303205

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa licencji wraz z wdrożeniem systemu informatycznego (narzędzia) wspomagającego zarządzanie zgodnością z przepisami o ochronie danych osobowych (RODO[1]) oraz krajowymi przepisami obowiązującymi w tym obszarze.

System ma wspierać realizację obowiązków nałożonych na administratora oraz podmiot przetwarzający wynikających z RODO oraz wspomagać pracę komórek organizacyjnych realizujących zadania w obszarze ochrony danych osobowych. System powinien umożliwiać prowadzenie pełnej dokumentacji dla procesów, w których Zamawiający występuje jako administrator danych, jak i dla procesów, w których Zamawiający występuje jako podmiot przetwarzający.

1. Wymagania funkcjonalne

Narzędzie ma umożliwiać w szczególności:

1) prowadzenia rejestrów i ewidencji, w szczególności:

- RCP (rejestr czynności przetwarzania) - tworzenie, edycja, aktualizacja;
  RCP powinien umożliwiać prowadzenie rejestru czynności przetwarzania zgodnie z art. 30 ust. 1 RODO, w tym wskazanie celu przetwarzania, kategorii osób, kategorii danych, odbiorców, transferów poza EOG, terminów retencji oraz ogólnego opisu środków technicznych i organizacyjnych stosowanych do zapewnienia bezpieczeństwa danych;
- RKCP (rejestr kategorii czynności przetwarzania) - tworzenie, edycja, aktualizacja;
  RKCP powinien umożliwiać prowadzenie rejestru kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO, z możliwością przypisania administratora, kategorii przetwarzań, transferów poza EOG oraz zabezpieczeń;
- rejestr podmiotów, których administrator powierzył przetwarzania danych osobowych, obejmujący co najmniej: dane podmiotu przetwarzającego, podstawę powierzenia, zakres i cel przetwarzania, kategorie danych, czas trwania powierzenia, informacje o podpowierzeniu oraz status umowy powierzenia;
- ewidencji upoważnień do przetwarzania danych osobowych w podziale: dla pracowników, dla innych osób wskazanych przez administratora, Ewidencja upoważnień powinna umożliwiać nadawanie, zmianę, cofanie i archiwizowanie upoważnień wraz z historią zmian, datą obowiązywania, zakresem upoważnienia oraz osobą zatwierdzającą;
- rejestru naruszeń ochrony danych osobowych. Rejestr naruszeń powinien umożliwiać dokumentowanie naruszeń zgodnie z art. 33 ust. 5 RODO, w tym opis naruszenia, kategorie danych i osób, ocenę ryzyka, decyzję o zgłoszeniu lub braku

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

zgłoszenia do PUODO, działania zaradcze oraz powiadomienie osób, których dane dotyczą.
- ewidencji wniosków podmiotów danych, Ewidencja wniosków osób, których dane dotyczą, powinna umożliwiać rejestrowanie rodzaju żądania, daty wpływu, terminu realizacji, statusu sprawy, odpowiedzi oraz podstawy odmowy, jeżeli dotyczy
- rejestru zgód na przetwarzanie danych, oraz innych rejestrów wymaganych przez Zamawiającego, możliwych do skonfigurowania przez administratora systemu.

2) zarządzanie ryzykiem - przeprowadzania dla procesów przetwarzania analizy ryzyka (PIA/DPIA) oraz oceny skutków przetwarzania w zakresie ochrony praw i wolności osób. System powinien umożliwiać przeprowadzanie analizy ryzyka dla praw i wolności osób fizycznych oraz oceny skutków dla ochrony danych zgodnie z art. 35 RODO, z możliwością dokumentowania środków minimalizujących ryzyko, akceptacji ryzyka oraz zatwierdzenia DPIA. „System powinien umożliwiać obieg akceptacyjny DPIA, w tym opiniowanie przez IOD, zatwierdzenie przez właściciela procesu/ADO oraz monitorowanie realizacji środków zaradczych;
Zamawiający wymaga zastosowania rozwiązania automatyzującego obieg dokumentów i zadań bez konieczności ręcznego przekazywania dokumentów. Liczba etapów i kolejność zostaną określone przez Zamawiającego. Szczegóły zostaną ustalone podczas warsztatów analityczno-wdrożeniowych (termin do 30 dni od podpisania umowy) i potwierdzone w dokumencie analizy przedwdrożeniowej stanowiącym element odbioru.

3) zarządzanie incydentami – moduł do rejestracji, analizy i obsługi naruszeń (zgłoszenie do Prezesa UODO, powiadamianie osób) oraz monitorowania realizacji rekomendacji. System powinien umożliwiać rejestrację incydentów bezpieczeństwa informacji oraz ich kwalifikację pod kątem wystąpienia naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.
W przypadku naruszeń podlegających zgłoszeniu do Prezesa UODO wymagana jest możliwość eksportu z Systemu danych i informacji do obowiązującego formularza *Zgłoszenia naruszenia ochrony danych osobowych*.
4) e-learning - przeprowadzania szkoleń dla ok. 700 pracowników, np. zamieszczanie prezentacji, nagrań, plików do zapoznania, z możliwością sprawdzenia wiedzy poprzez wykonanie testu oraz generowanie certyfikatu. Moduł e-learning powinien umożliwiać generowanie raportu uczestnictwa w szkoleniach, wyników testów, dat ukończenia szkolenia oraz generowanie potwierdzeń/certyfikatów ukończenia szkolenia przez poszczególnych pracowników;

5) przeprowadzania audytów i kontroli, w tym tworzenie raportów;
system powinien umożliwiać planowanie, prowadzenie oraz dokumentowanie audytów i kontroli w obszarze ochrony danych osobowych oraz bezpieczeństwa informacji, w tym:
   - tworzenie planów audytów;
   - definiowanie zakresu, kryteriów i harmonogramów audytów;
   - przypisywanie audytorów i osób odpowiedzialnych;
   - rejestrowanie ustaleń, niezgodności, ryzyk i rekomendacji;
   - monitorowanie realizacji działań korygujących i terminów ich wykonania;
   - generowanie raportów z audytów;
   - prowadzenie historii audytów i zmian;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

- eksport raportów do powszechnie używanych formatów;

6) baza wzorów dokumentów: np. upoważnień, raportów, DPIA, zgłoszenie naruszenia do PUODO, itd. System powinien zapewniać wersjonowanie dokumentów, historię zmian, oznaczanie statusu dokumentu oraz możliwość nadawania uprawnień dostępu do poszczególnych kategorii dokumentów;

7) stworzenia bazy wiedzy poprzez zamieszczenie, aktualizację, udostępnianie pracownikom regulacji wewnętrznych np. polityk, regulaminów, artykułów dotyczących RODO, linków do stron, itp System powinien umożliwiać dystrybucję regulacji wewnętrznych wraz z możliwością potwierdzenia zapoznania się przez pracownika oraz raportowania tych potwierdzeń;
Zamawiający zapewni zamieszczenie, aktualizację, udostępnianie pracownikom materiałów.

8) dystrybucja informacji/komunikatów dotyczących obszaru ochrony danych wśród pracowników;
system powinien umożliwiać dystrybucję komunikatów, informacji i alertów dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji, w tym:
   - kierowanie komunikatów do wybranych grup użytkowników;
   - definiowanie kategorii i priorytetów komunikatów;
   - potwierdzanie zapoznania się z komunikatem;
   - monitorowanie statusu odczytu;
   - planowanie publikacji i wycofania komunikatów;
   - prowadzenie historii komunikatów;
   - eksport raportów dotyczących dystrybucji i potwierdzeń zapoznania się;

9) monitorowanie terminów wskazanych w poszczególnych modułach, przekazywanie informacji do wskazanej osoby automatyczne przekazywanie powiadomień i przypomnień do użytkowników lub grup użytkowników wskazanych zgodnie z konfiguracją systemu i przypisanymi rolami.";

   system powinien umożliwiać monitorowanie terminów związanych z realizacją obowiązków w obszarze ochrony danych osobowych i bezpieczeństwa informacji, w szczególności:
   - terminów realizacji wniosków osób, których dane dotyczą;
   - terminów obsługi incydentów i naruszeń;
   - terminów realizacji działań korygujących;
   - terminów przeglądów DPIA i analiz ryzyka;
   - terminów ważności upoważnień;
   - terminów ukończenia szkoleń;
   - terminów wynikających z umów powierzenia.

   system powinien umożliwiać również:
   - definiowanie terminów i przypomnień;
   - konfigurację powiadomień;
   - przypisywanie osób odpowiedzialnych;
   - eskalację braku realizacji zadania;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

- monitorowanie statusu realizacji;
- generowanie raportów dotyczących terminowości realizacji zadań;

10) automatyczne przypisywanie zadań i powiadamianie pracowników na e-mail/Teams; Powiadomienia e-mail/Teams powinny być konfigurowalne i nie powinny zawierać nadmiarowych danych osobowych ani szczegółowych informacji o naruszeniach; powinny odsyłać użytkownika do systemu po uwierzytelnieniu.

11) generowanie raportów kwartalnych, rocznych z realizacji zadań. System powinien umożliwiać generowanie raportów okresowych (m.in. kwartalnych i rocznych) dotyczących realizacji zadań w obszarze ochrony danych osobowych i bezpieczeństwa informacji, w szczególności:
    - realizacji wniosków osób, których dane dotyczą;
    - obsługi incydentów i naruszeń;
    - realizacji działań korygujących;
    - przeprowadzonych audytów;
    - statusu analiz ryzyka i DPIA;
    - realizacji szkoleń;
    - statusu upoważnień;
    - terminowości realizacji zadań;

    system powinien umożliwiać:
    - definiowanie zakresu raportu;
    - filtrowanie danych;
    - raportowanie według procesu, jednostki organizacyjnej, administratora danych, systemu lub właściciela zadania;
    - eksport raportów do formatów XLSX, CSV i PDF;
    - tworzenie raportów zbiorczych oraz szczegółowych;

12) dostęp do regulacji prawnych (krajowych i unijnych), wytycznych i rekomendacji organów nadzorczych, standardów bezpieczeństwa obowiązujących w obszarze ochrony danych, dobrych praktyk z bieżącą ich aktualizacją; System powinien zapewniać dostęp do aktualnych informacji, wraz z możliwością ich wyszukiwania, filtrowania, wersjonowania oraz udostępniania użytkownikom zgodnie z nadanymi uprawnieniami. System powinien umożliwiać publikowanie komunikatów o zmianach regulacyjnych oraz powiadamianie użytkowników o dodaniu lub aktualizacji dokumentów.
    Zamawiający wymaga aby aktualizację bazy regulacji prawnych (krajowych i unijnych) zapewnił Wykonawca.
    Zamawiający wymaga aby system umożliwiał wysyłanie powiadomień o zmianach.

2. Funkcjonalności dodatkowe (opcjonalne)

Funkcjonalności dodatkowe oparte o sztuczną inteligencję (AI) – opcjonalne, punktowane w kryteriach oceny ofert. System może dodatkowo posiadać poniższe funkcjonalności; nie są one wymagane jako warunek spełnienia OPZ, a ich zaoferowanie podlega ocenie w ramach pozacenowego kryterium oceny ofert:

1) analiza ryzyka wspierana AI – system może automatycznie sugerować poziom ryzyka przetwarzania na podstawie kategorii danych i kontekstu procesu; sugestia ma charakter

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

wyłącznie pomocniczy i każdorazowo podlega obowiązkowej walidacji i zatwierdzeniu przez IOD lub właściciela procesu; system nie może samodzielnie podejmować decyzji wywołujących skutki prawne lub w podobny sposób istotnie wpływających na osobę w rozumieniu art. 22 RODO;

2) automatyczna klasyfikacja zgłoszeń i wniosków – system może automatycznie rozpoznawać rodzaj żądania osoby, której dane dotyczą, w celu skrócenia czasu rejestracji sprawy; wynik klasyfikacji musi podlegać weryfikacji i możliwości korekty przez uprawnionego użytkownika przed nadaniem biegu sprawie;
3) wyszukiwanie semantyczne – system może umożliwiać wyszukiwanie semantyczne w bazie wiedzy oraz w bazie regulacji prawnych, zwracające wyniki dopasowane znaczeniowo do zapytania, a nie wyłącznie na podstawie dosłownego dopasowania słów kluczowych;
4) chatbot wiedzy RODO – system może udostępniać pracownikom funkcję chatbota odpowiadającego na pytania z zakresu ochrony danych osobowych wyłącznie na podstawie dokumentów i bazy wiedzy zatwierdzonych przez Zamawiającego (tryb „closed-book"); interfejs chatbota musi zawierać czytelną informację, że udzielana odpowiedź nie stanowi stanowiska Inspektora Ochrony Danych ani porady prawnej;
5) generowanie wstępnych wersji dokumentacji – system może generować wstępny szkic dokumentacji (np. projekt DPIA) na podstawie danych wprowadzonych przez użytkownika w formularzu, wymagający obowiązkowej weryfikacji i zatwierdzenia przez uprawnionego użytkownika przed nadaniem dokumentowi statusu obowiązującego.

Warunkiem przyznania punktów za daną funkcjonalność jest łączne spełnienie wymogów bezpiecznego zastosowania AI, w tym: brak samodzielnego podejmowania decyzji w rozumieniu art. 22 RODO, możliwość odrzucenia/korekty sugestii przez użytkownika z odnotowaniem tego faktu w logu aktywności, oraz przedstawienie przez Wykonawcę klasyfikacji funkcjonalności AI zgodnie z ustawą o systemach sztucznej inteligencji oraz rozporządzeniem 2024/1689 (AI Act), wraz ze wskazaniem poziomu ryzyka systemu AI i zastosowanych środków zgodności.

3. Wymagania techniczne:

1) System powinien umożliwiać definiowanie ról i uprawnień, w szczególności ról: administrator systemu dla co najmniej 2 osób, użytkownik, właściciel procesu, IOD, audytor, osoba opiniująca oraz osoba zatwierdzająca; Liczba kont o uprawnieniach administratora systemu jest konfigurowalna i ustalana przez Zamawiającego (nie mniej niż 2), z zachowaniem zasady rozdziału obowiązków (segregation of duties) i możliwością przypisania odrębnych administratorów dla poszczególnych administratorów danych/procesów obsługiwanych w Systemie.
2) nadawanie pracownikom indywidualnych uprawnień i dostępów, w celu realizacji przydzielonych zadań. System powinien umożliwiać okresowy przegląd uprawnień, raportowanie aktywnych dostępów oraz odbieranie uprawnień użytkownikom, którzy utracili podstawę dostępu;
3) wykonywanie kopii zapasowych;
4) System powinien wspierać realizację obowiązków wynikających w szczególności z art. 5, 24, 25, 30, 32, 33, 34 i 35 RODO, w tym zasadę rozliczalności, minimalizacji danych, integralności i poufności, privacy by design oraz privacy by default;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

5) Wykonawca wskaże model wdrożenia oraz lokalizację przetwarzania danych, która musi znajdować się na terytorium EOG. Zamawiający zastrzega sobie prawo do audytu podwykonawców (subprocessors;
6) System oraz jego interfejs użytkownika muszą spełniać wymagania Krajowych Ram Interoperacyjności oraz ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (WCAG 2.1 poziom AA).".

4. Wymagania dotyczące bezpieczeństwa:

1) zasada najmniejszego uprzywilejowania implementowana poprzez model RBAC (w szczególności w odniesieniu do tożsamości usługowych/zarządzania);
2) wymuszony dostęp warunkowy dla operacji wrażliwych;
Zamawiający wymaga użycia MFA a w przypadku integracji ze środowiskiem Microsoft – Conditional Access;
3) szyfrowanie danych w spoczynku (min. AES-256) oraz w trakcie transmisji (TLS).
'Zamawiający dopuszcza rozwiązania równoważne pod względem funkcjonalnym i poziomu bezpieczeństwa, pod warunkiem wykazania równoważności przez Wykonawcę.;
4) integralność rejestru poprzez implementację zasady WORM (Write Once, Read Many) uniemożliwiającą edycję (określonych danych) lub ich usunięcie. Ewentualna modyfikacja wymaga rejestracji w logu audytowym;
Zasada WORM powinna dotyczyć logów audytowych, rejestru naruszeń oraz wpisów w RCP;
Zasadą WORM należy objąć również zatwierdzone dokumenty DPIA/analizy ryzyka - ich edycja po zatwierdzeniu wymaga utworzenia nowej wersji z zachowaniem historii;
Zamawiający dopuszcza rozwiązania równoważne pod względem funkcjonalnym i poziomu bezpieczeństwa, pod warunkiem wykazania równoważności przez Wykonawcę na etapie oferty.
5) ochrona przed wstrzykiwaniem kodu poprzez rygorystyczne sprawdzanie poprawności wprowadzanych danych;
6) API Security wymagające autoryzacji oraz ograniczenia liczby zapytań;
7) rejestracja aktywności każdego zdarzenia (odczyt, modyfikacja, usunięcie lub eksport danych z systemu musi zostać zarejestrowany), źródło aktywności, czas, data, operacja;
8) przekazywanie zarejestrowanych aktywności / zdarzeń do systemów klasy SIEM/SOAR (log audytu, log zmian zasobu, alarmy wykrycia zdarzeń bezpieczeństwa;
Zamawiający posiada system SIEM. Występuje możliwość integracji poprzez Syslog, API, CEF/LEEF, JSON. Oczekiwany zakres przekazywanych zdarzeń to wystąpienia dotyczące zagadnień bezpieczeństwa;
9) dostosowanie aplikacji do wymagań standardu OWASP ASVS (co najmniej poziom 2);
Zamawiający oczekuje potwierdzenia zgodności w formie raportu z audytu lub testów penetracyjnych. Wykonawca przeprowadzi test penetracyjny aplikacji co najmniej raz w okresie obowiązywania umowy oraz każdorazowo po istotnej zmianie Systemu, przekazując Zamawiającemu raport wraz z planem naprawczym.
10) linia bazowa bezpieczeństwa zgodna z benchmarkami CIS;
Zamawiający oczekuje zgodności z benchmarkami CIS dla systemu operacyjnego, serwera aplikacyjnego i bazy danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

11) implementacja możliwości wykonywania regularnego tworzenia backupu danych. Dostępność usługi powinna zostać zapewniona na poziomie nie niższym niż 99,9% w każdym miesiącu kalendarzowym, z wyłączeniem okien serwisowych Maksymalny RTO nie może przekroczyć 8 godzin, Maksymalny RPO nie może przekroczyć 4 godzin. Kopie zapasowe muszą być wykonywane automatycznie min. jeden raz na dobę z retencją minimum 30 dni. Kopie zapasowe muszą być szyfrowane. Kopie bezpieczeństwa muszą być chronione przed nieautoryzowanym usunięciem i modyfikacją. Wykonawca zapewni możliwość wykonywania testów odtworzenia co najmniej raz na kwartał. Wynik testu odtworzeniowego musi obejmować czas odtworzenia, zakres odtworzonych danych, wykryte błędy i działania korygujące. Na żądanie zamawiającego Wykonawca musi przekazać raport z ostatniego testu odtworzeniowego. Kopie bezpieczeństwa muszą obejmować również załączniki, historie zmian, zgody i konfigurację systemu.
12) Wykonawca zapewni depozyt kodu źródłowego u niezależnego podmiotu (escrow) lub przedstawi równoważny mechanizm zabezpieczenia ciągłości dostępu do Systemu i danych w przypadku zaprzestania świadczenia usług.

5. Informacje dodatkowe:

Termin realizacji: wdrożenie do 3 miesięcy od daty podpisania umowy. Wykonawca zapewni dostępność Systemu na poziomie min. 99,5% w skali miesiąca, czas reakcji na awarię krytyczną max. 8h robocze, czas usunięcia awarii krytycznej max. 48h, RPO ≤ 48h, RTO ≤ 24h."

Okres licencji: 12 miesięcy od daty podpisania protokołu odbioru. Wykonawca zapewni możliwość eksportu wszystkich danych i dokumentów zgromadzonych w Systemie w formatach powszechnie używanych (XLSX/CSV/PDF/XML) w terminie nie dłuższym niż 30 dni od zakończenia lub rozwiązania umowy, bez dodatkowych opłat.

Wsparcie: szkolenie administratorów systemu, wsparcie techniczne oraz aktualizacja systemu 12 miesięcy od daty podpisania protokołu odbioru

Przetwarzanie danych osobowych:
system będzie przetwarzał dane osobowe niezbędne do realizacji funkcjonalności systemu, w szczególności:

- dane użytkowników systemu;
- dane osób objętych upoważnieniami;
- dane osób zgłaszających incydenty i naruszenia;
- dane osób, których dotyczą wnioski realizowane w ramach praw wynikających z RODO;
- dane kontaktowe pracowników i współpracowników;
- dane związane z realizacją szkoleń;
- dane zawarte w dokumentacji audytowej, DPIA oraz analizach ryzyka;
- dane dotyczące administratorów danych, podmiotów przetwarzających oraz osób kontaktowych;

W przypadku zastosowania rozwiązania, w którym Wykonawca będzie przetwarzał dane osobowe w imieniu administratora, Zamawiający zawrze z Wykonawcą umowę powierzenia przetwarzania danych, o której mowa w art. 28 ogólnego rozporządzenia o ochronie danych- RODO.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706