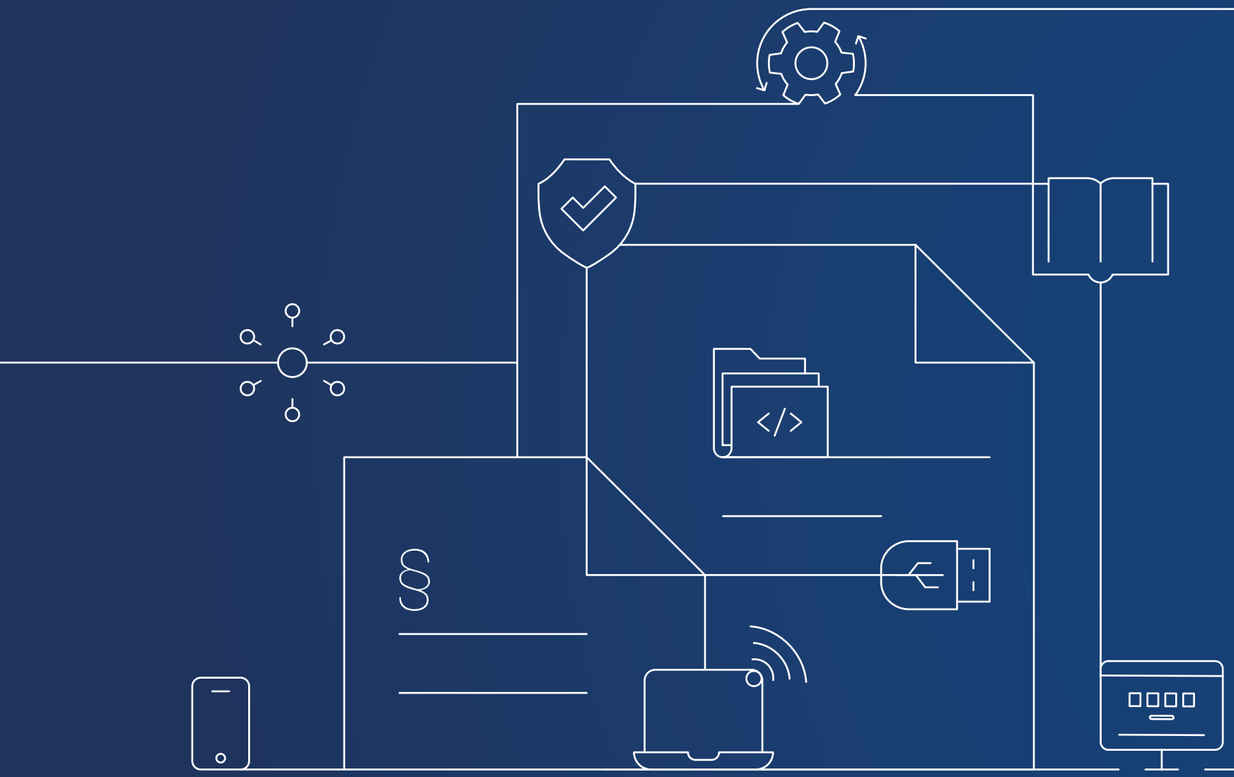
Cyberbezpieczny Samorząd



Vademecum bezpiecznych zakupów oprogramowania i rozwiązań IT

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
NASK
CENTRUM PROJEKTÓW POLSKA CYFROWA

Wstęp

Vademecum bezpiecznych zakupów oprogramowania i rozwiązań IT zostało przygotowane przez ekspertów z NASK-PIB i skierowane jest do osób odpowiedzialnych za zakupy w jednostkach samorządu terytorialnego. Jest to zbiór wskazówek i informacji jak w bezpieczny sposób przeprowadzić zakupy w projekcie Cyberbezpieczny Samorząd.

Opis Przedmiotu Zamówienia (OPZ) musi być zgodny z przepisami ustawy Prawo Zamówień Publicznych (PZP) w wersji aktualnie obowiązującej. Zgodnie z ustawą z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U.2023.1605 t.j.), OPZ jest dokumentem, który określa zakres i warunki zamówienia publicznego. Jest on kluczowy dla całego procesu, ponieważ to na jego podstawie wykonawcy przygotowują swoje oferty. Dlatego ważne jest, aby OPZ był prawidłowo sporządzony, aby zapewnić uczciwą konkurencję i wybór najkorzystniejszej oferty według określonych kryteriów.

W przypadku zamówień oprogramowania i rozwiązań IT, OPZ powinien zawierać następujące informacje:

01 **OPIS PRZEDMIOTU ZAMÓWIENIA** w tym jego zakres, funkcjonalność i wymagania techniczne

02 **WYMAGANIA** dotyczące jakości, bezpieczeństwa i niezawodności

03 **TERMINY REALIZACJI ZAMÓWIENIA**

04 **WYMAGANIA** dotyczące gwarancji i serwisu

Podczas tworzenia OPZ dla zamówień dot. oprogramowania i rozwiązań IT, należy pamiętać o zagrożeniach związanych z ujawnieniem wrażliwych informacji.

Poniżej przedstawiamy zagadnienia, na które należy zwrócić uwagę podczas przygotowania OPZ.

01 Dane dotyczące zakupu należy przekazywać w postaci sparametryzowanej, opisując dany produkt korzystając z parametrów technicznych oraz zachowując konkurencyjność;

02 W przypadku zakupów polegających na przedłużeniu wsparcia/licencjonowania należy jednoznacznie wskazać produkt wraz z okresem trwania usługi (zakres od – do), podając tylko niezbędne dane w przypadku przedłużania wsparcia;

03 Przy każdym postępowaniu należy przede wszystkim zrobić rozeznanie rynku ze wskazaniem na termin realizacji;

04 Postępowania należy przeprowadzać dzieląc na zakresy oraz etapy wdrażania projektu, co ułatwi rozliczalność zadań, jeżeli jest taka potrzeba;

05 Nie należy podawać jednoznacznie nazw własnych planowanych zakupów, aby uniknąć przypadku braku konkurencyjności;

06 Przy świadczeniu usług przez podmioty zewnętrzne należy bezwzględnie podpisać z takimi podmiotami oświadczenia o poufności oraz odpowiedzialności cywilnoprawnej wraz z odpowiedzialnością za poniesione szkody – w przypadku zaistnienia szkody;

07 W przypadku wyboru dostawcy/wykonawcy należy bezwzględnie wymagać poświadczeń w postaci certyfikatów oraz referencji potwierdzających doświadczenie w ramach świadczonych usług;

08 W przypadku wdrożeń należy utrzymać minimum 2 letni okres gwarancji na zakupione usługi;

09 W przypadku montażu dodatkowych źródeł zasilania należy pamiętać o dokumentacji powdrożeniowej oraz rejestracji dostępu w czasie prac do miejsc ograniczonego dostępu;

10 W przypadku zmiany w infrastrukturze należy wymagać dostarczenia dokumentacji w ramach wprowadzonych zmian;

11 Wymagania dotyczące realizacji zadań oraz usług wsparcia powinny być liczone w roboczogodzinach lub zakresie wykonania danego zadania i powinny zostać potwierdzane protokołem odbioru;

12 Każda realizacja zadania powinna opierać się o plan realizacji zaakceptowany obustronnie w formie dokumentu, dzięki czemu jasno i klarownie będzie znany zakres realizacji;

13 W przypadku zdarzeń losowych należy pamiętać o ubezpieczeniu sprzętu;

14 W przypadku wdrożenia generatorów prądu należy pamiętać o komplecie dokumentów jakie powinny być dostarczone w ramach realizacji zamówienia.

Ogólne zasady

Podczas sporządzania OPZ skorzystaj z poniższych zaleceń:

- **OPIS PRZEDMIOTU** zamówienia powinien być klarowny, jednoznaczny i zgodny z rzeczywistymi potrzebami instytucji;
- **UNIKAJ** ujawniania zbędnych szczegółów na temat aktualnych systemów i urządzeń, które mogłyby ułatwić dostęp do wrażliwych danych;
- **UNIKAJ** specyfikowania konkretnych rozwiązań i szczegółów dotyczących modeli sprzętu i oprogramowania używanego w Instytucji, aby nie ujawniać zbyt wielu informacji o aktualnym środowisku IT – te informacje (marki, modele, wersje oprogramowania, informacje o konfiguracji systemów bezpieczeństwa) mogą zostać wykorzystane przez przestępców przy typowaniu potencjalnego celu ataku – skup się na wymaganiach biznesowych, funkcjonalnych i wydajnościowych;
- **ZDEFINIUJ** minimalne wymagania dotyczące bezpieczeństwa, unikając ujawniania aktualnych braków w zabezpieczeniach;
- **ZAANGAŻUJ** specjalistów ds. bezpieczeństwa w proces tworzenia Opisu Przedmiotu Zamówienia;
- **REGULARNIE PRZEGLĄDAJ** i aktualizuj Opis Przedmiotu Zamówienia, aby uniknąć przypadkowego ujawnienia wrażliwych informacji;
- **ZWRÓĆ SZCZEGÓLNĄ UWAGĘ** na próby ataków socjotechnicznych, takich jak: fałszywe maile z prośbą o kliknięcie w link, szczegółowe pytania, które będą służyły wyłudzeniu danych, np. wskazanie osoby do kontaktu z działu IT. Mogą się pojawić prośby o umożliwienie wizji lokalnej w Urzędzie, które służą infiltracji pomieszczeń lub próbie pozyskania informacji o infrastrukturze;
- **NIE UDZIELAJ INFORMACJI** poprzez rozmowy telefoniczne, gdyż może okazać się, że zostaniemy posądzeni o brak zachowania zasad konkurencyjności lub ujawnimy dane, które nie powinny dostać się do obiegu publicznego;

Ogólne zasady

- **PRZY WYBIERANIU WYKONAWCÓW** przetargów zażądaj zabezpieczenia w postaci kar umownych z możliwością zerwania umowy w przypadku, gdy wykonawca nie wywiązuje się z umowy lub realizacja umowy jest niemożliwa;

- W przypadku, gdy usługa jest wdrażana, osoby wdrażające muszą posiadać do tego odpowiednie kwalifikacje potwierdzone **CERTYFIKATAMI** renomowanych firm z branży cyberbezpieczeństwa;

- W przypadku wdrażanej konfiguracji poprawiającej cyberbezpieczeństwo należy wymagać dostarczenia **DOKUMENTACJI** opisującej wprowadzone zmiany w oparciu o zalecenia, które zostaną opisane – należy podawać na podstawie czego zostały zmiany wprowadzone;

- **ZAMAWIAJ OPROGRAMOWANIE NOWE**, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych;

- **ZAMAWIAJ SPRZĘT,** który musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w np. styczniu 2023 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”;

- **ZAPISZ W DOKUMENTACJI** zakupowej możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u Producenta w przypadku wystąpienia wątpliwości co do jego legalności;

- **PRZY ZAMÓWIENIACH** w szczególności obejmujących świadczenie usług doradczych, wsparcia itp. podpisać z Wykonawcą umowę o poufności, która ograniczy ujawnianie na zewnątrz informacji dotyczących systemu i innych ważnych danych;

- Zgodnie z treścią **REGULAMINU KONKURSU GRANTOWEGO CYBERBEZPIECZNY SAMORZĄD** pamiętaj o warunkach udziału w postępowaniu:

  - **usługi wspomagające realizację Projektu,** w szczególności usługi doradcze podmiotów posiadających stosowne kwalifikacje i min. 2 letnie doświadczenie w prowadzeniu projektów z obszaru cyberbezpieczeństwa; oraz stosowne certyfikaty lub równoważne poświadczenia (np. kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia. Kwalifikowalność kosztów tylko w okresie realizacji Projektu;

  - **szkolenia:** zakup i organizacja szkoleń stacjonarnych lub/ i online dedykowanych dla pracowników JST zorganizowanych przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Kwalifikowalność kosztów tylko w okresie realizacji Projektu;

Ogólne zasady

- **PO WYKONANIU UMOWY** pamiętaj o usunięciu Wykonawcom dostępów do systemów IT;
- Pamiętaj o **ART. 133 UST. 3 USTAWY PZP** „Jeżeli zamawiający nie może udostępnić części SWZ na stronie internetowej prowadzonego postępowania z powodu ochrony poufnego charakteru informacji zawartych w SWZ, określa w ogłoszeniu o zamówieniu sposób dostępu do tych informacji oraz wymagania związane z ochroną ich poufnego charakteru”.
- **WYMAGAJ** od Wykonawców certyfikatów potwierdzających kwalifikacje;
- **KONTROLUJ** stan zamówienia na stronie producenta;
- **GDY ODNAWIASZ WSPARCIE**, pamiętaj, że gdy niezbędne jest zachowanie ciągłości, podaj w OPZ nr licencji, nazwę użytkownika i wskaż, że wsparcie ma być świadczone przez np. 24 miesiące od daty wygaśnięcia wsparcia;
- **NIE PRZEKAZUJ INFORMACJI** na temat wyników audytów w zakresie bezpieczeństwa, diagnoz bezpieczeństwa bez podpisanej umowy/ klauzuli o poufności;
- **UNIKAJ** opisywania docelowych lokalizacji instalacji urządzeń m.in. numeru pokoju, adresu danej instalacji;
- **PAMIĘTAJ**, żeby określić czas reakcji na zgłoszenie oraz maksymalny czas realizacji zgłoszenia (SLA);
- Na etapie postępowania **WERYFIKUJ** listę osób i podmiotów objętych sankcjami:

  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006R0765-20230805

  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0269-20230915

  https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami

  https://crbr.podatki.gov.pl/adcrbr/#/wyszukaj
- **PODZIEL ZAMÓWIENIE** na części ze względów ekonomicznych, technicznych, organizacyjnych.

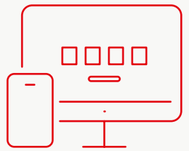
Aktualizacje i wsparcie

01 Wymagaj, aby oferowane oprogramowanie i sprzęt były regularnie aktualizowane i wspierane przez dostawcę (najlepiej certyfikowanego) przez wskazany czas planowanego wykorzystania produktu – np. wsparcie techniczne producent przez okres X;

02 W każdym przypadku, w którym producent oprogramowania udostępni jakiekolwiek aktualizacje, nowe wersje, poprawki, zmiany itp. dotyczące oprogramowania, wymagaj, by Wykonawca zapewnił takie aktualizacje niezwłocznie po ich udostępnieniu;

03 Reaguj i natychmiastowo wdrażaj dostępne aktualizacje w celu utrzymania odpowiedniego poziomu bezpieczeństwa;

04 Warto rozważyć, aby usługa wsparcia Producenta/Wykonawcy umożliwiała zakładanie spraw serwisowych w reżimie 24/7/365 oraz umożliwiała zgłaszanie problemów za pośrednictwem różnych kanałów łączności np. telefonu, wiadomości e-mail oraz dedykowanej strony internetowej.



Bezpieczna konfiguracja i zarządzanie dostępem

01 Wymagaj, aby dostawca sprzętu i oprogramowania stosował najlepsze praktyki i standardy związane z konfiguracją pod kątem bezpieczeństwa (m.in. *uwierzytelnianie dwuskładnikowe*, *zero-trust* itp.) w miarę możliwości potwierdzoną certyfikatami;

02 Zdefiniuj wymagania dotyczące zarządzania dostępem do systemu, danych, infrastruktury. Weź pod uwagę zakres dostępu Wykonawcy do twojej sieci).

Zgodność z normami bezpieczeństwa i wymaganiami prawnymi

01 Stosuj zgodność rozwiązań oferowanych przez Wykonawcę/Dostawcę z odpowiednimi standardami i normami bezpieczeństwa zarządzania informacją i ochroną danych przetwarzanych danych osobowych (RODO) – polityka prywatności, np. ISO (ISO-9001 oraz ISO-14001 lub równoważne w zakresie co najmniej produkcji, projektowania lub rozwoju urządzeń; deklaracja zgodności CE lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym);

02 Wykonawca musi stale utrzymywać i certyfikować bezpieczeństwo swojego systemu oraz jego bazy danych poprzez zgodność z normami z zakresu cyberbezpieczeństwa).

Testy bezpieczeństwa

Wymagaj, aby dostawca dostarczył dokumentację przeprowadzonych testów bezpieczeństwa dla oferowanego oprogramowania wraz z obustronnie podpisanymi protokołami odbioru.

Dokumentacja użytkowa

Wymagaj, aby Wykonawca przygotował i dostarczył dokumentację użytkową oferowanego systemu/oprogramowania, aby administratorzy/użytkownicy mogli w sposób właściwy z niego korzystać.

Przedmiotowe środki dowodowe

Pamiętaj o uwzględnieniu tego zapisu. Przedmiotowe środki dowodowe służą zawsze potwierdzeniu zgodności oferowanego rozwiązania z OPZ. Wykonawca będzie obowiązany dostarczyć dowody spełniania wymogów zawartych w dokumentacji.

Opisanie skuteczności rozwiązania w raportach.

Skuteczność systemu powinna być opisana i sklasyfikowana w publicznie dostępnych raportach i analizach.

Techniczne aspekty podnoszące cyberbezpieczeństwo

01 W przypadku opisu dotyczącego dostępu do systemu miej na uwadze, iż powinien być on możliwy jedynie poprzez MFA oraz kanały szyfrowane jak HTTPS, VPN, lub równoważne, zapewniające poufność przesyłanych danych;

02 W sytuacji jeśli System/oprogramowanie oferuje możliwość dedykowanego dostępu do programowalnego interfejsu API, dostęp API do Systemu powinien być zabezpieczony kryptograficznie przynajmniej protokołem SSL/TLS (w tym przypadku należy uwzględnić również szereg innych zabezpieczeń związanych z przesyłaniem danych).

Integracja

01 Pamiętaj o uwzględnieniu właściwej integracji oprogramowania/systemu z obecnym, tak aby nie narazić Instytucji na wyciek danych czy luki w systemie bezpieczeństwa;

02 Integracje powinny być realizowane w sposób zaplanowany oraz zgodny z normami bezpieczeństwa ograniczający wyciek informacji.

Uwagi końcowe

W przypadku wątpliwości zachęcamy do skonsultowania się z ekspertami ds. bezpieczeństwa IT podczas tworzenia opisu przedmiotu zamówienia lub szczegółowych wymogów zamówienia, aby zapewnić, że wszelkie aspekty związane z bezpieczeństwem systemów i użytkowników w organizacji są należycie uwzględnione.

W procesie opracowania OPZ zachęcamy również do zapoznania się z Rekomendacjami dotyczącymi zamówień publicznych na systemy informatyczne – Urząd Zamówień Publicznych (uzp.gov.pl)

https://www.uzp.gov.pl/baza-wiedzy/dobre-praktyki/rekomendacje-dotyczace-zamowien-publicznych-na-systemy-informatyczne

Cyberbezpieczny Samorząd

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

NASK

CENTRUM PROJEKTÓW POLSKA CYFROWA