• Wdrożenie sytemu informatycznego do SZBI.

Wymagania ogólne systemu

1. Aplikacja (system) powinna być utrzymywana w chmurze obliczeniowej Dostawcy.
2. Aplikacja powinna być dostępna z poziomu dowolnej popularnej przeglądarki internetowej (Edge, Firefox, Chrome, Safari), w wersji która była wypuszczona na rynek po 2024 roku. Po stronie użytkownika końcowego ani Zamawiającego nie powinna występować konieczność instalacji jakiegokolwiek dodatkowego oprogramowania.
3. Wszystkie dane zapisywane w aplikacji powinny być składowane w ramach chmury obliczeniowej Dostawcy, z zachowaniem powszechnie stosowanych standardów bezpieczeństwa. Dostawca usługi zapewni **kopię bezpieczeństwa składowanych danych**, wykonywaną przynajmniej raz na dobę.
4. Aplikacja powinna posiadać polską wersję językową, która stanowi domyślną wersję językową aplikacji.
5. Wszystkie moduły (części) aplikacji powinny ze sobą współpracować, stanowić jedną aplikację oraz nie powinny wymuszać na użytkownikach wprowadzania tych samych danych w kilku miejscach. Użytkownicy nie powinni być także zmuszani do logowania w kilku miejscach aplikacji.
6. Dostawca usługi umożliwi jednoczesną pracę w systemie przynajmniej 15 użytkowników Zamawiającego.
7. W okresie subskrypcji Dostawca usługi będzie dbał o jej niezbędną aktualizację (np. w przypadku zmiany aktów prawnych związanych ze składowanymi danymi lub wykrycia w systemie luki bezpieczeństwa).
8. Świadczenie usługi przez Dostawcę rozpocznie się do 30 dni od dnia podpisania Umowy przez okres **24 miesięcy**. Cena dotyczy wdrożenia systemu. Po wdrożeniu do 24 miesiąca nie będą pobierane żadne opłaty za funkcjonowanie sytemu.
9. Dostawca usługi będzie świadczył ją przez 24h na dobę, 7 dni w tygodniu, z zachowaniem SLA na poziomie 95% (mierzonego w skali roku).
10. Dostawca usługi udostępni adres mailowy, na który możliwe będzie wysyłanie zgłoszeń dotyczących nieprawidłowego działania aplikacji.
11. Dostawca usługi deklaruje usuwanie zgłoszonych błędów, które wynikają z nieprawidłowego działania aplikacji, w terminie:
    a. do 2 dni roboczych – w przypadku błędów krytycznych, które uniemożliwiają korzystanie z jakichkolwiek funkcji aplikacji;
    b. do 6 dni roboczych – w przypadku pozostałych błędów.

Autoryzacja użytkowników

1. Autoryzacja użytkowników powinna odbywać się za pomocą nazwy użytkownika oraz hasła.
2. Aplikacja powinna umożliwiać włączenie dwustopniowego logowania użytkowników z wykorzystaniem tokenów wysyłanych na adres e-mail użytkownika po podaniu przez niego prawidłowego loginu i hasła do systemu. Włączenie takiej opcji wymagać powinno od użytkownika powiązania jego konta z adresem e-mail.

3. Logowanie do aplikacji powinno bazować na loginach (nazwach użytkownika), a nie ich adresach e-mail przez co możliwe jest założenie konta użytkownikowi, który nie posiada służbowego adresu e-mail.

Użytkownicy

1. Aplikacja powinna umożliwiać logowanie się za pomocą jednego konta użytkownika do wielu organizacji oraz powinna umożliwiać zapraszanie użytkowników do organizacji za pomocą systemu zaproszeń (np. inspektorowi ochrony danych osobowych, który może obsługiwać wiele podmiotów korzystających z zamawianego oprogramowania).
2. Aplikacja powinna umożliwiać importowanie listy użytkowników wg dostarczonego wcześniej wzorca.
3. Każdy z użytkowników powinien mieć możliwość przypisywania dowolnej liczby uprawnień do konkretnych miejsc w systemie.
4. Aplikacja powinna umożliwiać podgląd karty dowolnego użytkownika, na której oprócz jego danych zaprezentowane powinny być powiązane z nim dane (min. składane przez niego oświadczenia, nadane mu upoważnienia dostępu do danych)
5. Każdy użytkownik powinien posiadać możliwość zmiany hasła, poprzez podanie:
    a. aktualnego hasła,
    b. nowego hasła i jego potwierdzenia.
6. Aplikacja powinna umożliwiać przypisanie do użytkownika adresu e-mail, na który mają być wysyłane wszelkie powiązane z nim powiadomienia (w sytuacji kiedy nie posiada on służbowego adresu e-mail).

Powiadomienia

1. Użytkownik powinien otrzymywać powiadomienia o różnych zdarzeniach w systemie, z którymi jest powiązany lub informacje systemowe przesyłane przez Dostawcę usługi.
2. Aplikacja powinna wyświetlać informację o liczbie nieodczytanych przez użytkownika powiadomień.
3. Każdy użytkownik powinien posiadać możliwość określenia dla swojego konta częstotliwości przysyłanych powiadomień min. dla następujących opcji (wyłączone, raz dziennie, raz w tygodniu, raz w miesiącu).

Listy kontrolne

1. Aplikacja powinna umożliwiać cykliczne wypełnianie list kontrolnych.
2. Aplikacja powinna posiadać obligatoryjne listy kontrolne, na podstawie których możliwe będzie ustalenie stopnia zgodności prowadzonej dokumentacji min. z wymaganiami: jakościowymi ISO 27001 i RODO. Wypełnianie tych list powinno być obligatoryjne, cykliczne, a system powinien informować użytkowników o stopniu zgodności stwierdzonym po wypełnieniu takiej listy oraz liczbie dni do następnego audytu.
3. Dostawca usługi powinien dostarczać także szablony innych list kontrolnych, na podstawie których Zamawiający będzie mógł stworzyć własne listy kontrolne. Użytkownicy powinni mieć też możliwość tworzenia własnej listy kontrolnej od podstaw.
4. Wypełnione przez użytkowników listy kontrolne powinny być widoczne w ramach zestawienia, które oprócz nazwy listy prezentuje przynajmniej następujące dane:
    a. nazwę użytkownika, który ją wypełnił
    b. procentową ocenę
    c. datę wypełnienia

Rejestr incydentów

1. Aplikacja powinna posiadać możliwość prowadzenia rejestru incydentów naruszenia ochrony danych osobowych.
2. Aplikacja powinna prezentować rejestr wprowadzonych incydentów w postaci tabeli, która będzie zawierała przynajmniej następujące informacje:
    a. nazwę incydentu;
    b. data wystąpienia zdarzenia;
    c. informację czy konieczne było powiadomienie organu nadzorczego;
    d. datę, do której organ nadzorczy powinien zostać powiadomiony (jeżeli było to wymagane);
    e. datę, w której organ nadzorczy został powiadomiony;
    f. nazwa użytkownika odpowiedzialnego za wpis;
    g. status incydentu (w trakcie procesowania, zakończone);
3. Użytkownicy aplikacji powinni mieć możliwość wprowadzenia nowych incydentów do rejestru poprzez podanie minimum następujących danych (dodanie innych danych wymaganych przez system powinno nie być obligatoryjne):
    a. nazwa incydentu;
    b. data i godzinę wystąpienia zdarzenia;
    c. kategoria danych;
    d. zakres danych;
    e. liczba wpisów ze zbioru danych;
    f. jakie były źródła naruszenia;
    g. jakie były skutki naruszenia;
    h. jakie czynności zaradcze zostały podjęte;
    i. nazwa użytkownika, który jest odpowiedzialny za czynności zaradcze;
    j. datę i godzinę podjęcia czynności zaradczych;
4. Aplikacja powinna pozwalać także na wykonanie oceny naruszenia, poprzez podanie następujących danych:
    a. rodzaju danych, których dotyczył incydent (np. finansowe, osobowe, lokalizacyjne) wraz z możliwością dodania szczegółowej notatki w tym zakresie;
    b. łatwości identyfikacji – stopnia określającego łatwość identyfikacji konkretnej osoby na podstawie tych danych;
    c. określenie stopnia naruszenia: poufności, integralności oraz dostępności;
    d. wskazanie czy incydent był zamierzony czy przypadkowy;
5. Na podstawie dodanego incydentu aplikacja powinna umożliwiać tworzenie zawiadomienia kierowanego do osób, których danych incydent dotyczyły. Zawiadomienie powinno być możliwe do pobrania z aplikacji w formie pliku DOCX lub PDF. W celu pobrania zawiadomienia użytkownik aplikacji powinien wypełnić formularz, w którym:
    a. dokona opisu zdarzenia;
    b. wskaże, których danych dotyczył incydent;
    c. opisze podjęte działania;
    d. sprecyzuje jakie są możliwe skutki naruszenia;
    e. wskaże odpowiednie zalecenia;
6. Aplikacja powinna umożliwić wprowadzenie informacji dotyczących zakończenia obsługi danego incydentu. W tym celu uprawnieni użytkownicy aplikacji powinni wypełnić formularz, w którym podadzą następujące dane:
    a. datę powiadomienia osób;
    b. datę powiadomienia organu nadzorczego;

c. załączą kopię dokumentu przesłanego do organu nadzorczego;
d. działania zaradcze, które zostały podjęte;

7. Aplikacja powinna umożliwiać podgląd bieżących i archiwalnych wpisów do rejestru, na którym będą prezentowane dane, o których mowa w pkt. 3, 4 oraz 6.

Rejestr czynności przetwarzania danych

1. Aplikacja powinna umożliwiać prowadzenie rejestru przetwarzania danych. Wszystkie wpisy dodane do tego rejestru powinny być widoczne dla użytkowników w formie tabeli, która zawiera min. nazwę wpisu oraz datę jego dodania.
2. Uprawnieni użytkownicy powinni posiadać możliwość tworzenia nowych wpisów do rejestru poprzez podanie min. następujących danych:
    a. nazwy czynności;
    b. lokalizacji, w której dana czynność jest wykonywana;
    c. nazwy i danych kontaktowych współadministratora;
    d. nazwy i danych kontaktowych podmiotu przetwarzającego;
    e. nazwy systemu/oprogramowania, w ramach którego przetwarzane są dane;
    f. wskazanie czy dane będą przetwarzane przez podmiotu pochodzący z kraju trzeciego lub organizację międzynarodową;
    g. wskazanie celów przetwarzania danych;
    h. określenie kategorii osób (np. pracownicy, kandydaci do pracy, stażyści, uczniowie);
    i. wskazanie kategorii danych;
    j. wskazanie ewentualnych podstaw prawnych dla czynności;
    k. wskazanie źródeł pochodzenia danych (np. formularz rekrutacyjny);
    l. określenie warunków, które muszą zostać spełnione, aby dane zostały usunięte;
    m. wskazanie kategorii odbiorców;
    n. opisanie wszystkich środków bezpieczeństwa, które chronią dane przed ewentualnym naruszeniami bezpieczeństwa;
3. Użytkownicy aplikacji powinni mieć możliwość wybrania jednego ze wzorów dla wpisu, który wstępni wypełni wspomniane w pkt 2 pola formularza.
4. Aplikacja powinna pozwalać użytkownikom na edytowanie wpisu dokonanego do tego rejestru oraz jego usunięcie.
5. Aplikacja powinna posiadać funkcję importowania wielu wpisów do rejestru za pomocą wgrywanego przez użytkowników arkusza kalkulacyjnego. Dostawca usługi powinien udostępnić Zamawiającemu szablon dla takiego arkusza.

Spis zabezpieczeń

1. Aplikacja powinna prowadzić rejestr dotyczący zabezpieczeń związanych z ochroną danych w danej organizacji. Rejestr (spis) powinien być dostępny w formie tabeli, która prezentuje kategorie zabezpieczeń oraz konkretne zabezpieczenia do nich przypisane.
2. Użytkownicy aplikacji powinni mieć możliwość dodawania, edytowania i usuwania zabezpieczeń z systemu.
3. Do każdej kategorii zabezpieczeń powinna istnieć możliwość dopisania dowolnej ilości rzeczywistych zabezpieczeń.
4. Aplikacja powinna posiadać także słownik, który pozwalałby na dodanie do spisu standardowych form zabezpieczeń (np. fizycznych, technicznych, informatycznych).

5. Spis powinien być możliwy do wykorzystania w innych częściach systemu (np. analizie ryzyka).

Rejestr aktyw

1. Aplikacja powinna pozwalać na tworzenie rejestru (spisu) aktyw (np. infrastruktura IT) i przypisanych do nich podaktyw (np. przełącznik sieciowy, ups, serwer).
2. Użytkownicy aplikacji powinni mieć możliwość dodawania, edytowania i usuwania aktyw do rejestru.
3. Do każdego aktywa powinna istnieć możliwość przypisania dowolnej ilości podaktyw.
4. Aplikacja powinna posiadać także słownik, który pozwalałby na dodanie do spisu standardowych aktyw (np. infrastruktury IT, pracowników)
5. Rejestr powinien być możliwy do wykorzystania w innych częściach systemu (np. analizie ryzyka).

Systemy informatyczne

1. Aplikacja powinna umożliwiać tworzenie spisu wszystkich systemów informatycznych wykorzystywanych przez Zamawiającego.
2. Spis powinien być prezentowany w formie tabeli, która oprócz nazwy systemu powinna prezentować też jego: opcjonalny opis, datę wygaśnięcia licencji. Każdy wpis widoczny w tabeli powinien posiadać też flagę/status/ikonę, która określa czy dany system służy do przetwarzania danych osobowych.
3. Użytkownicy powinni mieć możliwość dodawania, edytowania i usuwania systemów z spisu. Powinni mieć możliwość wyświetlenia wszystkich danych na karcie informacyjnej dotyczącej konkretnego systemu.
4. Spis powinien być możliwy do wykorzystania w innych częściach systemu (np. analizie ryzyka).

Analiza ryzyka

1. Aplikacja powinna umożliwiać sporządzania analiz ryzyka na potrzeby różnych sytuacji, dotyczących przynajmniej: bezpieczeństwa informacji, ochrony danych osobowych.
2. Uprawnieni użytkownicy mają posiadać możliwość sporządzenia takiej analizy poprzez:
    a. wybranie lub dodanie nowego zagrożenia z/do listy zagrożeń (możliwość dodania wielu zagrożeń do jednej analizy);
    b. wskazanie rejestrów czynności przetwarzania danych, których analiza dotyczy (możliwość powiązania wielu rejestrów);
    c. oceny prawdopodobieństwa wystąpienia zdarzenia;
    d. oceny jakie skutki może spowodować wystąpienie zdarzenia;
3. W przypadku wystąpienia ryzyka aplikacja powinna uaktywnić formularz związany z redukowaniem ryzyka. W ramach formularza użytkownik powinien podać dla każdego zagrożenia wymagającego interwencji:
    a. datę, do której ryzyka musi zostać zredukowane;
    b. osobę odpowiedzialną za redukcję;
    c. opis działań, które muszą być wykonane w związku z wystąpieniem ryzyka;

Umowy powierzenia

1. Aplikacja powinna umożliwiać tworzenie spisu umów powierzenia danych osobowych. Spis powinien być dostępny dla użytkowników w formie tabeli zawierającej min. następujące dane:

    a. nazwa administratora danych;
    b. nazwa podmiotu przetwarzającego dane;
    c. rola jednostki (Zamawiającego) w zakresie danej umowy: podmiot przetwarzający/administrator danych;
    d. data zawarcia umowy;
    e. data zakończenia umowy;
    f. status umowy: obowiązująca/zakończona;
2. Uprawnieni użytkownicy powinni mieć możliwość dodawania, edytowania i usuwania umów do spisu.
3. Aplikacja powinna umożliwiać import danych dotyczących wielu umów jednocześnie, np. z wykorzystaniem szablonu (dostarczonemu Zamawiającemu) sporządzonym w formacie arkusza kalkulacyjnego.

Oświadczenia

1. Aplikacja powinna umożliwiać tworzenie spisu oświadczeń składanych przez użytkowników. Spis powinien być dostępny w formie tabeli zawierającej min. imię i nazwisko użytkownika, nazwę oświadczenia, opcjonalny opis.
2. Uprawnieni użytkownicy powinni mieć możliwość dodawania, edytowania i usuwania nowych oświadczeń do spisu.
3. W celu dodania nowego oświadczenia użytkownik powinien wypełnić formularz, w którym:
    a. poda imię i nazwiska osoby składającej oświadczenie;
    b. wprowadzi nazwę oświadczenia;
    c. opcjonalnie wprowadzi opis oświadczenia;
    d. załączy skan lub dokument elektroniczny zawierający oświadczenie.

Rejestr upoważnień

1. Aplikacja powinna umożliwiać tworzenie rejestru zawierającego informacje o sporządzonych upoważnieniach do przetwarzania danych.
2. Rejestr powinien umożliwiać dodawania upoważnień dotyczących przetwarzania danych wewnątrz organizacji (przez Zamawiającego) oraz na zewnątrz (przez upoważnione podmioty).
3. Uprawnieni użytkownicy powinni mieć możliwość dodawania, edytowania i usuwania upoważnień do rejestru.
4. W celu dodania nowego upoważnienia do rejestru użytkownik powinien wypełnić formularz, w którym:
    a. określi użytkownika lub podmiot (dotyczy umów zewnętrznych), którego upoważnienie dotyczy;
    b. podstawy upoważnienia (np. z tytułu zajmowanego stanowiska);
    c. określi datę wygaśnięcia upoważnienia;
    d. wskaże zbiory danych, których dotyczy upoważnienie;
    e. wskaże systemy informatyczne, których dotyczy upoważnienie.
5. System powinien umożliwiać wysyłanie upoważnienia do kierownika organizacji, w celu jego zatwierdzenia.