

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie audytu zgodności systemów informatycznych wykorzystywanych w Powiatowym Urzędzie Pracy w Siedlcach z wymogami określonymi w RODO<sup>1</sup>.

Audyt dotyczy następujących systemów

- 1) Syriusz<sup>STD</sup> - dedykowany system teleinformatyczny wspomagający w sposób kompleksowy realizację statutowych zadań powiatowych urzędów pracy;
- 2) eDok - elektroniczny system obiegu dokumentów przeznaczony dla administracji publicznej;
- 3) Płatnik - system umożliwiający wysyłanie dokumentów ubezpieczeniowych do Zakładu Ubezpieczeń Społecznych w formie elektronicznej;
- 4) AssetsNinja - program do ewidencji środków trwałych oraz wyposażenia (STOCK);
- 5) Samorządowa Elektroniczna Platforma Informacyjna (SEPI) – system pozwalający na dwukierunkową wymianę informacji dotyczących klientów Urzędu z uprawnionymi podmiotami administracji publicznej;  
w zakresie ich użytkowania przez Zamawiającego.

Dane Zamawiającego niezbędne do przeprowadzenia audytu:

- 1) jedna lokalizacja;
- 2) liczba pracowników mających dostęp do systemów informatycznych: 60;
- 3) liczba wykorzystywanych stacji roboczych użytkowników: 60;
- 4) liczba serwerowni: 1;
- 5) liczba serwerów: 3 fizyczne i 11 wirtualnych;
- 6) liczba hostów IT: 3;
- 7) rodzaje najważniejszych usług sieciowych: DNS, FTP.

Zakres działań audytowych dla systemów podlegających audytowi:

- 1) Analiza i ocena bezpieczeństwa przetwarzania zgodnie z art. 32 RODO, w szczególności w zakresie:
  - rejestru ryzyka,
  - architektury bezpieczeństwa, w tym izolacji i separacji hostów - sieć, systemy wewnętrzne, punkty styku z zewnętrznymi systemami, LAN/WAN/DMZ/VPN,
  - bezpieczeństwa wirtualizacji,
  - kontroli dostępu do systemów, w tym przegląd uprawnień oraz kont użytkowników uprzywilejowanych,
  - monitorowania logów systemów,
  - zakresu rozliczalności operacji wykonywanych przez użytkowników w systemie,
  - poprawności procesu wprowadzania zmian,
  - szybkiego przywrócenia dostępności danych osobowych w systemach,
  - raportów z poprzednich audytów, w szczególności przeprowadzonych testów bezpieczeństwa,
  - kopii zapasowych i ich retencji oraz rotacji,
  - stosowania zasady 3-2-1,

---

<sup>1</sup> 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) (Dz. Urz. UE L 119 z 4.5.2016 r.)

- szyfrowania i pseudonimizacji,
  - zasad anonimizacji,
  - sposobów uwierzytelniania,
  - transferu danych pomiędzy systemami;
- 2) Analiza zasad wprowadzania zmian w systemach;
  - 3) Analiza odpowiedzialności za system;
  - 4) Weryfikacja przeprowadzonych analiz dla systemów zgodnie z art. 25 RODO oraz art. 35 RODO: DPIA oraz DPbDD;
  - 5) Weryfikacja wykonywania obowiązków związanych z przetwarzaniem danych osobowych w systemie zgodnie z: art. 13-22, 28, 30, 32, 33, 46 RODO.

Działania audytowe kończą się opracowaniem raportu z audytu, który winien zawierać:

- 1) Ocenę zgodności z właściwymi artykułami RODO;
- 2) Zalecenia w zakresie bezpieczeństwa i adekwatności zabezpieczeń stosowanych w odniesieniu do wrażliwości danych przetwarzanych w systemach zgodnie z zakresem audytu.

Zamawiający wymaga, aby działania audytowe wykonywane były w siedzibie Powiatowego Urzędu Pracy w Siedlcach.

Termin realizacji zamówienia: **do 30 listopada 2023 r.**