Fundusze Europejskie

Jak kupować bezpieczne rozwiązania elektroniczne w postępowaniach o udzielenie zamówienia publicznego?

Piotr Pieprzyca

Warszawa, 7 września 2026

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Zakres zagadnień

1. Czy osoby przygotowujące dokumenty zamówienia od strony formalnoprawnej muszą być informatykami?
2. Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?
3. W jakim zakresie warunków zamówienia będzie przeprowadzana analiza zapisów dotyczących cyberbezpieczeństwa?
4. Czy przesłanki odrzucenia oferty w zakresie cyberbezpieczeństwa wymagają szczególnych zapisów w dokumentach zamówienia?
5. Jak oceniać oferty w zakresie wymogów cyberbezpieczeństwa?
6. Jak ważna jest procedura odbiorowa przedmiotu zamówienia i czy cyberbezpieczeństwo kończy się wraz z podpisaniem protokołu odbioru?

Czy osoby przygotowujące dokumenty zamówienia od strony formalnoprawnej muszą być informatykami?

Osoby zajmujące się zamówieniami publicznymi wiedzą wszystko?

Co oznaczają skróty: **SOC, SIEM, EDR, XDR, MFA, RTO czy RPO**?

Jak skonfigurować **firewall**?

Jaki **algorytm szyfrowania** powinien zostać zastosowany?

Osoby zajmujące się zamówieniami publicznymi wiedzą wszystko w zakresie zamówień publicznych

Osoby te powinny wiedzieć

- **jakich informacji** potrzebują od osób merytorycznych,
- **jakie pytania powinny im zadać i**
- **jak** uzyskane **odpowiedzi przełożyć na dokumenty zamówienia** określając warunki zamówienia

Osoby zajmujące się zamówieniami publicznymi wiedzą wszystko w zakresie zamówień publicznych

Wiedza będzie potrzebna do:

- określenia wymagań w ramach warunków zamówienia
- przewidzenia odpowiedniej weryfikacji ofert
- podpisania umowy, która uwzględnia ryzyka związane z cyberbezpieczeństwem

Nie wystarczy wpisać w dokumenty zamówienia zdania:

Oferowany system musi być zgodny z wymaganiami cyberbezpieczeństwa

Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?

Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?

Typowy stan faktyczny:

do komórki zamówień publicznych przychodzi kolega z IT i mówi:

- musimy kupić system cyberbezpieczeństwa
- potrzebujemy nowych firewalli
- realizujemy projekt i musimy kupić serwery, backup

Jaką otrzymuje odpowiedź?

Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?

Dostajemy np. 60-stronicowy dokument (OPZ), z którego niewiele rozumiemy (nie jesteśmy informatykami), po przeczytaniu warto zadać kilka pytań:

- **do kiedy działa** nasze obecne rozwiązanie
- **co się stanie, gdy nie zdążymy wdrożyć** nowego w założonym terminie lub nowe rozwiązanie nie zadziała prawidłowo po tygodniu od wdrożenia
- **jakiego rodzaju informacje będą przetwarzane**
- **kto będzie miał dostęp** do systemu
- **jak długo ma on funkcjonować**
- **od kogo będziemy zależni** po podpisaniu umowy

Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?

Nie można bezrefleksyjnie przyjmować każdego wymagania przekazanego przez komórkę IT

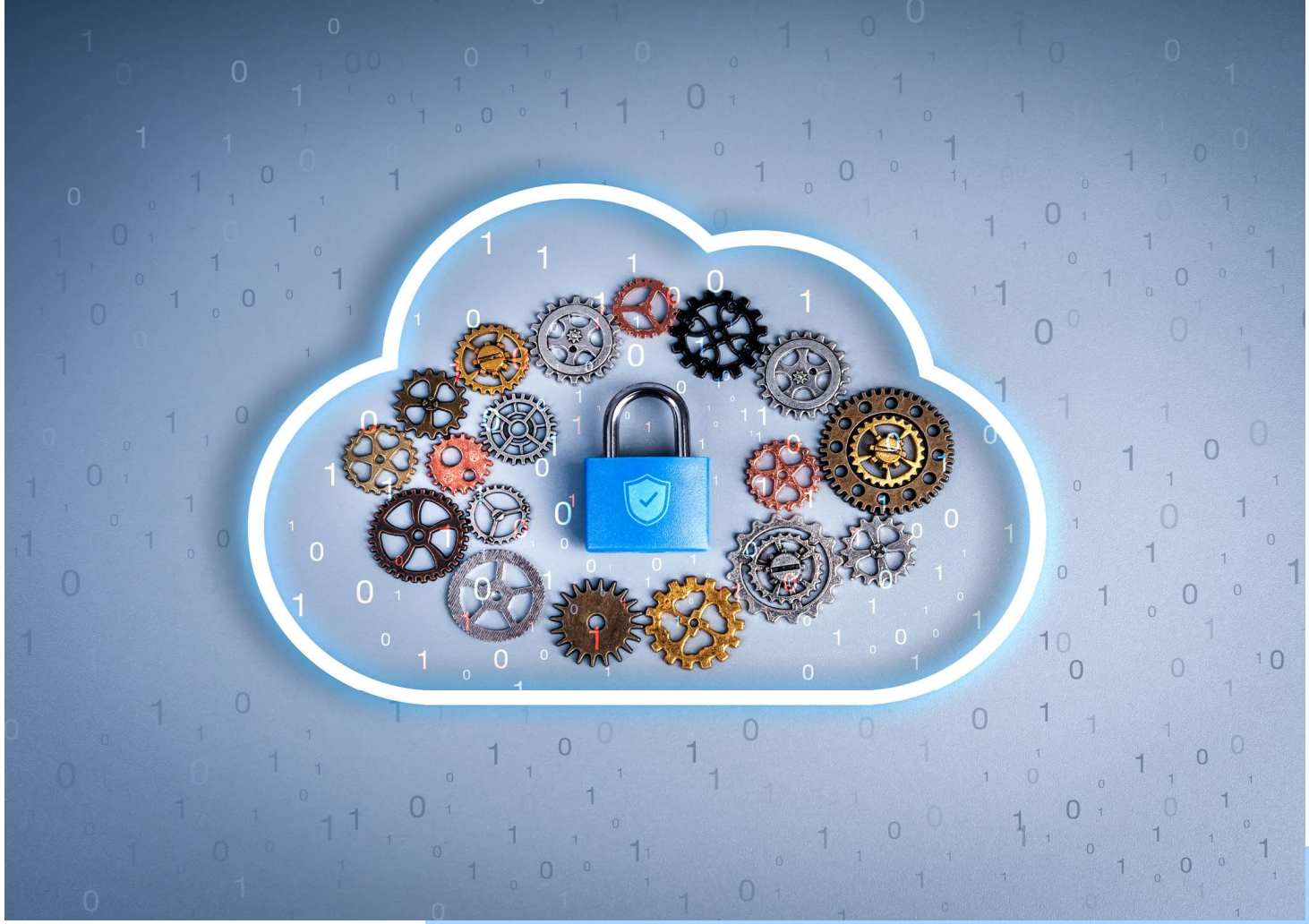
W OPZ znajdujemy:

- konkretną technologię,
- bardzo szczegółowe parametry,
- konkretny certyfikat,
- określoną liczbę ekspertów,
- wymagane doświadczenie,
- regulacje dotyczące gwarancji, odbiorów, zmian technologii

Czy przed przygotowaniem SWZ koniecznie należy przeczytać OPZ?

Komórka **IT nie musi wiedzieć**:

- czy wymaganie jest proporcjonalne w rozumieniu Pzp,
- czy może ograniczać konkurencję,
- czy powinno być warunkiem udziału,
- czy powinno być wymaganiem przedmiotowym,
- czy może być kryterium oceny ofert,
- czy powinno znaleźć się dopiero w umowie.



W jakim zakresie warunków zamówienia będzie przeprowadzana analiza zapisów dotyczących cyberbezpieczeństwa?

Warunki zamówienia dotyczące cyberbezpieczeństwa

1. opis przedmiotu zamówienia
2. przedmiotowe środki dowodowe
3. termin realizacji
4. warunki udziału w postępowaniu
5. kryteria oceny ofert
6. obowiązki umowne

Opis przedmiotu zamówienia

Parametry wskazane w OPZ powinny być traktowane jako:

- precyzyjne wymaganie
- docelowe albo minimalne/maksymalne wymaganie
- podstawa weryfikacji złożonej oferty

Jakie konsekwencje poniesie wykonawca, jeżeli oferowane rozwiązanie nie będzie zgodne z OPZ?

Przedmiotowe środki dowodowe

1. Etykiety
2. Certyfikaty
3. Inne przedmiotowe środki dowodowe

*Skoro zamawiający nie ma pełnej wiedzy technicznej, może warto oprzeć się na certyfikacie – np. określony certyfikat ISO albo certyfikat potwierdzający kompetencje osoby

Przedmiotowe środki dowodowe

Co dokładnie certyfikat ma potwierdzić:

- sposób organizacji działalności wykonawcy
- kompetencje konkretnej osoby
- właściwość produktu
- jakość określonej usługi
- sposób zarządzania bezpieczeństwem

Jeżeli zadamy wyłącznie pytanie, jakiego certyfikatu należy zażądać – pewnie otrzymamy odpowiedź… nie wiedząc, czemu ma on tak naprawdę służyć

Przedmiotowe środki dowodowe

SCHEMAT tworzenia zapisów

- nazwa przedmiotowego środka dowodowego
- co ma potwierdzać
- czy jest związany z kryterium oceny ofert
- czy podlega uzupełnieniu
- w jakiej formie i kiedy będzie wymagany

Certyfikat nie powinien być celem samym w sobie

Jest środkiem służącym potwierdzeniu określonej cechy lub zdolności.

Termin realizacji

Przedstawiany jest zawsze jako dwie podstawowe informacje:

- **od kiedy** rozwiązanie z zakresu cyberbezpieczeństwa ma działać?
- na **jak długo** będzie zawarta umowa?

Dodatkowo...

- **etapowanie** realizacji
- co stanie się po wygaśnięciu umowy?

Warunki udziału w postępowaniu

Zdolność techniczna lub zawodowa

- **doświadczenie** w podobnych wdrożeniach

doświadczenie obejmujące co najmniej dwa (2) wdrożenia obejmujące rozbudowę środowiska IT szpitala o elementy sprzętowe i programowe związane z podniesieniem poziomu cyberbezpieczeństwa wraz z dostawą urządzeń oraz usługami wsparcia lub równoważnymi wdrożeniami o wartości co najmniej ... zł brutto każde

Warunki udziału w postępowaniu

Zdolność techniczna lub zawodowa

- **specjaliści** posiadający określone doświadczenie/kompetencje

dysponowanie co najmniej 1 osobą posiadającą doświadczenie wdrożeniowe w obszarze IT obejmujące wdrożenie, integrację i rozbudowę środowiska IT o elementy sprzętowe i programowe związane z podniesieniem poziomu cyberbezpieczeństwa wraz z dostawą urządzeń oraz usługami wsparcia lub równoważnymi wdrożeniami, która uczestniczyła na tym stanowisku w co najmniej 2 projektach obejmujących wdrożenie i integrację rozwiązań sprzętowo-programowych w zakresie cyberbezpieczeństwa w ostatnich 5 latach.

Kryteria oceny ofert

Kryterium powinno służyć premiowaniu wartości dodanej ponad wymagane minimum

Zamawiający uznaje, że maksymalny dopuszczalny czas reakcji na incydent krytyczny wynosi **60 minut**. To jest **minimum**.

Ale można rozważyć **przyznanie punktów**:

- 60 minut – 0 punktów,
- 30 minut – dodatkowe punkty,
- 15 minut – jeszcze więcej punktów.

Kryteria oceny ofert

Wsparcie

Minimum: 5 lat.

Premiowanie: 6 albo 7 lat.

Dodatkowe doświadczenie osób ponad wymogi warunku udziału w postępowaniu (podobny mechanizm)

Czy ta dodatkowa jakość rzeczywiście ma wartość dla zamawiającego?

Premiujemy takie cechy, które realnie poprawiają jakość albo bezpieczeństwo realizacji

Obowiązki umowne

Należy pamiętać o następujących obowiązkach:

- obowiązek **informowania o incydencie**,
- **współpraca** z zamawiającym podczas incydentu,
- **monitorowanie podatności**,
- instalowanie **aktualizacji oprogramowania**,
- **aktualizowanie** dokumentacji,
- zgłaszanie istotnych zmian dotyczących podwykonawców,
- **pomoc przy migracji danych po zakończeniu umowy**.

Czy przesłanki odrzucenia oferty w zakresie cyberbezpieczeństwa wymagają szczególnych zapisów w dokumentach zamówienia?

Przesłanki odrzucenia oferty

Zamawiający odrzuca ofertę, jeżeli:

obejmuje ona produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;

(art. 226 ust. 1 pkt 17 Pzp)

https://dane.gov.pl/pl/dataset/20102,rekomendacje-pelnomocnika-rzadu-ds-cyberbezpieczenstwa/resource/897674/table?page=1&per_page=20&q=&sort=

Są już opublikowane rekomendacje Pełnomocnika — każdorazowo trzeba sprawdzić ich zakres

Przesłanki odrzucenia oferty

Zamawiający odrzuca ofertę, jeżeli:

- obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub usługę ICT, lub proces ICT, określone w tej decyzji.

(art. 226 ust. 1 pkt 19 Pzp)

https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---procedura-dot-listy-dostawcow-wysokiego-ryzyka

Jeszcze nie ma takich dostawców

Przesłanki odrzucenia oferty

Co musi zrobić zamawiający:

1. **przeanalizować OPZ** pod kątem ICT (osoby merytoryczne odpowiedzialne za OPZ)
2. **przygotować odpowiednie postanowienia SWZ i załączniki do SWZ (narzędzie do weryfikacji)**
3. **zażądać od wykonawców**
   - **odpowiedniego opisu, danych technicznych lub wykazu urządzeń** objętych ofertą oraz
   - **oświadczenia wykonawcy**

   zamawiający musi mieć narzędzie do weryfikacji przesłanek odrzucenia oferty

Przesłanki odrzucenia oferty

4. Sprawdzić wykaz/oświadczenie wykonawcy

Wykaz rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

https://dane.gov.pl/pl/dataset/20102,rekomendacje-pelnomocnika-rzadu-ds-cyberbezpieczenstwa/resource/897674/table?page=1&per_page=20&q=&sort=

UWAGA NA UMOWĘ

- zmiany rekomendacji
- zmiany produktów zaoferowanych przez wykonawcę

Jak oceniać oferty w zakresie wymogów cyberbezpieczeństwa?

Weryfikacja oferty

Wykonawca nie musi w treści składanej oferty wprost potwierdzać wszystkich wymagań OPZ:

- Backup – TAK.
- Szyfrowanie – TAK.
- Eksport logów – TAK.
- Aktualizacje – TAK.
- (...)

Do tego... dziesiątki dokumentów potwierdzających postawione wymagania

Weryfikacja oferty

Każdy dodatkowy dokument:

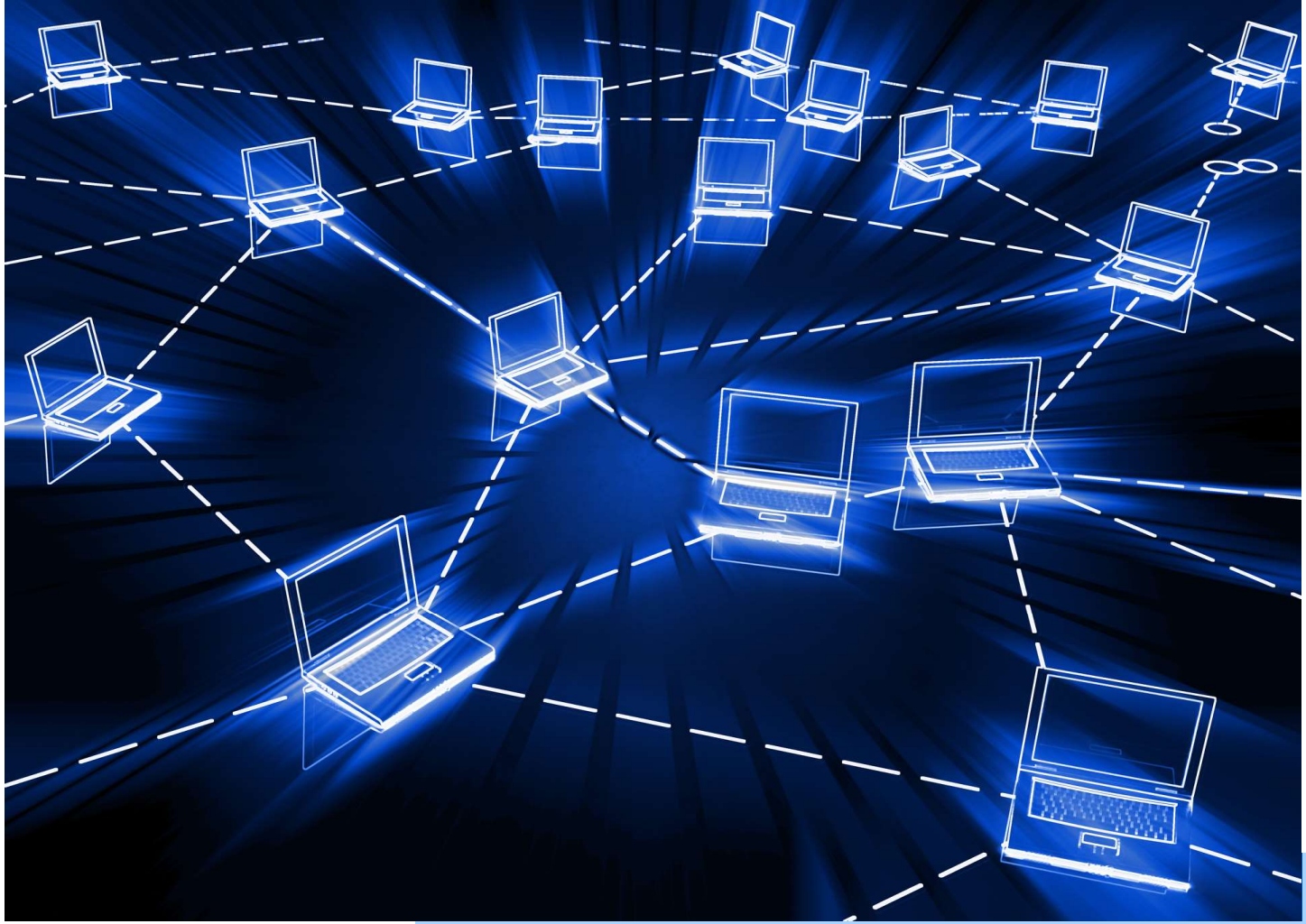
- zwiększa **obciążenie wykonawców**,
- zwiększa **ryzyko błędów**,
- zwiększa **nakład pracy zamawiającego**,
- **może wpływać na konkurencyjność** postępowania.

Weryfikacja oferty

Zastanówmy się, które pięć albo dziesięć wymagań jest dla nas naprawdę krytycznych i których nie chcemy pozostawić wyłącznie na poziomie deklaracji wykonawcy

Wyłącznie **w takim zakresie wymagajmy** wskazania konkretnych **parametrów** i **dokumentów**, które je potwierdzają

*dokumentacja producenta, karta techniczna, raport, certyfikat, próbka, test.



Jak ważna jest procedura odbiorowa przedmiotu zamówienia i czy cyberbezpieczeństwo kończy się wraz z podpisaniem protokołu odbioru?

Procedura odbiorowa

Wzór protokołu podsumowuje odbiór w następujący sposób:

„Przedmiot umowy został wykonany zgodnie z umową”

Warto przewidzieć różne **TESTY**:

- Jeżeli wymagamy backupu – można wykonać test odtworzenia.
- Jeżeli wymagamy eksportu logów – można wygenerować określone zdarzenie i sprawdzić, czy zostało przekazane.
- Jeżeli wymagamy redundancji – można przeprowadzić test awarii komponentu.
- Jeżeli wymagamy określonego czasu odtworzenia – można zweryfikować procedurę.

Procedura odbiorowa

Ważne, aby:

- **test był przewidziany** w dokumentach zamówienia,
- **wykonawca wiedział o nim** przed złożeniem oferty,
- **kryteria jego zaliczenia były określone**,
- **wynik testu miał konsekwencje** dla odbioru.

Podpisanie protokołu odbioru – czy to koniec umowy?

W przypadku systemów ICT:

- system może być bezpieczny w dniu odbioru.
- dwa miesiące później może zostać ujawniona krytyczna podatność.

Podatności

- czy wykonawca ma obowiązek je monitorować?
- kiedy ma poinformować zamawiającego?
- jak szybko ma podjąć działania?
- co, jeżeli producent jeszcze nie udostępnił poprawki?

Podpisanie protokołu odbioru – czy to koniec umowy?

Aktualizacje

- kto je instaluje?
- czy instalacja jest objęta wynagrodzeniem?
- czy wykonawca najpierw testuje aktualizację?
- co, jeżeli aktualizacja spowoduje problem z kompatybilnością?

Incydenty

- kiedy wykonawca ma poinformować zamawiającego?
- kto jest punktem kontaktowym?
- jakie informacje ma przekazać?
- czy ma obowiązek współpracować przy analizie incydentu?

Podpisanie protokołu odbioru – czy to koniec umowy?

Zakończenie wsparcia

- co dzieje się, kiedy producent przestaje wspierać produkt?
- czy wykonawca ma nas wcześniej poinformować?
- czy ma zaproponować rozwiązanie zastępcze?

Podwykonawcy

- czy wykonawca może swobodnie zmienić podmiot odpowiedzialny za kluczową usługę?
- czy powinien nas o tym poinformować?

Podpisanie protokołu odbioru – czy to koniec umowy?

Wyjście z systemu

- czy otrzymamy wszystkie dane?
- w jakim formacie?
- czy nowy wykonawca będzie mógł je przejąć?
- jak długo poprzedni wykonawca będzie pomagał w migracji?
- kiedy usunie dane ze swoich systemów?
- jak to potwierdzi?

Fundusze Europejskie

Dziękuję za uwagę

Piotr Pieprzyca