

Nr sprawy: PZP2/2016

Załącznik nr 3 do Umowy w sprawie udzielenia zamówienia publicznego o świadczenie kompleksowej usługi na wydruk, konfekcjonowanie oraz wysyłkę imiennych zaproszeń na badania mammograficzne

PROCEDURA PRZEKAZANIA I SZYFROWANIA DANYCH

I. Procedura przekazania danych

1. W celu realizacji Umowy nr Zamawiający będzie przekazywał Wykonawcy bazę/y danych w następującej formie:
 - a) w postaci zaszyfrowanej elektronicznej na adres(-y) e-mail:
2. Niezależnie od formy przekazania baz/y danych, określonej w pkt. 1 niniejszego załącznika, przekazywanie odbywać się będzie z wykorzystaniem metod gwarantujących bezpieczeństwo baz/y danych tzn.:
 - a) poprzez szyfrowanie baz/y danych przekazywanych w pliku PDF,
 - b) kluczem **programu PGP** wraz z podpisem zaszyfrowanej paczki przez nadawcę, zgodnie z pkt. II załącznika nr 3 do Umowy - „Instrukcja szyfrowania i użytkowania kluczy kryptograficznych PGP”,
 - c) innym sposobem szyfrowania, po wcześniejszym uzgodnieniu z Wykonawcą (zasady będą określone przez Strony i będą stanowiły załącznik do Umowy).
3. Szyfrowanie, o którym mowa odbywać się będzie z wykorzystaniem programu PGP lub innego, po wcześniejszym uzgodnieniu z Wykonawcą.

II. Instrukcja szyfrowania i użytkowania kluczy kryptograficznych PGP

1. W celu przekazania do Wykonawcy baz/y danych zaszyfrowanych kluczem PGP należy wykonać niżej określone kroki (kroki a-d wykonujemy przy pierwszej instalacji kluczy lub po ich wymianie):
 - a) wygenerować przy pomocy zainstalowanego narzędzia:
 - klucz prywatny – służący do szyfrowania danych,
 - klucz publiczny – służący do deszyfrowania danych,
 - b) wygenerowany klucz publiczny przekazać do Wykonawcy na adres e-mail osoby odpowiedzialnej za komunikację w zakresie kontaktów związanych z zasadami szyfrowania baz danych wskazanej w pkt. III załącznika nr 3 do Umowy – „Lista osób upoważnionych” (klucz służący do deszyfrowania danych przez Wykonawcę), przekazać do Wykonawcy innym kanałem komunikacyjnym odcisk klucza, np. za pomocą faxu,

Nr sprawy: PZP2/2016

Załącznik nr 3 do Umowy w sprawie udzielenia zamówienia publicznego o świadczenie kompleksowej usługi na wydruk, konfekcjonowanie oraz wysyłkę imiennych zaproszeń na badania mammograficzne

- c) odebrać klucz publiczny otrzymany poprzez e-mail z Wykonawcą i zainstalować na komputerze (klucz służący do deszyfrowania danych z Wykonawcą) – *krok konieczny do wykonania tylko w przypadku gdy Wykonawca przekazywał będzie do klienta dane zawierające dane osobowe, odebrać od Wykonawcy innym kanałem komunikacyjnym odcisk klucza, np. za pomocą faxu,*
 - d) po wykonaniu prawidłowej instalacji klucza publicznego zweryfikować poprawność zainstalowanych kluczy poprzez weryfikację odcisku klucza otrzymanego z zainstalowanym,
 - e) zaszyfrować, przy użyciu klucza Wykonawcy bazy danych planowane do przesłania do Wykonawcy z jednoczesnym podpisaniem szyfrogramu kluczem własnym,
 - f) przekazać zaszyfrowane dane do Wykonawcy w ustalonej formie.
2. Zasady użytkowania kluczy kryptograficznych:
- a) Klucze kryptograficzne będą zabezpieczone przed przypadkowym dostępem osób nieupoważnionych poprzez nałożenia hasła na klucz prywatny (długość hasła minimum 8 znaków, hasło składa się co najmniej z jednej wielkiej i małej litery oraz co najmniej jednej cyfry lub znaku specjalnego).
 - b) Dostęp do kluczy kryptograficznych będą miały tylko upoważnione osoby Stron. Każda ze Stron prowadzi ewidencję osób upoważnionych do dostępu do kluczy kryptograficznych.
 - c) Czas użytkowania kluczy kryptograficznych wynosi maksymalnie 2 lata.
 - d) Klucze kryptograficzne będą użytkowane do chwili, gdy zaistnieje podejrzenie ich kompromitacji lub do upływu okresu ich ważności.
 - e) Kompromitację kluczy kryptograficznych należy zgłosić wyznaczonym osobom natychmiast po ujawnieniu tego faktu w sposób zapewniający rozliczalność zgłaszającego np. wysyłając wiadomość elektroniczną na adres e-mail osoby odpowiedzialnej za komunikację w zakresie kontaktów związanych z zasadami szyfrowania baz danych wskazanej w pkt. III załącznika nr 3 do umowy – „Lista osób upoważnionych”.
 - f) Strony niezwłocznie wzajemnie powiadamiają się o zmianie adresów, na które należy zgłaszać kompromitację kluczy kryptograficznych.
 - g) W razie podejrzenia kompromitacji kluczy kryptograficznych nie można używać skompromitowanych kluczy kryptograficznych do szyfrowania i przekazywania danych oraz należy niezwłocznie wygenerować i przekazać drugiej Stronie nowe klucze kryptograficzne.
 - h) Zmiana kluczy kryptograficznych będzie poprzedzona każdorazowo pisemnym powiadomieniem i odbywać się będzie zgodnie z zasadami opisanymi w Załączniku Instrukcja szyfrowania i użytkowania kluczy kryptograficznych PGP.
3. Strony zobowiązują się wykorzystywać klucze kryptograficzne tylko w celu realizacji przedmiotu Umowy.

Nr sprawy: PZP2/2016

Załącznik nr 3 do Umowy w sprawie udzielenia zamówienia publicznego o świadczenie kompleksowej usługi na wydruk, konfekcjonowanie oraz wysyłkę imiennych zaproszeń na badania mammograficzne

III. Lista osób upoważnionych

1. Lista osób upoważnionych ze strony Zamawiającego do kontaktów z Wykonawcą w zakresie przekazywania i szyfrowania danych:

lp.	Imię i nazwisko/ jednostka organizacyjna	Zakres komunikacji	telefon	e-mail
1		Kontakty związane z zasadami szyfrowania baz danych		
2		Przekazanie bazy danych		

2. Lista pracowników ze strony Wykonawcy upoważnionych do kontaktów z Zamawiającym w zakresie przekazywania i szyfrowania danych:

lp	Imię i nazwisko, struktura/jednostka/komórka organizacyjna	Zakres komunikacji	telefon	e-mail
1		Kontakty związane z zasadami szyfrowania baz danych		
2		Odbiór bazy danych		

3. Strony niezwłocznie wzajemnie powiadamiają się o zmianie osób upoważnionych do kontaktów w zakresie realizacji Umowy.
4. Zmiana osób upoważnionych do kontaktów w zakresie realizacji Umowy nie wymaga sporządzenia aneksu. Strona inicjująca zmiany zobowiązana jest przekazać drugiej Stronie nowe dane na piśmie.