Fundusze Europejskie
Polska Cyfrowa

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego

Grant w projekcie „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21,
współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego, Program Operacyjny Polska Cyfrowa (POPC) na lata 2014-2020, pakiet REACT-UE
Umowa o powierzenie grantu o numerze 3223/1/2021

UMOWA O WSPÓŁPRACY

zawarta w Jastrzębiu-Zdroju z dnia 07.06.2023 r.
pomiędzy:

Sylwią Kochman prowadzącą jednoosobową działalność gospodarczą pod firmą **ISO-LEX Sylwia Kochman**, zarejestrowaną w Centralnej Ewidencji i Informacji o Działalności Gospodarczej o nr NIP: 6511654906 oraz o nr regon: 241720845 z siedzibą przy ul. Podhalańskiej 31 w Jastrzębiu-Zdroju, 44-335 Jastrzębie-Zdrój

zwaną dalej **Zleceniobiorcą**,
a

Nazwa organizacji:	**Gmina Kędzierzyn-Koźle**
Adres organizacji:	**ul. Piramowicza 32 47-200 Kędzierzyn-Koźle**
NIP organizacji:	**7492055601**
reprezentowaną przez:	**Prezydenta Miasta Kędzierzyn-Koźle - Sabinę Nowosielską**

zwanym dalej **Zleceniodawcą**, o następującej treści:

§ 1. PRZEDMIOT UMOWY

1. Zleceniodawca zleca, a Zleceniobiorca dokona audytu dokumentacji SZBI pod względem technicznym i formalno-prawnym oraz szacowania ryzyka polegające na:
   1) przeprowadzenie audytu zdalnego na zgodność w zakresie Krajowych Ram Interoperacyjności w obszarze wskazanym przez Ministerstwo Cyfryzacji tj.: „zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych" w oparciu o Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".
   2) przeprowadzenia audytu zdalnego z zakresu bezpieczeństwa informacji w oparciu o *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE.*
   3) przygotowania Oceny Skutków dla Ochrony Danych (DPIA) oraz analizy ryzyka ogólnego zgodnie z art. 35 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.* w oparciu o wskazane w § 1 ust. 1 pkt 2 normy międzynarodowe ISO oraz wytyczne Grupy Roboczej art. 29.

2. **Zlecenie, o którym mowa § 1 ust. 1 pkt 1 obejmuje w szczególności:**
   1) Audyt procesów zapewniających szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
      a) zagrożenia bezpieczeństwa informacji,
      b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
      c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
   2) Audyt ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, pod kątem:
      a) monitorowania dostępu do informacji,
      b) czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
      c) zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
   3) Audyt ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
   4) Audyt zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
   5) Audyt umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji
   6) Audyt zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
   7) Audyt odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
      a) dbałości o aktualizację oprogramowania,
      b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
      c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
      d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
      e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

8) Audyt poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.
9) Audyt komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
10) Audyt ciągłości wykonywania audytu wewnętrznego.
11) Audyt występowania dodatkowych zabezpieczeń, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne.
12) Audyt prowadzenia / występowania dzienników systemowych odnotowujących działania użytkowników lub obiektów systemowych, polegających na dostępie do:
    a) systemu z uprawnieniami administracyjnymi,
    b) konfiguracji systemu, w tym konfiguracji zabezpieczeń,
    c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
13) Audyt występowania procedur mogących stanowić odnotowywanie działań użytkowników lub obiektów systemowych, a także innych zdarzeń związanych z eksploatacją systemu w postaci:
    a) działań użytkowników nieposiadających uprawnień administracyjnych,
    b) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
    c) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.
14) Audyt procedur związanych z dziennikami systemowymi.

3. **Zlecenie, o którym mowa § 1 ust. 1 pkt 2 obejmuje w szczególności:**

1) Audyt polityk ochrony danych osobowych wprowadzonych/stosowanych przez organizację (w kontekście uwzględnienia atrybutu poufności, dostępności i integralności)
2) Weryfikacja: czynności przetwarzania danych/kategorii czynności przetwarzania, kategorii przetwarzanych danych
3) Weryfikacja klauzul informacyjnych w zakresie przetwarzania danych (weryfikacja ich treści, sposobu ich spełniania)
4) Weryfikacja przyjętych regulacji w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrona danych
5) Weryfikacja stosowanego wzoru umowy powierzenia przetwarzania danych oraz audyt wprowadzonych do obiegu umów powierzenia przetwarzania danych osobowych
6) Audyt działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji
7) Weryfikacja przyjętych regulacji w zakresie zarządzania naruszeniem - audyt komunikowania naruszeń bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań naprawczych
8) Weryfikacja zarządzania ryzykiem w kontekście ryzyka ogólnego oraz ryzyka dla podmiotów danych (oceny skutków) – w ślad za Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.

4. **Zlecenie, o którym mowa § 1 ust. 1 pkt 1 i 2 obejmuje:**
    1) przygotowanie i przesłanie raportu poaudytowego w terminie do 14 dni licząc od dnia zakończenia czynności audytu.

5. **Zlecenie, o którym mowa § 1 ust. 1 pkt 3 obejmuje:**
    1) przygotowanie i przesłanie procedur z zakresu Oceny Skutków dla Ochrony Danych (DPIA) i analizy ryzyka ogólnego w terminie do 14 dni licząc od dnia zakończenia audytu wewnętrznego.

§ 2. WARUNKI WSPÓŁPRACY

1. Przeprowadzenie audytu, o którym mowa w § 1 ust. 1 pkt 1 i 2 odbędzie się w terminie od **14.06.2023r. do 15.06.2023r. w** godzinach pracy organizacji, natomiast proces wykonywania zewnętrznych testów podatności może rozpocząć się od dnia nawiązania niniejszej umowy.
2. Zleceniobiorca wystawia f-rę VAT za wykonanie zlecenia, o którym mowa w § 1 ust. 1 na kwotę łączną **11500,00 zł NETTO** (jedenaście tysięcy pięćset złotych netto) plus należny podatek VAT 23% tj. **14145,00 zł BRUTTO** (czternaście tysięcy sto czterdzieści pięć złotych brutto) w dniu przesłania raportu poaudytowego z 14 dniowym terminem płatności.
3. Całość wynagrodzenia określonego w niniejszej umowie zawiera wszelkie koszty operacyjne mogące być poniesione przez Zleceniobiorcę w związku z realizacją niniejszej umowy. Zleceniobiorcy nie przysługuje prawo do żądania zwiększenia kwoty wynagrodzenia.

4. Do obowiązków Zleceniodawcy należy:
   1) terminowa zapłata za należycie wykonane i udokumentowane usługi;
   2) przekazanie Zleceniobiorcy wszelkich informacji, materiałów oraz dokumentów niezbędnych do należytego wykonywania jego obowiązków;
   3) wyznaczenie osoby odpowiedzialnej za bieżące kontakty ze Zleceniobiorcą, której zadaniem będzie nadzorowanie oraz pomoc Zleceniobiorcy w należytym wykonywaniu jego obowiązków

§ 3. POUFNOŚĆ

1. Zleceniobiorca zobowiązuje się do zachowania w tajemnicy wszelkich informacji uzyskanych od Zleceniodawcy oraz informacji, do których otrzymał dostęp w związku z wykonywaniem usług na rzecz Zleceniodawcy lub innego podmiotu powiązanego ze Zleceniodawcą kapitałowo, personalnie, gospodarczo lub organizacyjnie (na rzecz lub na zlecenie).
2. Zleceniobiorca zobowiązuje się do przechowywania wszelkich informacji i dokumentów związanych z wykonywaniem usług na rzecz Zleceniodawcy w sposób uniemożliwiający ich wykorzystanie przez osoby nieuprawnione. Dokumenty i informacje powinny być przechowywane z należytą starannością.

§ 4. WYPOWIEDZENIE LUB ODSTĄPIENIE OD UMOWY

1. Każda ze Stron może wypowiedzieć lub odstąpić od Umowy ze skutkiem natychmiastowym i w drodze pisemnego oświadczenia przesłanego drugiej Stronie w razie zaistnienia zdarzenia, którego skutkiem jest niemożność wykonania obowiązków wynikających z Umowy przez którąkolwiek ze Stron.
2. Strony ustalają, iż w przypadku wypowiedzenia lub odstąpienia od Umowy z przyczyn leżących po stronie Zleceniobiorcy, Zleceniobiorca zapłaci Zleceniodawcy karę umowną w wysokości 10 % wynagrodzenia brutto, o którym mowa § 2 niniejszej Umowy.

§ 5. POSTANOWIENIA KOŃCOWE

1. Wszelkie spory i roszczenia majątkowe, powstałe pomiędzy Stronami umowy będą ostatecznie rozstrzygnięte przez sąd powszechny właściwy ze względu na siedzibę Zleceniobiorcy.
2. W sprawach nieuregulowanych postanowieniami niniejszej umowy zastosowanie mają odpowiednie przepisy Kodeksu cywilnego.
3. Każda ze Stron zobowiązuje się do niezwłocznego wzajemnego zawiadomienia na piśmie o wszelkich zmianach danych wskazanych w niniejszej umowie, w szczególności o zmianie adresu siedziby lub prowadzenia działalności gospodarczej. W razie braku powiadomienia korespondencję kierowaną na dotychczasowy adres uważa się za doręczoną.
4. Zleceniobiorca zastrzega sobie prawo wystąpienia czynnika losowego w kwestii dnia wykonania zlecenia takich jak: nagły wypadek, kolizje drogowe, sytuacja rodzinna – Zleceniobiorca zobowiązuje się do wykonania zlecenia w ciągu 7 dni roboczych.
5. Umowa może zostać zmieniona lub uzupełniona jedynie w formie pisemnego aneksu pod rygorem nieważności.
6. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

PREZYDENT MIASTA
Sabina Nowosielska
pieczęć i podpis Zleceniodawcy

pieczęć i podpis Zleceniobiorcy

RADCA PRAWNY
Z-ca Skarbnika Miasta
Główny Księgowy
Urzędu Miasta Jastrzębie-Zdrój