Bezpieczeństwo danych osobowych w systemie eDokumenty

SPIS TREŚCI

Bezpieczeństwo danych osobowych w systemie eDokumenty 1
1. Wstęp 2
2. Struktury danych osobowych 2
3. Zasady dostępu do danych 2
4. System zarządzania uprawnieniami do modyfikacji i usuwania danych osobowych. 4
5. Oznaczanie sprzeciwu do przetwarzania 4
6. Zabezpieczenie prawa do przenoszenia danych 5
7. Zabezpieczenie prawa do sprostowania danych 5

METRYKA DOKUMENTU

Data utworzenia: 2018.01.18
Data ostatniej zmiany: 2018.03.19

1. Wstęp

Dane osobowe w systemie eDokumenty mogą dotyczyć:
- bazy danych pracowników,
- bazy danych klientów oznaczonych jako osoby fizyczne,
- baz danych zdefiniowanych przez użytkownika.

Niniejsza specyfikacja opisuje struktury danych predefiniowanych – czyli pracowników i klientów, oraz prawidłowy sposób postępowania z danymi zdefiniowanymi przez użytkownika.

2. Struktury danych osobowych

1. Wykaz systemowych tabel przechowujących dane pozwalające na zidentyfikowanie osób:

Lp	Nazwa tabeli	Opis
1	contacts	Baza klientów. Osoby fizyczne oznaczone są wartością TRUE w polu phyper. Przechowywane są Imię, Nazwisko, PESEL, Telefon.
2	addresses	Adresy – zawierają odwołania do tabeli contacts. Przechowuje: Ulica, Nr bud, Nr lok, Kod, Miasto, Gmina, Woj., Państwo.
3	contact_persons	Osoby kontaktowe. Osoby skojarzone są z firmami. Przechowywane Imię, Nazwisko, Nr telefonu, Email, Data urodzin.
4	users	Użytkownicy. Przechowywane dane: Imię, Nazwisko, Nr telefonu.
5	documents	Dokumenty – metryki. W polu srctxt oraz trgtxt zapisywana jest tekstowa wartość imienia, nazwiska i stanowiska pracownika przekazującego oraz odbierającego dokument.
6	events	Zadania/Zdarzenia – W polu emptxt przechowywana jest wartość tekstowa imienia i nazwiska pracownika, którego dotyczy zdarzenie.
7	processes	Sprawy – W polu addtxt przechowywana jest tekstowa wartość imienia i nazwiska pracownika który utworzył sprawę.
8	register_entry	Tabela ogólna rejestru, po której dziedziczą własności wszystkie założone w systemie rejestry **zdefiniowane przez użytkownika**.23
9	log	Tabela ogólna systemowego loga (dziennika zdarzeń), w której przechowywane są informacje o zmianach w danych wyżej wymienionych obiektów

Pozostałe tabele przechowują dane skojarzone za pomocą identyfikatora użytkownika (usr_id) lub klienta (contid).

3. Zasady dostępu do danych

Dostęp do wszelkich danych w systemie eDokumenty wymaga przeprowadzenia procesu autentykacji (sprawdzenie czy osoba logująca się dysponuje odpowiednim poświadczeniem potwierdzającym że to rzeczywiście ta osoba) i autoryzacji użytkownika (przyznaniem przypisanych do osoby uprawnień). Autentykacja może być realizowana w oparciu o wewnętrzną bazę danych lub zewnętrzny system autentykacji np. LDAP/ActiveDirectory.

System uprawnień

System eDokumenty posiada wielowarstwowy mechanizm zarządzania uprawnieniami użytkowników, w tym uzytkowników będących administratorami. Uprawnienia określane są poprzez przypisanie użytkownikowi odpowiednich grup(ról) agregujących uprawnienia, lub poprzez przypisanie tych uprawnień bezpośrednio dla konta użytkownika.

Konta użytkowników

System pozwala niezależnie od siebie określić uprawnienia do funkcji systemu, oraz uprawnienia do danych. Uprawnienia do danych definiowane są dla następujących obiektów:
- elementów drzewa struktury organizacyjnej
- teczek

- spraw
- dokumentów
- kartotek klientów

W sposób szczególny ważne są uprawnienia do struktury organizacyjnej, gdyż elementy struktury stanowią bazowe kontenery, do których przywiązywane są teczki, sprawy, dokumenty i zdarzenia. Tak więc osoba dysponująca uprawnieniem do stanowiska lub działu automatycznie posiada dostęp do znajdujących się tam danych - o ile uprawnienia nie zostaną zmienione dla poszczególnych rekordów danych.

Podczas tworzenia konta użytkownika, konieczne jest zdefiniowanie nazwy użytkownika i hasła, oraz wybranie grup uprawnień, oraz przydzielenie dostępu do poszczególnych stanowisk. Przydzielanie uprawnień działa z uwzględnieniem drzewiastej struktury tych uprawnień, wykorzystując mechanizm propagacji uprawnień. System nadane uprawnienia oznacza plusem, a odebrane minusem. Dodatkowo kolorami zielonym i czerwonym oznaczane są uprawnienia nadane/odebrane bezpośrednio, a uprawnienia uzyskane z grup widoczne są jako szare.

Definicje grup/ról

Zdefiniowane grupy i role mogą być całkowicie dowolnie skonfigurowane, jednakże dla łatwości i czytelności systemu uprawnień zaleca się odróżniać role administracyjne od ról biznesowych. Ponadto zaleca się stosowanie zasady domyślnego zabraniania, która oznacza w praktyce to, że pracownik nowo założony, dysponuje minimalną ilością uprawnień, nie pozwalających na nic więcej niż zalogowanie się. Kolejne uprawnienia powinien uzyskiwać poprzez udział w grupach, które w swoich definicjach dodają kolejne uprawnienia.
Każdy użytkownik może mieć przypisanych jednocześnie wiele ról. W razie wykluczających się ustawień (jedna rola przydziela, podczas kiedy inna zabiera prawo) brana jest pod uwagę pierwsza od góry przypisana do użytkownika rola. Kolejność grup można zmieniać.

Stosowane metody i środki uwierzytelnienia

Zaleca się, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. Użytkownik po otrzymaniu hasła powinien być zobowiązany do jego zmiany, chyba, że system nie umożliwia wykonania takiej operacji. W zależności od ustalonej polityki dotyczącej haseł system może wymuszać okresową zamianę hasła. Zaleca się by hasło użytkownika było zmieniane nie rzadziej niż co 30 dni i składało się z co najmniej 8 znaków, oraz zawierało duże i małe litery oraz cyfry - jeżeli w systemie są przetwarzane dane osobowe.
Hasła przechowywane są w postaci zaszyfrowanej za pomocą funkcji jednokierunkowych.
Hasło operatora
System eDokumenty umożliwia zdefiniowanie następujących parametrów ustawiania hasła:

- Minimalna długość hasła,
- sprawdzanie zasad złożoności hasła (czy są odpowiednio długie i zawierają cyfry oraz różnej wielkości znaki tzn. zawierała małe i wielkie litery oraz cyfry lub znaki specjalne,
- wymuszanie zmiany hasła przez użytkownika, po upływie określonego terminu,
- wymuszenie historycznej niepowtarzalności hasła,
- określenie liczby prób logowania do systemu z jednego adresu IP przed zablokowaniem konta, jeżeli użytkownik podaje niepoprawne hasło,
- czas, po którym może nastąpić automatyczne odblokowanie konta.

Integralność i poufność danych

Każdy rekord danych, w których mogą być zapisane dane osobowe chroniony jest za pomocą mechanizmów integralności i poufności danych. Poufność jest zapewniona poprzez wskazanie indywidualnie dla każdego rekordu lub dla zbioru rekordów uprawionych ról lub użytkowników. Dzięki temu system zapewnia, że każda konkretna informacja może być modyfikowana lub usuwana jedynie przez osoby uprawnione do wykonywania tych operacji na przydzielonych rekordach.
Integralność chroniona jest poprzez rejestr modyfikacji każdego z rekordów. System utrwala informacje o każdym pojedynczym zdarzeniu modyfikacji i usuwania danych. Rejestry zmian dostępne są za pomocą przycisku Historia znajdującego się na formatce każdego obiektu danych.

4. System zarządzania uprawnieniami do modyfikacji i usuwania danych osobowych.

Kartoteki klientów oznaczonych jako osoby fizyczne podlegają w systemie dodatkowej ochronie. Aby wyświetlić taką kartotekę użytkownik musi posiadać przywilej dostępu do danych osobowych (w gałęzi Systemowe > Przywileje). Prawo usuwania tych kartotek posiada użytkownik, który jednocześnie posiada ten przywilej oraz prawo do usuwania kartotek klientów. Prawo modyfikacji danych kartoteki osoby fizycznej posiada użytkownik, który jednocześnie posiada:
- przywilej dostępu do danych osobowych,
- prawo do edycji danych klientów,
- prawo do indywidualnej kartoteki klienta lub prawo do oglądania całej bazy klientów

5. Zabezpieczenie prawa do dostępu do danych

Co do zasady użytkownikami systemu eDokumenty są pracownicy firm, zatem zabezpieczenie dostępu do danych polega na umożliwieniu przygotowaniu zestawienia zawierającego wszystkie powiązane dane zebrane na temat osoby fizycznej. Tego rodzaju zestawienie w zakresie systemowych obiektów udostępniane jest w kartotece klienta na zakładkach: Terminarz, Dokumenty i Sprawy. Dane utworzone w rejestrach zdefiniownych przez użytkownika dostępne są na kolejnych zakładkach o tej samej nazwie jak utworzony rejestr.

6. Oznaczanie sprzeciwu do przetwarzania

Zgoda na kontakt

Do ewidencji zgody na kontakt można skorzystać z dodatkowego zestawu Cech, lub z systemowej tabeli (dotyczy najnowszych wersji systemu). Tabela zawiera następujące dane:

contact_form_agreement	
Wysyłka email	Zgoda / Brak zgody
Śledzenie wiadomości	Zgoda / Brak zgody
Newsletter	Zgoda / Brak zgody
Telefon	Zgoda / Brak zgody
Faks	Zgoda / Brak zgody
Poczta tradycyjna	Zgoda / Brak zgody

Zaprzestanie przetwarzania

System umożliwia oznaczenie rekordów obiektów biznesowych jako objętych sprzeciwem podmiotu danych na dwóch poziomach: sprzeciwu do dalszego przetwarzania oraz żądania zapomnienia. Odbywa się to za pomocą rozszerzenia GDPR, pozwalającego na dodawanie wpisów w tabeli gdpr_extension przechowujących rozszerzone informacje dotyczące RODO.

gdpr_extension	
Powód przetwarzania:	Słownik:
Źródło pozyskania:	Słownik: e-mail | telefon | spotkanie
Status przetwarzania	PROCESSED, REJECTED, ANONYMISED
CLSNAM	
KEYVAL	
Kto dodał	
Kiedy dodał	
Kto zmienił	
Kiedy zmienił	

Poprzez oznaczenie rekordu statusem typu REJECTED wraz z ustawieniem własności is_del (usunięto) zapobiega się dalszemu przetwarzaniu danych, w tym wyświetlaniu się rekordu we wszelkich formatkach i listach systemu. W takiej postaci system nie pozwala na wykonanie żadnych operacji na tych danych poza samym ich przechowywaniem.

Anonimizacja
W razie otrzymania zgłoszenia zaprzestania przetwarzania wraz z żądaniem anonimizacji danych, system poza oznaczeniem rekordów jako niepodlegających przetwarzaniu, może dokonać anonimizacji danych osobowych. Operacja jest wykonywana w zakresie danych osobowych opisanych w części 2 Struktury danych osobowych (dla struktur systemowych).

Zachowanie w celu zabezpieczenia
Jeśli istnieją przesłanki do zatrzymania danych, należy odpowiedniej roli przydzielić prawo do przeglądania danych o statusie REJECTED pobieranych za pomocą dodatkowych widoków (raportów).

7. Zabezpieczenie prawa do przenoszenia danych

System umożliwia wyeksportowanie wszystkich danych osobowych lub informacji selektywnie wyodrębnionych dotyczących konkretnej osoby fizycznej i przez nią dostarczonych do maszynowego odczytywania powszechnie stosowanego formatu.

W tym celu należy przygotować raporty zawierające zestawienia zawierające dane. Wzorcowe raporty są do pobrania z repozytorium raportów umieszczonym w sekcji download serwera na którym udostępniane są wersje systemu.
W celu eksportu pozostałych danych należy skorzystać z funkcji „Eksport paczki archiwalnej". Odpowiedni CustomScript wraz z instrukcją instalacji i użycia jest dostępny w tym samym miejscu, gdzie raporty. Paczka zawiera pliki oraz zestawienia metadanych możliwych do importu do innych systemów.

8. Zabezpieczenie prawa do sprostowania danych

System umożliwia modyfikację / w tym aktualizację każdej przetwarzanej w nim informacji dot. konkretnej osoby fizycznej. W razie wpływu do firmy prośby o sprostowanie, odpowiednio uprawniony użytkownik może skorzystać z dostępnych funkcji do ich modyfikacji.