Umowa powierzenia przetwarzania danych osobowych nr …....

W dniu ……. roku w Lublinie pomiędzy:
1. Gminą Lublin, Plac Króla Władysława Łokietka 1, 20-109 Lublin,
zwaną dalej Gminą, z upoważnienia którego działają:
1)
2)

a
2……., reprezentowaną przez …….. – zwanym dalej Przetwarzającym
zwanymi dalej Stronami a każda osobno Stroną.

§ 1 Postanowienia ogólne

1. Dla potrzeb niniejszej umowy, Gmina 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 nr .....…..... zawarta pomiędzy Stronami w dniu ..……..…, której przedmiotem jest …….
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 Gmina 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 Gminy, przy czym za udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz inne polecenia przekazywane przez Gminę drogą elektroniczną na adres …… lub na piśmie.
5. Przetwarzający zapewnia, że:
   1) posiada fachową wiedzę i zasoby konieczne do należytej realizacji niniejszej Umowy Powierzenia, w szczególności wdrożył odpowiednie środki techniczne i organizacyjne gwarantujące bezpieczeństwo powierzonych do przetwarzania danych osobowych, w tym m.in. wdrożył w obrębie własnej organizacji– 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, odpowiadające temu ryzyku;
   2) będzie zabezpieczał interes prawny osób, których dane przetwarza, w obrębie własnej organizacji;
   3) będzie realizował wytyczne Gminy w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych, nie stojące w sprzeczności z RODO i Umowy powierzenia, oraz nie wychodzące poza ustalony zakres prac ujętych w Umowie;
   4) 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 Gminy i musi spełniać szczególne wymagania określone w rozdziale V RODO;
   5) 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;

6) będzie prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Gminy, o którym mowa w art. 30 ust. 2 RODO, i udostępniać go Gminie 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 Gminy. Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych, musi uprzednio poinformować Gminę 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 Gminę w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

§ 2 Określenie zakresu i okresu powierzenia przetwarzania

1. Gmina powierza Przetwarzającemu dane osobowe następujących kategorii osób, których dane dotyczą:
   1) …
   2) ...
2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:
   1) co do [kategoria osób]: .....;
   2) co do [kategoria osób]: .....
3. Przetwarzający uprawiony jest do przetwarzania danych osobowych przez okres obowiązywania Umowy.
4. Przetwarzający zobowiązany jest do natychmiastowego zaprzestania przetwarzania danych w przypadku:
   1) rozwiązania Umowy Powierzenia;
   2) ustania celu, dla którego niniejsza umowa została zawarta, w szczególności w przypadku rozwiązania/wygaśnięcia Umowy.
5. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający, zależnie od decyzji Gminy, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.
6. W przypadku usunięcia danych – Przetwarzający zobowiązany jest, w terminie 3 dni roboczych od dnia wykonania operacji, poinformować pisemnie Gminę o wykonaniu tej operacji oraz o sposobie jej wykonania.
7. Zapisy § 2 ust. 5 oraz ust. 6 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 w celu ……..
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 Gminy.
4. Przetwarzający będzie otrzymywał dane osobowe od Gminy
   1) ...
   2) ...

§ 4 Obowiązki Przetwarzającego

Przetwarzający zobowiązuje się, że w obrębie własnej organizacji i w zakresie posiadanych uprawnień czy możliwości:

1) podejmie wszelkie środki wymagane na mocy art. 32 RODO;

2) będzie pomagał Gminie wywiązać się z obowiązków określonych w art. 32-36 RODO;

3) będzie pomagał Gminie 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 Gminy do przygotowania i przekazania Gminie 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 Miasta Lublin) będącym częścią Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin (SZBI), który w związku z tym, że dokumentacja SZBI jest na mocy zarządzenia Prezydenta Miasta Lublina wyłączona z jawności, zostanie udostępniony Przetwarzającemu po podpisaniu Umowy;

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 przetwarzane dane osobowe jak i sposoby ich zabezpieczenia lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania ich w tajemnicy; obowiązek ten 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 Gminie wszelkie informacje niezbędne do potwierdzenia, że spełnia obowiązki Przetwarzającego określone w przepisach prawa powszechnie obowiązującego;

9) umożliwi Gminielub osobom upoważnionym przez Gminę przeprowadzanie audytów oraz kontroli zapowiedzianych minimum na 10 dni przed planowany terminem audytu/kontroli;

10) w sytuacji podejrzenia naruszenia ochrony danych osobowych:

- **a)** przekaże Gminie 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 sytuacji naruszenia praw i wolności osób, których dane dotyczą, i przekaże wyniki tej analizy do Gminie;
- **c)** przekaże Gminie – na jego żądanie – wszystkie informacje niezbędne do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 2 RODO;

11) będzie informować Gminę o:

- **a)** jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych,
- **b)** jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczących przetwarzania powierzonych danych osobowych, skierowanych do Przetwarzającego,
- **c)** 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 nr 1 ŚTO (środki techniczne i organizacyjne) do Umowy Powierzenia.

2. Przetwarzający udokumentuje wdrożenie środków technicznych i organizacyjnych określonych w Załączniku nr 1 ŚTO i na wniosek Gminy przedstawi taką dokumentację Gminie 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 Gminy. 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 Powierzenia.
4. Przetwarzający może wdrożyć odpowiednie alternatywne środki techniczne i organizacyjne w trakcie okresu obowiązywania Umowy i Umowy Powierzenia. 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 nr 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 Gminą. Wszelkie takie działania będą dokumentowane na piśmie i staną się częścią Umowy Powierzenia. Załącznik nr 1 ŚTO zostanie odpowiednio zmieniony przez Przetwarzającego za zgodą Gminy.

§ 6 Prawo kontroli

1. Gmina, 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 Gmina jest uprawniona do żądania udzielenia przez Przetwarzającego wszelkich informacji dotyczących powierzonych danych osobowych, po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli lub audycie w terminie nie krótszym niż 10 dni przed planowanym audytem lub kontrolą. W przypadku sytuacji naruszenia ochrony danych osobowych Strony dopuszczają możliwość dokonania kontroli po uprzednim poinformowaniu Przetwarzającego w terminie nie krótszym niż 3 dni przed planowanym audytem lub kontrolą.
2. Gmina 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 Gminę lub podmioty trzecie upoważnione przez Gminę.
3. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli i audytów w terminie wskazanym przez Gminę nie dłuższym niż 7 dni kalendarzowych.
4. Strony zapewniają, iż osoby wydelegowane do przeprowadzenia kontroli/audytu posiadać będą stosowne upoważnienia do przetwarzania danych osobowych, jak również zostaną zobowiązane do zachowania poufności w zakresie powierzonych danych czy informacji.

§ 7 Odpowiedzialność

1. Gmina 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 Gmina będzie zobowiązana 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 Gminę z odpowiedzialności z tytułu wszelkich roszczeń i przejmie taką odpowiedzialność. Podmiot Przetwarzający dołoży najlepszych starań w celu wsparcia Gminy w obronie przeciwko wszelkim roszczeniom.
3. Postanowienia ust. 2 nie mają wpływu na inne roszczenia Gminy. Przetwarzający zobowiązuje się prowadzić wymaganą przepisami prawa dokumentację na temat przetwarzania oraz wykorzystywania powierzonych niniejszą umową danych osobowych w zakresie swojej organizacji, która umożliwi Gminie przekazywanie dowodów na takie uporządkowane przetwarzanie i wykorzystywanie danych po stronie Przetwarzającego. Przetwarzający przekaże taką dokumentację Gminie także po rozwiązaniu Umowy Przetwarzania w przypadku, gdy będzie

ona niezbędna dla Gminy do obrony przeciwko roszczeniom osób, których dane dotyczą lub innych osób trzecich.

§ 8 Rozwiązanie umowy

1. Gmina może rozwiązać niniejszą Umowę Powierzenia ze skutkiem natychmiastowym, gdy Przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas audytu lub kontroli nie usunie ich w wyznaczonym terminie;
   2) przetwarza dane osobowe w sposób niezgodny z Umową Powierzenia lub RODO;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Gminy danych osobowych.

§ 9 Postanowienia końcowe

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

.....… *….....*
(data i podpis Gminy) *(data i podpis Przetwarzającego)*

Załączniki:
1. Załącznik nr 1 - ŚTO (środki techniczne i organizacyjne)

Środki Techniczne i Organizacyjne

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: …….

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, złożoność hasła, regularna zmiana hasła)
- **b)** Automatyczna blokada dostępu (np. koniec czasu w systemie)
- **c)** Szyfrowanie nośników danych dla urządzeń komputerowych wynoszonych poza siedzibę Przetwarzającego
- **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: …….

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 wykonywanych prac
- **c)** Dostęp
- **d)** Zmiana
- **e)** Usuwanie

f) Unikalny identyfikator użytkownika
g) Inne

Należy opisać wdrożone środki: …….

4. Kontrola ujawnienia**.**
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: …….

5. Zasada rozliczalności wprowadzanych danych.
Ryzyko braku zapewnienia rozliczalności danych poprzez umożliwienie weryfikacji osób dokonujących operacji na danych.

Przykład:
mechanizmy kontroli logowania i rejestracji wprowadzania i zmian danych w aplikacjach

Należy opisać wdrożone środki: …….

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: …….

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: …….

Gmina

Podpis:

Imię, nazwisko, data

Przetwarzający

Podpis:

Imię, nazwisko, data