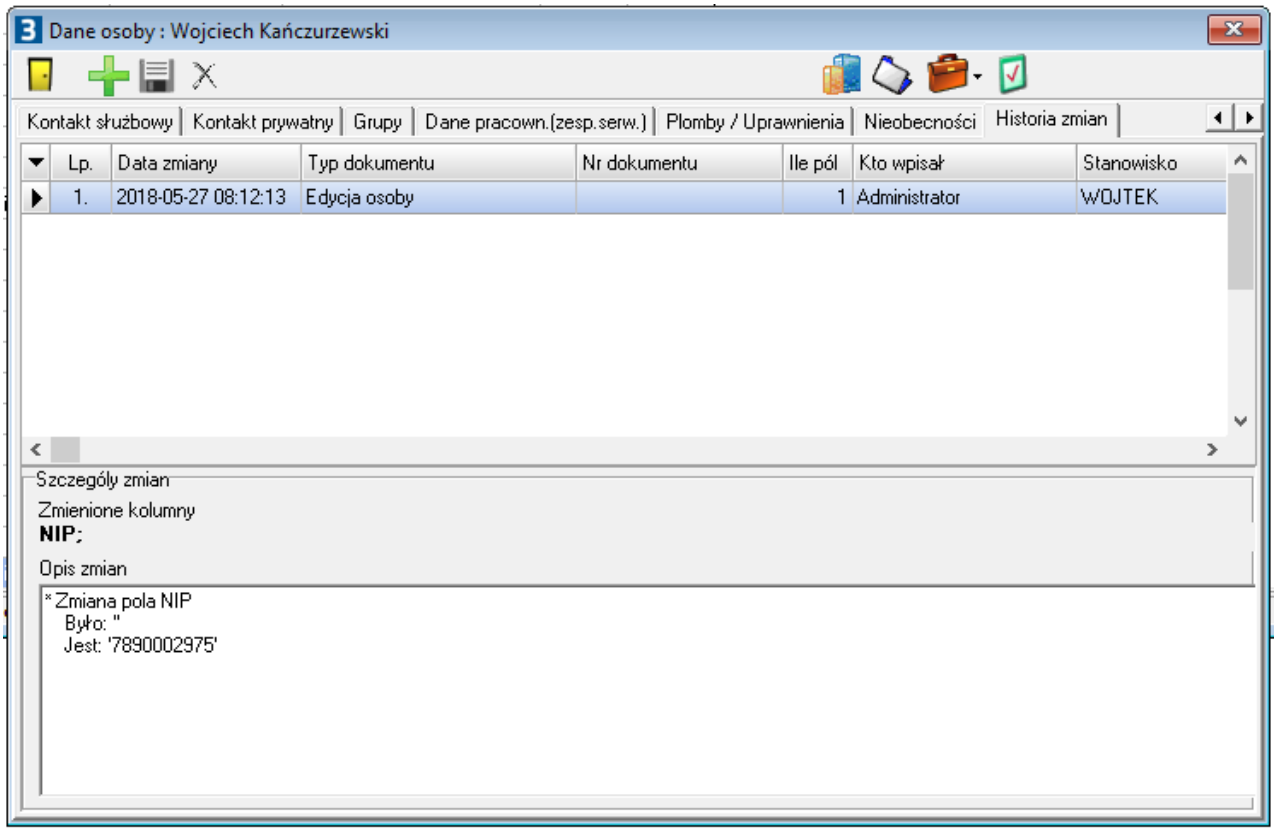
7. Nowa zakładka na kartotece Kontrahentów
   Kartoteki -> Kontrahenci -> Historia zmian



W kartotece kontrahenta pojawiła się nowa zakładka „Historia zmian”. Będą się tutaj pojawiać wszystkie modyfikacje wykonane na danych wybranego kontrahenta. Na liście wszystkie informacje wyświetlane będą od najnowszych do najstarszych, dzięki czemu na samej górze będą widoczne najnowsze wpisy.

Informacje te pozwalają w łatwy sposób sprawdzić kto i kiedy dokonywał zmian na danych konkretnego kontrahenta, z jakiego miejsca były wykonane te zmiany oraz jakie konkretnie dane zostały zmodyfikowane.

8. Nowa zakładka na kartotece Osób
   Kartoteki -> Osoby -> Historia zmian

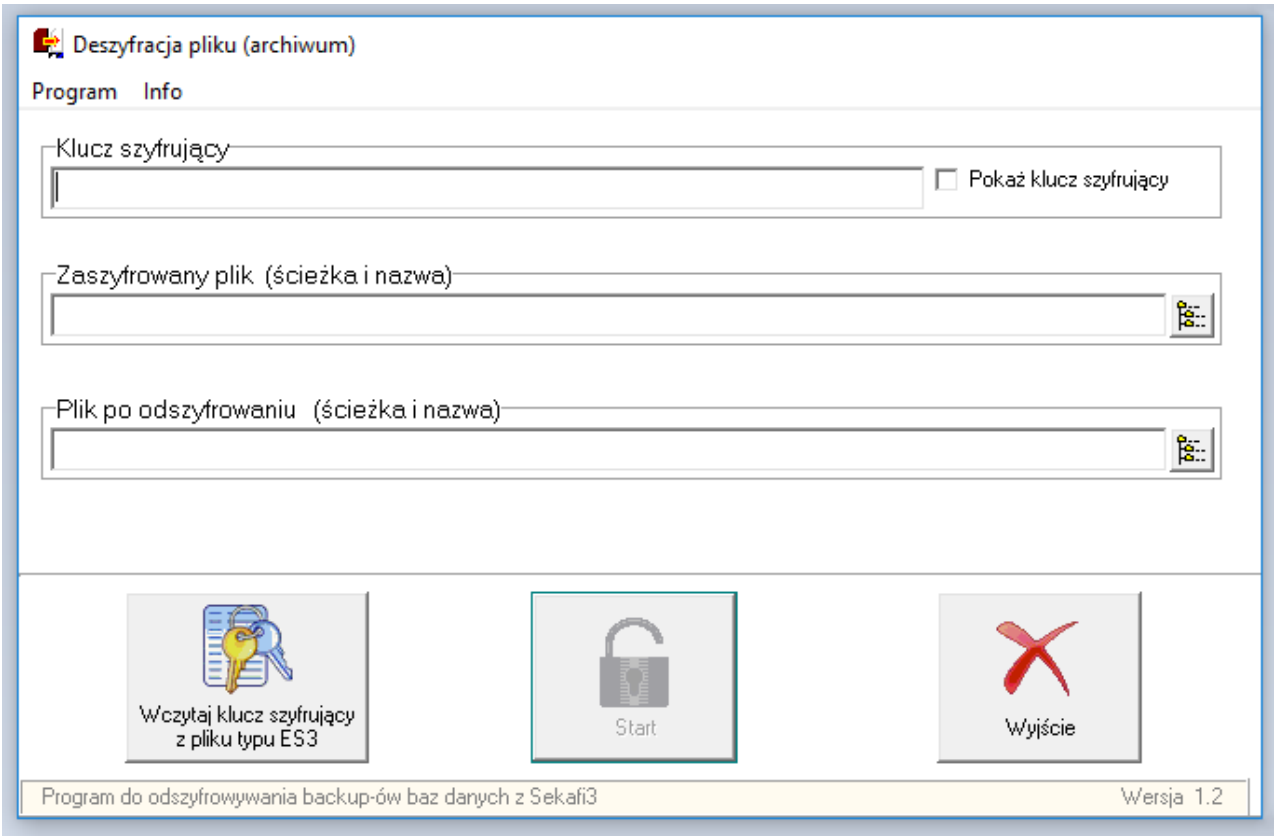


Podobnie jak zostało to opisane w punkcie 8. powyżej, na kartotece osób została dodana zakładka Historia Zmian, za pomocą której w łatwy sposób można przejrzeć wszystkie zmiany jakie były wykonywane na danych osób / pracowników / serwisantów.

9. Zmodyfikowane szablony wydruków, na których umieszczono stosowne informacje dotyczące klauzuli informacji przetwarzania danych osobowych:
   „Administratorem Państwa danych osobowych jest Nazwa Firmy , kod pocztowy Miejscowość, ul. nr. Państwa dane osobowe będą przetwarzane w celu realizacji zlecenia i wystawienia faktury oraz w celach księgowych. Dane mogą zostać udostępnione wyłącznie podmiotom upoważnionym na podstawie przepisów prawa. Przysługuje Państwu prawo dostępu do treści swoich danych i ich poprawiania.
   Podanie danych jest dobrowolne, ale niezbędne do realizacji zlecenia i wystawienia faktury.”

   Powyższa klauzula została dodana do szablonów wydruków takich dokumentów jak np. Pokwitowania przyjęcia i wydania sprzętu, protokół przeglądu ustawowego, zlecenie naprawy, itp.

10. Nowa aplikacja „Odszyfruj plik”



Wszystkie zaszyfrowane kopie zapasowe utworzone przez Sekafi można odszyfrować za pomocą specjalnie w tym celu utworzonej nowej aplikacji „Odszyfruj plik”. Aplikacja ta będzie dołączana do każdej nowej wersji programu Sekafi.

Aby odszyfrować plik kopii należy wskazać plik znajdujący się na dysku, miejsce gdzie ma się zapisać odszyfrowane archiwum oraz podać klucz szyfrujący. Poza standardową opcją wprowadzenia klucza w odpowiednie pole na formularzu powyżej, istnieje także możliwość wczytania zaszyfrowanego klucza w postaci pliku ES3.