

UMOWA NR
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu roku w Łodzi pomiędzy:

Województwem Łódzkim, w imieniu którego występuje **Zarząd Województwa Łódzkiego** z siedzibą Al. Piłsudskiego 8, 90-051 Łódź, działający jako **Administrator danych** zwany dalej „Administratorem” reprezentowany przez:

reprezentowanym przez

.....

.....,

.....

.....

.....

zwanym w treści umowy „**Podmiotem przetwarzającym**”

reprezentowanym przez

.....

Zważywszy, że:

1. Administrator jest Administratorem danych osobowych w rozumieniu art. 4 pkt 7 Rozporządzenia 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 zwanego dalej „RODO”.
2. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych, a Podmiot przetwarzający przyjmuje powierzone mu dane osobowe do przetwarzania w imieniu Administratora, zgodnie z umową oraz z przepisami

regulującymi przetwarzanie danych osobowych, wiążącymi Podmiot przetwarzający i Administratora.

Strony postanowiły, co następuje:

§ 1

Przedmiot, cel i zakres przetwarzania danych

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wyłącznie w celu i zakresie określonym w ust. 3-5 niniejszego paragrafu, a Podmiot przetwarzający zobowiązuje się przetwarzać te dane w sposób zgodny z:
 - 1) RODO,
 - 2) przepisami krajowymi oraz
 - 3) postanowieniami umowy.
2. Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.
3. Przedmiotem umowy jest powierzenie przetwarzania danych osobowych w związku z umową główną na świadczenie usług związanych z udostępnieniem systemu zarządzania Budżetem Obywatelskim.
4. Zakres kategorii osób i zakres powierzonych danych osobowych obejmują:
 - 1) dane zwykle pracowników Administratora: imię, nazwisko, numer telefonu, adres e-mail, adres zamieszkania, login, adres IP;
 - 2) dane zwykle użytkowników systemu, które założą konto w systemie: imię, nazwisko, numer telefonu, adres e-mail, adres zamieszkania, login, adres IP
 - 3) dane zwykle użytkowników systemu, którzy zgłoszą projekt lub są rodzicami/opiekunami prawnymi użytkowników zgłaszających projekt - imię, nazwisko, numer telefonu, adres e-mail, login, adres IP, adres zamieszkania - ulica, nr domu, nr mieszkania, kod pocztowy, miejscowość, powiat,
 - 4) dane zwykle osób, które wezmą udział w głosowaniu na projekty zgłoszone do budżetu obywatelskiego - imię, nazwisko, data urodzenia, powiat zamieszkania, adres mail, numer telefonu, adres IP,

- 5) dane zwykłe osoby fizyczne, które złożą podpisy poparcia pod projektem do budżetu obywatelskiego lub są rodzicami/opiekunami prawnymi (dostarczone przez użytkowników systemu): imię, nazwisko, powiat zamieszkania, podpis.
5. Zakres operacji na powierzonych danych obejmuje: przechowywanie, wgląd, kopiowanie, usuwanie oraz inne operacje niewskazane w niniejszym ustępie, w zakresie niezbędnym dla potrzeb wynikających z realizacji umowy wyłącznie na pisemne polecenie administratora, bez konieczności aneksowania umowy.

§ 2

Oświadczenie Podmiotu przetwarzającego

Podmiot przetwarzający oświadcza, że:

1. wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą te dane;
2. dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającym prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonym w umowie.

§ 3

Przetwarzanie danych osobowych

1. Z zastrzeżeniem ust. 2, przetwarzanie danych osobowych przez Podmiot przetwarzający może następować wyłącznie w przypadkach wynikających z umowy lub na podstawie odrębnych poleceń Administratora, wyrażonych w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej).
2. Podmiot przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku Podmiot przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.
3. Przetwarzanie danych osobowych przez Podmiot przetwarzający jest ograniczone do celu i zakresu wskazanego w § 1 ust. 3-5 umowy.

4. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych, Podmiot przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.
5. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
6. Podmiot przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
 - 1) otrzymają dostęp do danych osobowych w zakresie bezwzględnie koniecznym do wykonania umowy, zarządzania nią i jej monitorowania;
 - 2) otrzymają pisemne upoważnienia do przetwarzania danych osobowych oraz zobowiążą się do bezterminowego zachowania w poufności otrzymanych danych osobowych oraz stosowanych przez Podmiot przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.
 - 3) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
 - 4) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2.
7. Podmiot przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych, o których mowa w ust. 6 pkt 2).
8. Podmiot przetwarzający po zakończeniu świadczenia usługi związanej z przetwarzaniem w terminie 14 dni zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

§ 4

Bezpieczeństwo danych osobowych

1. Podmiot przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą,

modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem. Wykaz środków technicznych i organizacyjnych zawiera **załącznik nr 1** do umowy.

2. Podmiot przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa, i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.
3. Podmiot przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.
4. Podmiot przetwarzający, na pisemne żądanie Administratora, w terminie 14 dni od dostarczenia żądania, przekazuje Administratorowi analizę ryzyka dotyczącą przedmiotu umowy.
5. Podmiot przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:
 - 1) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
 - 2) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.
6. Podmiot przetwarzający niezwłocznie, jednak nie później niż w terminie 24 godzin informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi przetwarzającemu informacje na temat naruszenia, w szczególności:
 - 1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
 - 2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
 - 3) możliwe konsekwencje naruszenia ochrony danych osobowych;
 - 4) środki zastosowane lub proponowane przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych, negatywnych skutków.
7. Podmiot przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem w szczególności przyczyn

i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.

8. Podmiot przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.
9. Ze strony Administratora osobami upoważnionymi i odpowiedzialnymi za nadzór nad realizacją umowy są:

1) tel.:

2) dane kontaktowe Inspektora Ochrony Danych: iod@lodzkie.pl

Ze strony Podmiotu przetwarzającego nadzór nad prawidłową realizacją umowy pełni:

3)

4) dane kontaktowe Inspektora Ochrony Danych (*jeśli dotyczy*):

Ewentualna zmiana osób wskazanych w pkt 1 i 3 dla swej skuteczności będzie wymagała jedynie jednostronnego pisemnego oświadczenia skierowanego do drugiej Strony i nie wymaga dla swej ważności zmiany umowy w formie aneksu.

§ 5

Dalsze powierzenie przetwarzania

Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu Administratora zgodnie z umową podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej, pisemnej zgody Administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody, co najmniej 14 dni przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by Administrator mógł podjąć decyzję w sprawie zgody. Wykaz podmiotów podprzetwarzających zawiera załącznik nr 2 do umowy.

§ 6

Kontrola

1. Podmiot przetwarzający zobowiązuje się do umożliwienia Administratorowi realizacji uprawnień wynikających z art. 28 ust. 3 lit. h) RODO.

2. Czynności kontrolne Administrator wykonuje w godzinach pracy Podmiotu przetwarzającego. O podjęciu czynności kontrolnych Administrator poinformuje Podmiot co najmniej siedem dni roboczych przed ich rozpoczęciem.
3. Z czynności kontrolnych przedstawiciel Administratora sporządza protokół, który podpisują i otrzymują przedstawiciele obu Stron. Podmiot przetwarzający może wnieść zastrzeżenia do protokołu w terminie siedmiu dni roboczych od daty jego podpisania.
4. Podmiot przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania powierzonych danych osobowych. O sposobie i terminie usunięcia uchybień, Podmiot przetwarzający poinformuje Administratora w formie pisemnej.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za niewywiązanie się z postanowień umowy.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym oraz o jakiegokolwiek skierowanej do Podmiotu przetwarzającego decyzji administracyjnej lub orzeczeniu, a także o wszelkich planowanych (o ile są wiadome) lub realizowanych kontrolach i inspekcjach w związku z przetwarzaniem powierzonych danych osobowych.

§ 8

Obowiązywanie umowy

Umowa obowiązuje od dnia jej podpisania do zakończenia realizacji umowy nr
.....wskazanej w § 1 pkt 3

§ 9

Rozwiązanie umowy

1. Administrator ma prawo rozwiązać umowę bez zachowania terminu wypowiedzenia, gdy Podmiot przetwarzający:

- 1) udostępnił lub wykorzystał powierzone dane osobowe w sposób niezgodny z umową,
 - 2) powierzył przetwarzanie danych osobowych Podmiotom podprzetwarzającym bez zgody Administratora,
 - 3) nie zaprzestał niewłaściwego przetwarzania danych osobowych, stwierdzonego w wyniku kontroli,
 - 4) nie usunął uchybień stwierdzonych podczas kontroli w wyznaczonym przez Administratora terminie.
2. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

§ 10

Postanowienia końcowe

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, RODO i innych przepisów prawa powszechnie obowiązującego.
2. Wszelkie zmiany w umowie wymagają zachowania formy pisemnej pod rygorem nieważności z wyłączeniem § 1 ust. 6
3. Sądem właściwym dla rozpatrzenia sporów wynikających z umowy będzie sąd właściwy dla siedziby Administratora.
4. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach dla każdej ze Stron.

Administrator:

Podmiot przetwarzający

.....

.....

Załączniki:

1. **załącznik nr 1** – Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający;
2. **załącznik nr 2** – Wykaz podwykonawców Podmiotu przetwarzającego.

Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający w celu zapewnienia bezpieczeństwa danych

1. Wdrożenie przez Podmiot przetwarzający polityk i procedur mających zapewnić bezpieczeństwo, poufność, integralność i dostępność, m.in.:
 - a) politykę bezpieczeństwa,
 - b) zasady przebywania na terenie Podmiotu przetwarzającego i dostępu do pomieszczeń,
 - c) politykę ciągłości działania,
 - d) zasady użytkowania aktywów i wnoszenie sprzętu*,
 - e) zasady zabezpieczenia komputerów osobistych*,
 - f) politykę zarządzania siecią informatyczną*,
 - g) zasady administracji systemami i aplikacjami*,
 - h) zasady korzystania z nośników informacji*,
 - i) zasady dostępu zdalnego*,
 - j) zasady bezpieczeństwa poczty elektronicznej*,
 - k) politykę haseł*,
 - l) polityki antywirusowej*,
 - m)
(inne środki stosowane przez Podmiot przetwarzający - należy wymienić)
2. Prowadzenie rejestru wszystkich kategorii czynności przetwarzania, zawierającego informacje wskazane w art. 30 ust. 2 RODO.
3. Przeprowadzanie oceny ryzyka oraz DPIA (jeśli ma to zastosowanie).
4. Zapewnienie szkoleń dla pracowników w zakresie ochrony danych osobowych.
5. Zobowiązanie pracowników do zachowania w tajemnicy wszelkich informacji związanych z przetwarzaniem danych osobowych.
6. Korzystanie przez podmiot przetwarzający z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych.
7. Wdrożenie przez Podmiot przetwarzający adekwatnych do poziomu zagrożeń środków technicznych i organizacyjnych, zapewniających ograniczenie dostępu do budynków, systemów i zbiorów danych wyłącznie dla osób upoważnionych.
8. W przypadku przetwarzania danych osobowych w systemach informatycznych, zapewnienie by każdy pracownik otrzymał indywidualne konto i hasło. Zapewnienie okresowej zmiany haseł zgodnie z polityką haseł*.

* punkt ma zastosowanie, gdy przetwarzanie danych osobowych odbywa się przy użyciu systemów informatycznych.

Wykaz podmiotów podprzetwarzających