ZAŁĄCZNIK NR 3 - WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ……. pomiędzy:

……, z siedzibą w ……. (kod: ……..)

przy ulicy ……, NIP ……..., REGON

……, zwanym dalej Administratorem danych osobowych lub Administratorem, reprezentowanym przez :

1) ……..

a

……, z siedzibą w ……. (kod: ……..)

przy ulicy ……, NIP ……..., REGON

……, zwanym dalej Przetwarzającym, reprezentowanym przez:

1) ……..

§ 1
Postanowienia ogólne

1. Dla potrzeb niniejszej umowy, Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

   1) Umowa Powierzenia – niniejsza umowa;

   2) RODO - 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. U. UE. L. z 2016 r. Nr 119, str. 1);

   3) Umowa - umowa zawarta pomiędzy Stronami, której przedmiotem jest:

   1) przeprowadzenie diagnozy cyberbezpieczeństwa w Gminie Lublin,

   2) dostawa sprzętu komputerowego wraz z oprogramowaniem,

   na potrzeby działania Gminy Lublin w ramach projektu grantowego „CYFROWA GMINA" realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" i której wykonanie wymaga przekazania przez Administratora Przetwarzającemu danych osobowych.

2. Strony oświadczają, że Umowa Powierzenia została zawarta w celu wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy.
3. W trybie art. 28 ust. 3 RODO, na mocy niniejszej umowy Administrator powierza Przetwarzającemu dane osobowe w zakresie określonym w § 2 niniejszej umowy a Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem i Umową Powierzenia.

4. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie Powierzenia oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz inne polecenia przekazywane przez Administratora drogą elektroniczną na adres _____ lub na piśmie.

5. Przetwarzający zapewnia, że:
   a) posiada fachową wiedzę i zasoby konieczne do należytej realizacji niniejszej umowy, w szczególności wdrożył odpowiednie środki techniczne i organizacyjne gwarantujące bezpieczeństwo powierzonych do przetwarzania danych osobowych, w tym m.in. wdrożył - przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia - odpowiednie środki techniczne i organizacyjne, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku,
   b) będzie zabezpieczał interes prawny osób, których dane przetwarza,
   c) będzie realizował wytyczne Administratora w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych,
   d) dane osobowe będą przetwarzane wyłącznie na obszarze Państw Członkowskich Unii Europejskiej (UE) lub państw sygnatariuszy Umowy o Europejskim Obszarze Gospodarczym (EOG). Jakiekolwiek przekazanie powierzonych danych osobowych do państwa trzeciego wymaga uprzedniej pisemnej zgody Administratora i musi spełniać szczególne wymagania określone w rozdziale V RODO,
   e) każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, będzie je przetwarzała wyłącznie w celach i zakresie przewidzianym w Umowie Powierzenia,
   f) będzie prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

6. Przetwarzający nie jest uprawiony do dalszego przekazywania danych osobowych innemu podmiotowi, bez uprzedniej pisemnej zgody Administratora. Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych, musi uprzednio poinformować Administratora o zamiarze podpowierzenia, tożsamości (firmie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie a także o: charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia.
7. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie przetwarzania będzie mieć za podstawę umowę, na podstawie której subprocesor zobowiąże się do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy Powierzenia nałożone są na Przetwarzającego.
8. W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Przetwarzający poinformuje o tym fakcie Administratora w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

§ 2

Określenie zakresu i okresu powierzenia przetwarzania

1. Administrator powierza Przetwarzającemu dane osobowe następujących kategorii osób, których dane dotyczą:
   a) _____
   b) _____
2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:
   a) co do [*kategoria osób*]: _____

   b) co do [*kategoria osób*]: _____

   Przetwarzający uprawiony jest do przetwarzania danych osobowych przez okres obowiązywania Umowy.
3. Przetwarzający zobowiązany jest do natychmiastowego zaprzestania przetwarzania danych w przypadku:
   a) rozwiązania Umowy Powierzenia ;
   b) ustania celu, dla którego niniejsza umowa została zawarta, w szczególności w przypadku rozwiązania/wygaśnięcia Umowy.

4. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.
5. W przypadku usunięcia danych - Przetwarzający zobowiązany jest, w terminie 3 dni roboczych od dnia wykonania operacji, poinformować pisemnie Administratora o wykonaniu tej operacji oraz o sposobie jej wykonania .
6. Zapisy § 2 ust. 4 oraz ust. 5 nie obowiązują w przypadku gdy przepisy prawa powszechnego zobowiązują Przetwarzającego do przechowywania dokumentacji zawierającej powierzone dane osobowe. W takim przypadku Przetwarzający obowiązany jest do zachowania poufności tych danych.

§ 3

Określenie celu

1. Powierzenie przetwarzania danych osobowych następuje w celu wykonania Umowy, w szczególności _____.
2. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: _____.
3. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych oraz w formie papierowej.
4. Przetwarzający będzie zbierał/otrzymywał dane osobowe od _____ [sposób, źródła zbierania danych].

§ 4

Obowiązki Przetwarzającego

1. Przetwarzający zobowiązuje się, że:

1) podejmie wszelkie środki wymagane na mocy art. 32 RODO,
2) będzie pomagał Administratorowi wywiązać się z obowiązków określonych w art. 32 – 36 RODO,
3) będzie pomagał Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO; w szczególności Przetwarzający zobowiązuje się, na każde żądanie Administratora, do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą,
4) będzie przestrzegał wymogów określonych w *Regulaminie Ochrony Informacji dla Wykonawcy* (jeżeli będzie posiadać dostęp do systemów informatycznych Urzędu),

będącym częścią Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin,

5) nada imienne upoważnienia do przetwarzania powierzonych danych osobowych osobom, które dopuści do przetwarzania w swoim imieniu,
6) zapewni aby osoby upoważnione do przetwarzania danych osobowych zachowały w tajemnicy przetwarzanie dane osobowe jak i sposoby ich zabezpieczenia lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania ich w tajemnicy. Obowiązek wskazany w zdaniu poprzednim obowiązuje bezterminowo, mimo rozwiązania lub wygaśnięcia niniejszej umowy,
7) będzie przestrzegał minimalnych środków technicznych i organizacyjnych gwarantujących bezpieczeństwo powierzonych do przetwarzania danych osobowych, które określono w § 5 niniejszej umowy,
8) udostępni Administratorowi wszelkie informacje niezbędne do potwierdzenia, że spełnia obowiązki Przetwarzającego określone w przepisach prawa powszechnie obowiązującego,
9) umożliwi Administratorowi lub osobom upoważnionym przez Administratora przeprowadzanie audytów oraz kontroli,
10) w sytuacji podejrzenia naruszenia ochrony danych osobowych:
    a) przekaże Administratorowi informacje dotyczące naruszenia ochrony danych osobowych, w tym informacje, o których mowa w art. 33 ust. 3 RODO niezwłocznie, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia,
    b) przeprowadzi wstępną analizę ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekaże wyniki tej analizy do Administratora ,
    c) przekaże Administratorowi – na jego żądanie – wszystkie informacje niezbędne do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 2 RODO.
11) będzie informować Administratora o:
    1) jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych,
    2) jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczących przetwarzania powierzonych danych osobowych, skierowanej do Przetwarzającego,
    3) wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

§ 5

Minimalne środki techniczne i organizacyjne gwarantujące bezpieczeństwo powierzonych do przetwarzania danych osobowych

1. Minimalne środki techniczne i organizacyjne, do których podjęcia zobowiązany jest Przetwarzający zostały określone w Załączniku 1 ŚTO (środki techniczne i organizacyjne) do Umowy Powierzenia.
2. Przetwarzający udokumentuje wdrożenie środków technicznych i organizacyjnych określonych w Załączniku 1 ŚTO i na wniosek Administratora przedstawi taką dokumentację Administratorowi do wglądu przed rozpoczęciem przetwarzania danych osobowych.
3. Na przetwarzanie danych osobowych poza siedzibą Przetwarzającego, np. w lokalach prywatnych lub w kontekście pracy na odległość, wymagana jest uprzednia pisemna zgoda Administratora. Przetwarzający gwarantuje i zapewnia, że świadczenie usług lub wykonywanie pracy poza siedzibą Przetwarzającego przez jego pracowników lub współpracowników spełnia określone środki i wymogi, w tym w szczególności zagwarantowane są odpowiednie środki techniczne i organizacyjne w rozumieniu art. 32 RODO oraz środki wymagane przez Umowę.
4. Przetwarzający może wdrożyć odpowiednie alternatywne środki w trakcie okresu obowiązywania Umowy. Takie środki muszą być zgodne z postanowieniami art. 32 RODO i muszą zapewniać poziom ochrony równy lub wyższy w porównaniu do środków określonych w Załączniku 1 ŚTO. Przetwarzający jest zobowiązany do aktualizacji i podnoszenia jakości środków organizacyjnych i technicznych wraz z rozwojem istniejących technologii oraz wraz z pojawianiem się nowych zagrożeń.
5. Wdrożenie alternatywnych środków technicznych i organizacyjnych, o których mowa powyżej wymaga uzgodnienia z Administratorem. Wszelkie takie działania będą dokumentowane na piśmie i staną się częścią Umowy Powierzenia. Załącznik 1 ŚTO zostanie odpowiednio zmieniony przez Przetwarzającego za zgodą Administratora.

§ 6

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia RODO i Umowy Powierzenia; w szczególności Administrator jest uprawniony do żądania udzielenia przez Przetwarzającego wszelkich informacji dotyczących powierzonych danych osobowych.

2. Administrator ma także prawo przeprowadzania audytów lub kontroli Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub kontrole mogą być przeprowadzane przez Administratora lub podmioty trzecie upoważnione przez Administratora.
3. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni kalendarzowych.

§ 7

Odpowiedzialność

1. Administrator ponosi odpowiedzialność w stosunku do osób, których dane dotyczą z tytułu szkód, jakie osoba, której dane dotyczą może ponieść w wyniku niezgodnego z prawem lub nieprawidłowego przetwarzania lub wykorzystywania danych w trakcie wykonywania Umowy, stanowiącego naruszenie przepisów określonych w RODO lub innych przepisów dotyczących ochrony danych.
2. W przypadku, gdy Administrator będzie zobowiązany do zapłaty odszkodowania/zadośćuczynienia/grzywny/kary itp. z powodu niezgodnego z prawem lub nieprawidłowego przetwarzania lub wykorzystania danych, za które odpowiedzialność ponosi Przetwarzający, wówczas Przetwarzający zwolni Administratora z odpowiedzialności z tytułu wszelkich roszczeń i przejmie taką odpowiedzialność. Podmiot Przetwarzający dołoży najlepszych starań w celu wsparcia Administratora w obronie przeciwko wszelkim roszczeniom.
3. Postanowienia ust. 2 nie mają wpływu na inne roszczenia Administratora. Przetwarzający zobowiązuje się prowadzić wymaganą przepisami prawa dokumentację na temat przetwarzania oraz wykorzystywania powierzonych danych osobowych, która umożliwi Administratorowi przekazywanie dowodów na takie uporządkowane przetwarzanie i wykorzystywanie danych. Przetwarzający przekaże taką dokumentację Administratorowi także po rozwiązaniu Umowy Przetwarzania w przypadku, gdy będzie ona niezbędna dla Administratora do obrony przeciwko roszczeniom osób, których dane dotyczą lub innych osób trzecich.

§ 8

Rozwiązanie umowy

Administrator może rozwiązać niniejszą Umowę Powierzenia ze skutkiem natychmiastowym gdy Przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas audytu lub kontroli nie usunie ich w wyznaczonym terminie,
b) przetwarza dane osobowe w sposób niezgodny z Umową Powierzenia lub RODO;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych osobowych.

§ 9

Zasady zachowania poufności (jeżeli nie opisano zasad poufności w umowie głównej)

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych, o których mowa w § 9 ust. 1, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy Powierzenia i Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa.

§ 10

Postanowienia końcowe

1. Strony zgodnie postanawiają, że Przetwarzającemu nie przysługuje wynagrodzenie z tytułu zawarcia i wykonywania niniejszej Umowy Powierzenia.
2. Strony umowy postanawiają, że będą się kontaktowały za pośrednictwem następujących osób:
   a) ze strony Administratora: ……
   b) ze strony Przetwarzającego: ……
3. Zmiana postanowień niniejszej umowy wymaga zachowania formy pisemnej – pod rygorem nieważności .
4. Umowa została zawarta w 2 egzemplarzach, po 1 dla każdej ze Stron.

……. ……..

(data i podpis Administratora) *(data i podpis Przetwarzającego)*

Załącznik nr 1

Podmiot przetwarzający dane musi opisać stosowane przez niego środki bezpieczeństwa (*przed podpisaniem umowy)*. Przetwarzający może podać odniesienia do wdrożonych procedur/ dokumentów i/lub certyfikatów.

1. Kontrola dostępu do lokali i obiektów, w których przetwarzane są dane

Ryzyko nieuprawnionego dostępu do danych (w sensie fizycznym).

Środki techniczne i organizacyjne służące do kontroli dostępu do lokali i obiektów, w szczególności do kontroli autoryzacji:

Przykłady zabezpieczeń:

a. System kontroli dostępu (czytnik identyfikatorów, karta magnetyczna, karta z chipem)
b. System wydawania kluczy
c. Zamykanie drzwi (elektroniczne systemy otwierające drzwi itp.)
d. Ochrona, dozorcy
e. Zamykane na klucz szafki
f. sejfy
g. Urządzenia do nadzoru (system alarmowy, monitor wideo/CCTV)
h. Regularne przeglądy pozwoleń na stały dostęp
i. Inne

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez jednostkę organizacyjną Urzędu) spośród wymienionych sposobów zabezpieczeń.

2. Kontrola dostępu do systemów
Ryzyko nieuprawnionego dostępu do systemów informatycznych.

Techniczne (identyfikator/zabezpieczenie hasłem) i organizacyjne (podstawowe dane użytkownika) środki służące do identyfikacji użytkownika i uwierzytelniania:

Przykłady zabezpieczeń:

a. Procedury dotyczące hasła (minimalna długość, w tym specjalne znaki, regularna zmiana hasła)
b. Automatyczna blokada dostępu (np. koniec czasu w systemie)
c. Szyfrowanie nośników danych dla urządzeń komputerowych wynoszonych poza siedzibę Podmiotu Przetwarzajacego
d. Regularne testowanie, uzyskiwanie dostępu do i ocena środków technicznych i organizacyjnych (np. Testy Penetracji) w celu zapewnienia bezpieczeństwa przetwarzania
e. Zarządzanie reakcjami na incydenty
f. inne

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez jednostkę organizacyjną Urzędu) spośród wymienionych sposobów zabezpieczeń.

3. Kontrola dostępu do danych

Ryzyko dostępu do danych przez osoby nieuprawnione

Przykłady zabezpieczeń:

a. Zróżnicowane prawa dostępu (profile, role, grupy uprawnień, transakcje i obiekty)
b. Raporty z wykonywnych prac
c. Dostęp
d. Zmiana
e. Usuwanie
f. unikalny identyfikator użytkownika
g. inne

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez jednostkę organizacyjną Urzędu) spośród wymienionych sposobów zabezpieczeń.

4. Kontrola ujawniania

Ryzyko ujawnienia danych: przesyłanie elektronicznie, transport danych, przekazywanie danych itp., aby zapobiegać utracie, zmianie lub nieuprawnionemu ujawnieniu.

Przykłady zabezpieczeń:

a. Szyfrowanie/tunelowanie (VPN = Virtual Private Network - Wirtualna Sieć Prywatna)
b. Podpis elektroniczny
c. Szyfrowanie SSL
d. Logowanie do nośników, plików przesyłanych e-mail
e. Bezpieczeństwo transportu,
f. Inne

.

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez jednostkę organizacyjną Urzędu) spośród wymienionych sposobów zabezpieczeń

5. Zasada rozliczalności wprowadzanych danych

Ryzyko braku zapewnienia rozliczalności danych poprzez umożliwienie weryfikacji osób dokonujących operacji na danych:

Przykład:

mechnizmy kontroli logowania i rejestracji wprowadzania i zmian danych w aplikacjach

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez Wydział) spośród wymienionych sposobów zabezpieczeń

6. Kontrola dostępności/ integralności danych

Dane należy chronić przed przypadkowym zniszczeniem lub utratą poprzez stosowanie fizycznych/ logicznych środków zabezpieczeń.

Przykłady zabezpieczeń:

a) Procedury dotyczące kopii zapasowych Replikacja lustrzana dysków twardych np. technologia RAID
b) Nieprzerwana dostawa zasilania (UPS)
c) Systemy antywirusowe / firewalle
d) Plan odzyskiwania na wypadek katastrofy,
e) inne

Należy opisać wdrożone środki:…….

Wymagane jest stosowanie minimum …..(do wyboru przez Wydział) spośród wymienionych sposobów zabezpieczeń

7. Powiązane dokumenty i/lub certyfikaty

Proszę dodać powiązane dokumenty i/lub certyfikaty, które stanowią dowód lub wyjaśnienie dotyczące wyżej wymienionych wdrożonych środków (jeśli dotyczy):
Przykłady: Proszę określić odpowiedni dokument

a. Certyfikat ISO27001
b. Wiążące Zasady Korporacyjne (BCR)
c. Koncepcja bezpieczeństwa
d. Certyfikat RODO (Art. 42 RODO)
e. Certyfikat TISAX
f. Inne: Proszę wyszczególnić

Należy opisać wdrożone środki:…….
Wymagane jest stosowanie minimum …..(do wyboru przez Wydział) spośród wymienionych sposobów zabezpieczeń

Podmiot Przetwarzający	Administrator
Podpis:	Podpis:
_____	_____
Imię, nazwisko, data	Imię, nazwisko, data