

Załącznik nr 2 do umowy - wzór umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych nr (WZÓR)

zawarta w dniu pomiędzy:

Prezydentem Miasta Lublin, Plac Króla Władysława Łokietka 1, 20-109 Lublin,
zwanym dalej Administratorem danych osobowych lub Administratorem, z upoważnienia
którego działają:

- 1)
- 2)

a

....., z siedzibą w (kod:) przy ulicy,
NIP, REGON, zwanym dalej Przetwarzającym,
reprezentowanym przez:

- 1)
- 2)

zwanymi dalej Stronami a każda osobno Stroną.

§ 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 nr zawarta pomiędzy Stronami w dniu, której przedmiotem jest: ... 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:
 - 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. wdrożyć – 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;
 - 3) będzie realizował wytyczne Administratora w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych;
 - 4) dane osobowe będą przetwarzane wyłącznie na obszarze Państw Członkowskich Unii Europejskiej (UE) lub państw sygnatariuszy Umowy o Europejskim Obszarze Gospodarczym (EOG); jakiegokolwiek przekazanie powierzonych danych osobowych do państwa trzeciego wymaga uprzedniej pisemnej zgody Administratora 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 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 uprawniony 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 subprocessor 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 informuje 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:
 - 1) ...;
 - 2) ...;
 - 3)
2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje ...
 - a. co do (kategoria osób):
 - b. co do (kategoria osób):

Przetwarzający uprawniony jest do przetwarzania danych osobowych przez okres obowiązywania Umowy.

3. 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.
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 Administratora oraz w formie papierowej.
4. Przetwarzający będzie zbierał/otrzymywał dane osobowe od (sposób, źródła zbierania danych).

§ 4 Obowiązki Przetwarzającego

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) jeżeli będzie posiadać dostęp do systemów informatycznych Urzędu, będzie przestrzegał zasad pracy w tych systemach określonych w *Regulaminie Ochrony Informacji dla Wykonawcy* 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 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) prześle 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 prześle wyniki tej analizy do Administratora ,
 - c) prześle 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:
 - a) jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych,
 - b) jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczących przetwarzania powierzonych danych osobowych, skierowanej 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 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 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 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 i audytów w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.

§ 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

1. Umowa Powierzenia zawarta została na czas wykonywania Umowy.
2. Umowa Powierzenia wygasa z chwilą wygaśnięcia lub rozwiązania Umowy.

3. Administrator 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 Administratora danych osobowych.
4. Przetwarzający ma prawo rozwiązania Umowy Powierzenia wyłącznie w przypadkach jednoczesnego rozwiązania Umowy i w trybie w niej przewidzianym.

§ 9 Zasady zachowania poufności

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 postanawiają, że będą się kontaktowały za pośrednictwem następujących osób:
 - 1) ze strony Administratora:
 - 2) ze strony Przetwarzającego:
3. Zmiana postanowień Umowy Powierzenia wymaga zachowania formy pisemnej – pod rygorem nieważności.
4. Umowa Powierzenia została zawarta w trzech jednobrzmiących egzemplarzach, dwa dla Administratora i jeden dla Przetwarzającego.

.....
(data i podpis Administratora)

.....
(data i podpis
Przetwarzającego)

Załącznik nr 1 ŚTO do umowy powierzenia nr

Środki Techniczne i Organizacyjne

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

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

Ryzyko nieuprawnionego dostępu do danych (w sensie fizycznym).

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

- a) system kontroli dostępu (czytnik identyfikatorów, karta magnetyczna, karta z chipem),
- b) ochrona, dozorczy,
- c) sejfy,
- d) urządzenia do nadzoru (system alarmowy, monitor wideo/CCTV),
- e) regularne przeglądy pozwoleń na stały dostęp.

2. Kontrola dostępu do systemów.

Ryzyko nieuprawnionego dostępu do systemów informatycznych.

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

- 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) zarządzanie reakcjami na incydenty.

3. Kontrola dostępu do danych.

Ryzyko dostępu do danych przez osoby nieuprawnione.

Wymagane zabezpieczenia:

- a) zróżnicowane prawa dostępu (profile, role, grupy uprawnień, transakcje i obiekty),

- b) raporty z wykonywanych prac,
- c) unikalny identyfikator użytkownika.

4. Kontrola ujawnienia.

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

Wymagane zabezpieczenia:

- a) szyfrowanie/tunelowanie (VPN = Virtual Private Network - Wirtualna Sieć Prywatna),
- b) szyfrowanie SSL,
- c) logowanie do nośników.

5. Zasada rozliczalności wprowadzanych danych.

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

Wymagane zabezpieczenia:

- a) raporty z wykonywanych prac,
- b) unikalny identyfikator użytkownika.

6. Kontrola dostępności/ integralności danych.

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

Wymagane zabezpieczenia:

- a) procedury dotyczące kopii zapasowych,
- b) nieprzerwana dostawa zasilania (UPS),
- c) systemy antywirusowe / firewalle,
- d) plan odzyskiwania na wypadek katastrofy.

7. Powiązane dokumenty i/lub certyfikaty

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..... spośród wymienionych sposobów zabezpieczeń

Podmiot Przetwarzający

Podpis:

Podpis:

Imię, nazwisko, data

Imię, nazwisko, data