

Umowa nr

W dniu w Lublinie pomiędzy:

1. Gminą Lublin, Plac Króla Władysława Łokietka 1, 20-109 Lublin, NIP: 946-25-75-811, REGON 431019514, reprezentowaną przez:

a)

b)

– zwaną dalej **Zamawiającym**

a

2.

– zwaną dalej **Wykonawcą**

zawarta została umowa, zwana dalej Umową, o następującej treści.

§ 1 Definicje

System – wdrożony u Zamawiającego system SYSTEMU ZARZĄDZANIA RUCHEM W LUBLINIE (ITS);

awaria Systemu – całkowity brak funkcjonowania Systemu w wyniku jego uszkodzenia;

błąd Systemu – każde poważne pogorszenie funkcjonalności lub wydajności Systemu mające wpływ na jakość usług;

usterka Systemu – problemy z pojedynczymi funkcjami Systemu, występujące sporadycznie lub na lokalnych stanowiskach i inne nie mające znamion błędu Systemu;

Strony – strony Umowy, tj. Zamawiający i Wykonawca;

siła wyższa – występujące po zawarciu Umowy zewnętrzne, niemożliwe do przewidzenia i zapobieżenia oraz niezależne od Stron zdarzenie takie, jak: katastrofy naturalne (katastrofalne działania przyrody i klęski żywiołowe), wojny, ataki terrorystyczne, akty władzy państwowej (np. stan wojenny, stan wyjątkowy), strajki o zasięgu krajowym uniemożliwiające należyte wykonanie przez Strony przedmiotu Umowy;

dzień roboczy – dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.

§ 2 Przedmiot umowy

Przedmiotem Umowy jest:

a) Świadczenie usługi asysty technicznej Systemu;

b) Transfer wiedzy dla administratorów.

§ 3 Obowiązki Wykonawcy

1. W ramach usługi asysty technicznej Systemu Wykonawca zobowiązuje się do zapewnienia ciągłości funkcjonowania oraz Wsparcia technicznego dla administratorów Systemu wraz z podsystemami IT oraz podsystemami Systemu Zarządzania Ruchem;

2. Przekazania Zamawiającemu aktualnej dokumentacji użytkowej Systemu

oraz wykonania – w terminie 1 miesiąca od dnia wejścia Umowy w życie:

- a) Usługi audytu systemu SZR;
 - b) Inwentaryzacji sprzętu oraz aplikacji;
 - c) Weryfikacji uszkodzeń, stanów awaryjnych;
 - d) Aktualizacji dokumentacji w zakresie zestawień ilościowych sprzętu.
3. Przyjmowania przez wszystkie dni tygodnia zgłoszeń dotyczących awarii Systemu, błędów Systemu i usterek Systemu za pomocą systemu helpdesk Zamawiającego oraz poczty elektronicznej pod adresem
4. Realizowania zgłoszeń, o których mowa powyżej:
- a) termin usunięcia awarii Systemu ustala się na 1 dzień;
 - b) termin usunięcia błędu Systemu ustala się na 3 dni;
 - c) termin usunięcia usterki Systemu ustala się na 5 dni.
5. Wprowadzania modyfikacji oraz stałej aktualizacji poszczególnych modułów i elementów Systemu.
6. Przekazywania Zamawiającemu aktualnej dokumentacji użytkowej Systemu albo aneksu do dokumentacji użytkowej Systemu, każdorazowo po jego modyfikacji lub aktualizacji – w terminie 7 dni roboczych od dokonania zmian w środowisku Zamawiającego.
7. Nadzoru technicznego nad automatycznym systemem wykonywania dobowych kopii bezpieczeństwa Systemu.
8. Wsparcie techniczne w zakresie wykonywania kopii archiwalnych Systemu na prośbę Zamawiającego.
9. Odtwarzania Systemu lub danych Systemu z kopii bezpieczeństwa, na prośbę Zamawiającego.
10. Udzielania pracownikom i administratorom Zamawiającego, w dni robocze w godzinach od 7.30 do 15.30, pomocy konsultacyjnej i doradczej związanej z funkcjonowaniem Systemu, pod numerem telefonu: oraz adresem e-mail:.....
11. Wykonawca będzie dokonywał transferu wiedzy w formie instruktaży na rzecz administratorów systemu w obszarach:
- a) infrastruktury serwerowej, bazodanowej, środowiska wirtualizacji, architektury aplikacji i backupu;
 - b) infrastruktury transmisji danych, topologii sieci, routingu, firewallingu
 - c) administrowania uprawnieniami użytkowników
12. Instruktaże w ramach transferu wiedzy obejmą czynności wykonywane on on-site w wymiarze nie mniejszym niż 40 godzin oraz nielimitowane konsultacje i obejmą:
- a) Podsystem IT (Infrastruktura sprzętowa): Macierze dyskowe, Przełączniki sieciowe, Firewall, Serwery oraz wirtualizacja, Backup.
 - b) Podsystemy - Infrastruktura aplikacyjna
 - c) Systemy zarządzania ruchem
 - d) System analizy obrazu;

w zakresie:

- a) Działania modułu/urządzeń;
- b) Topologii podsystemu/modułu;
- c) Przetwarzanych danych oraz ich postaci wyjściowej;
- d) Konsoli zarządzającej, uruchomienie oraz zarządzanie;
- e) Monitorowania środowiska/identyfikacji problemów;

- f) Monitorowania pracy aplikacji zarządzania ruchem;
- g) Raportów w systemie.

13. Usługi dodatkowe związane z zapewnieniem ciągłości pracy systemu, a nie objęte umową, będą rozliczane wg stawki godzinowej zł netto/h, zł brutto/h w wymiarze nie przekraczającym ... godzin i wymagają dodatkowego zlecenia uzgadnianego każdorazowo przez Strony Umowy.

14. Płatność za usługę asysty będzie odbywała się w stałej, zryczałtowanej kwocie miesięcznej zł netto zł brutto. W przypadku świadczenia usługi asysty krócej niż pełny miesiąc kalendarzowy wynagrodzenie zostanie pomniejszone o 1/30 zryczałtowanej kwoty miesięcznej asysty za każdy dzień, w którym usługa nie była świadczona.

§ 4 Obowiązki Zamawiającego

1. Zamawiający zobowiązuje się do współpracy z Wykonawcą w celu realizacji Umowy, a w szczególności do:
 - a) zapewnienia terminowości wszelkich obustronnie ustalanych kontaktów roboczych oraz zaplanowanych prac;
 - b) uzgadniania z Wykonawcą wszelkich planowanych zmian sprzętowych i systemowych, mogących mieć znaczenie dla poprawności i efektywności pracy Systemu;
 - c) zapewnienia i utrzymywania przez czas trwania Umowy dostępu pracowników Wykonawcy do Systemu, przy zachowaniu bezpiecznego kanału transmisji danych wykorzystującego technologię VPN Zamawiającego.
 - d) udostępnienia dedykowanego adresu e-mail oraz numeru telefonu Zamawiającego do obsługi zgłoszeń.
2. Przedstawicielami Zamawiającego, koordynującym prace będące przedmiotem Umowy, upoważnionym do zgłaszania Wykonawcy potrzeby wykonania prac w formie zlecenia i podpisywania protokołów realizacji prac, są:
 - w zakresie funkcjonowania systemu i urządzeń CSR Grzegorz Rejak, tel. 81 466 2957, email: grzegorz_rejak@lublin.eu;
 - w zakresie zasobu serwerowego, storage i backupu Bartłomiej Kwaśniewski, tel. 81 466 1150, email: bartlomiej.kwasniewski@lublin.eu;
 - w zakresie urządzeń sieciowych Andrzej Małecki, tel. 81 466 1131, email: andrzej.malecki@lublin.eu;
 - w zakresie zarządzania uprawnieniami do Systemu Tomasz Kleczek, tel. 81 466 1196 email: tomasz.kleczek@lublin.eu;

§ 5 Podwykonawcy

W przypadku wykonywania przedmiotu Umowy przy pomocy podwykonawców, Wykonawca jest odpowiedzialny za działania i zaniechania osób, z których pomocą wykonuje przedmiot Umowy, jak za własne działania oraz ponosi pełną odpowiedzialność za jakość i terminowość prac, które wykonuje przy pomocy podwykonawców.

BW

f

§ 6 Ochrona danych osobowych

1. Zamawiający powierzy Wykonawcy przetwarzanie danych osobowych w zakresie, w celu i na zasadach określonych w Załączniku nr 1 do Umowy.
2. Wykonawca w terminie 3 dni od podpisania Umowy podpisze z Zamawiającym porozumienie dot. powierzenia przetwarzania danych osobowych, którego treść stanowi Załącznik nr 1 do Umowy.

§ 7 Poufność

1. Informacje Poufne – niezależnie od formy ich utrwalenia lub przekazania – są to informacje Zamawiającego, które nie zostały podane do publicznej wiadomości, a zostały przekazane lub udostępnione Wykonawcy w związku z realizacją Umowy, które Zamawiający oznaczył jako poufne lub w inny sposób poinformował Wykonawcę, że traktuje je jako poufne. Informacjami poufnymi są także informacje przekazane Wykonawcy w toku postępowania poprzedzającego zawarcie Umowy, oznaczone jako poufne. Dla uniknięcia wątpliwości Strony potwierdzają, że Informacje Poufne obejmują także dane osobowe powierzone Wykonawcy do przetwarzania na zasadach określonych w umowie powierzenia przetwarzania danych osobowych.
2. Za Informacje Poufne nie są uważane informacje, które Zamawiający jest zobowiązany ujawnić na mocy obowiązujących przepisów, w tym Prawa zamówień publicznych.
3. Wykonawca zobowiązuje się:
 - a) nie ujawniać Informacji Poufnych innym podmiotom, bez uprzedniej zgody Zamawiającego wyrażonej na piśmie, pod rygorem nieważności;
 - b) wykorzystywać Informacje Poufne jedynie w celu realizacji Umowy;
 - c) nie powielać Informacji Poufnych w zakresie szerszym, niż jest to potrzebne dla realizacji Umowy;
 - d) zabezpieczać otrzymane Informacje Poufne przed dostępem osób nieuprawnionych w stopniu niezbędnym do zachowania ich poufnego charakteru.
4. Wykonawca może, jeżeli jest to potrzebne do realizacji Umowy, udostępnić Informacje Poufne personelowi Wykonawcy (pracownikom, współpracownikom) oraz podwykonawcom, przy czym dostęp do Informacji Poufnych oraz korzystanie z Informacji Poufnych przez te osoby i podmioty nie może wykroczyć poza zakres, w jakim Wykonawca może z nich korzystać. Wykonawca zobowiąże te osoby i podmioty do przestrzegania poufności. Wykonawca jest odpowiedzialny za naruszenia spowodowane przez takie osoby i podmioty.
5. W przypadku rozwiązania Umowy (niezależnie od powodu rozwiązania) lub jej wygaśnięcia, Wykonawca zobowiązuje się do niezwłocznego zwrotu w terminie 14 dni materiałów zawierających Informacje Poufne, a Informacje Poufne przechowywane w wersji elektronicznej usunie ze swoich zasobów i nośników elektronicznych. Ten sam obowiązek będzie ciążył na osobach i podmiotach, o których mowa w poprzednim ustępie.
6. Wykonawca zobowiązuje się na pisemne żądanie Zamawiającego niezwłocznie zniszczyć materiały zawierające Informacje Poufne.
7. Niezależnie od kar umownych opisanych w § 9 Umowy, Zamawiający ma prawo naliczyć kary umowne w przypadku naruszenia zasad ochrony Informacji Poufnych – w wysokości 20 000 zł (słownie: dwadzieścia tysięcy złotych) za każdy przypadek naruszenia.

BŁ

§ 8 Wynagrodzenie

1. Łączna wartość wynagrodzenia nie może przekroczyć kwoty zł brutto (słownie: złotych 00/100), w tym wynagrodzenie netto w wysokości zł (słownie: złotych 00/100) oraz podatek VAT w wysokości zł (słownie:złotych 00/100).
Wynagrodzenie w kwocie zł płatne: dział 750 rozdział 75023 § 4300 zadanie IT/W/023/00/10/0360 "Funkcjonowanie Urzędu Miasta Lublin" projektu budżetu miasta na 2019 rok. Wynagrodzenie za wykonanie przedmiotu Umowy w poszczególnych latach kalendarzowych jej obowiązywania nie może przekroczyć środków budżetowych przewidzianych w budżecie miasta na te lata.
 2. Wynagrodzenie, o którym mowa w ust. 1 będzie wypłacane Wykonawcy w ratach ratach miesięcznych i zgodnie z zapisami § 3 ust. 13 i 14 na koniec każdego miesiąca kalendarzowego trwania Umowy.
 3. Podstawą wypłaty Wykonawcy wynagrodzenia, o którym mowa w ust. 2 jest poprawnie wystawiona przez Wykonawcę faktura VAT z zaakceptowanym przez Zamawiającego raportem miesięcznym zawierającym wykaz potwierdzający wykonanie czynności oraz kalkulację wynagrodzenia za asystę oraz czynności dodatkowe.
 4. Wynagrodzenie zostanie wpłacone na rachunek Wykonawcy wskazany na fakturze VAT, w terminie 21 dni od dnia otrzymania przez Zamawiającego poprawnie wystawionej faktury VAT wraz z raportem.
 5. Zamawiający upoważnia Wykonawcę do wystawienia faktury VAT bez jego podpisu.
 6. Z tytułu realizacji zamówienia Wykonawca oświadcza, iż wyśle/nie wyśle* ustrukturyzowaną fakturę elektroniczną w sposób, o którym mowa w art. 4 ust. 1 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U z 2018 r. poz.2191) z uwzględnieniem właściwego numeru GLN 5907653870019 Zamawiającego.
- * niepotrzebne skreślić

§ 9 Kary umowne

1. W przypadku niedotrzymania terminu przekazania Zamawiającemu aktualnej dokumentacji użytkowej Systemu, o której mowa w § 3 ust. 2 Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
2. W przypadku niedotrzymania terminu usunięcia awarii Systemu, o którym mowa w § 3 lit. a Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
3. W przypadku niedotrzymania terminu usunięcia błędu Systemu, o którym mowa w § 3 lit. b Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
4. W przypadku niedotrzymania terminu usunięcia usterki Systemu, o którym mowa w § 3 lit. c Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
5. W przypadku niedotrzymania terminu przekazania Zamawiającemu aktualnej dokumentacji użytkowej Systemu albo aneksu do dokumentacji użytkowej

- Systemu, o którym mowa w §3 ust. 6 Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
6. W przypadku niedotrzymania terminu wykonania zmian w środowisku Zamawiającego, określonego przez Zamawiającego w przyjętym przez Wykonawcę zleceniu, o którym mowa w §3 ust. 5 Umowy, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100).
 7. Kary, o których mowa w ust. 1-6 powyżej, nie będą miały zastosowania, kiedy niedotrzymanie terminu realizacji nastąpi z przyczyn technicznych lub technologicznych, nie leżących po stronie Wykonawcy.
 8. W przypadku odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy zapłaci on Zamawiającemu karę umowną w wysokości 20 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1 Umowy.
 9. W przypadku odstąpienia od Umowy z przyczyn leżących po stronie Zamawiającego zapłaci on Wykonawcy karę umowną w wysokości 20 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1 Umowy.
 10. Zamawiający może dokonać potrącenia kar umownych z wynagrodzenia przysługującego Wykonawcy, po uprzednim pisemnym powiadomieniu Wykonawcy o potrąceniu i o jego wysokości.

§ 10 Siła wyższa

1. Strony uznają niedotrzymanie lub opóźnienie terminu wykonania przedmiotu Umowy uniemożliwiające należyte wykonanie obowiązków za usprawiedliwione, jeśli zostały spowodowane przez okoliczności, które powstały na skutek działania siły wyższej.
2. W przypadku wystąpienia siły wyższej Strona dotknięta jej działaniem, niezwłocznie, nie później jednak niż w ciągu dwóch dni, od kiedy nawiązanie komunikacji stanie się możliwe, przekaże drugiej Stronie pisemną informację o zaistnieniu siły wyższej i jej przewidywanych skutkach dla realizacji Umowy oraz, o ile będzie to możliwe, przedstawi niebudzące wątpliwości dokumenty potwierdzające jej wystąpienie.
3. Strony niezwłocznie, lecz nie później niż w ciągu pięciu dni roboczych od dnia otrzymania powyższej informacji, uzgodnią na piśmie tryb dalszego postępowania w przedmiocie realizacji Umowy.

§ 11 Odpowiedzialność Wykonawcy

1. W przypadku powstania szkody przewyższającej wysokość kar umownych określonych w Umowie, Zamawiający uprawniony jest do dochodzenia naprawienia szkody na zasadach ogólnych określonych w Kodeksie Cywilnym, z wyłączeniem utraconych korzyści oraz z zastrzeżeniem ust. 2 poniżej.
2. Łączna odpowiedzialność Wykonawcy z jakiegokolwiek tytułu związanego z realizacją Umowy (m.in. kary umowne, odszkodowanie uzupełniające itp.), dla wszystkich zdarzeń, przez cały okres obowiązywania Umowy nie przekroczy 50% wynagrodzenia brutto, określonego w § 8 ust. 1 Umowy.
3. W przypadku wystąpienia awarii, błędu lub usterki Wykonawca zobowiązuje się usuwać przyczyny ich powstania, a pojawienie się tej samej awarii, błędu czy usterki w przeciągu kolejnych 7 dni będzie traktowane jako nienależyte wykona-

nie Umowy.

4. Wykonawca zobowiązuje się, że wykonując przedmiot Umowy nie naruszy praw majątkowych osób trzecich.

§ 12 Ograniczenia odpowiedzialności Wykonawcy

1. Wykonawca nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy wynikające z działania siły wyższej lub gdy niewykonanie lub nienależyte wykonanie nastąpi z przyczyn nie leżących po stronie Wykonawcy.
2. Wykonawca nie ponosi odpowiedzialności za szkody wynikłe z nieprawidłowego działania lub zaprzestania funkcjonowania Systemu spowodowane:
 - a) uszkodzeniem Systemu na skutek niezgodnionego z Wykonawcą, nieprawidłowego używania lub naprawiania Systemu przez Zamawiającego;
 - b) uszkodzeniami mechanicznymi, termicznymi, chemicznymi, przepięciami elektrycznymi wywołanymi przyczynami nie leżącymi po stronie Wykonawcy lub wynikającymi z działania siły wyższej;
 - c) błędami Systemu na skutek używania przez Zamawiającego niezgodnionego z Wykonawcą oprogramowania osób trzecich, mogącego mieć znaczenie dla poprawności i efektywności pracy Systemu;
 - d) błędami Systemu na skutek wprowadzenia przez Zamawiającego do używania sprzętu niezgodnionego z Wykonawcą, mogącego mieć znaczenie dla poprawności i efektywności pracy Systemu;
 - e) błędami Systemu na skutek nieuprawnionej ingerencji w kod źródłowy lub wynikowy Systemu;
 - f) błędami Systemu na skutek zmian w konfiguracji sprzętowej lub systemowej, które wprowadzono bez uzgodnienia z Wykonawcą;
 - g) korzystaniem z Systemu przez osoby nieupoważnione i nieprzeszkolone w związku z udostępnieniem hasła dostępu przez pracownika Zamawiającego.

§ 13 Czas trwania umowy

1. Umowa zostaje zawarta na okres 6 miesięcy.
2. Umowa wchodzi w życie z dniem zawarcia.

§ 14 Zmiany umowy

Zmiana postanowień Umowy może nastąpić wyłącznie za zgodą obu Stron wyrażoną w formie pisemnego aneksu pod rygorem nieważności.

§ 15 Odstąpienie od umowy

1. Niezależnie od podstaw odstąpienia od Umowy przewidzianych w przepisach prawa, Zamawiający zastrzega sobie również prawo do odstąpienia od Umowy w przypadkach, gdy:
 - a) Wykonawca nie przystąpi do realizacji przedmiotu Umowy;
 - b) Wykonawca będzie wykonywał Umowę w sposób nienależyty, w szczególności dopuści się naruszenia postanowień Umowy;
 - c) zostanie rozwiązana umowa powierzenia przetwarzania danych osobowych, o której mowa w § 6 Umowy, zgodnie z § 8 ust. 3 Załącznika nr 1 do Umowy;
 - d) Wykonawca nie podpisze umowy powierzenia przetwarzania danych osobowych, w terminie wskazanym w § 6 ust. 2 Umowy.

2. Strony mogą odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o okolicznościach uzasadniających odstąpienie.

§ 16 Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie przepisy obowiązującego prawa, m.in. Kodeks Cywilny.
2. W przypadku powstania sporów w trakcie realizacji Umowy, Strony dołożą starań zmierzających do polubownego ich rozstrzygnięcia.
3. W przypadku niemożności polubownego załatwienia sporów, Strony ustalają, że będą one rozstrzygane w drodze postępowania sądowego przez sąd właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w dwóch egzemplarzach, po jednym dla każdej ze Stron.

.....
(Zamawiający)

.....
(Wykonawca)

.....
(Kontrasygndata Skarbnika)

Radca Prawny


Anna Bukowska

ZASTĘPCA DYREKTORA
Wydziału Informatyki i Komunikacji

ZAŁĄCZNIK NR 1 - WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu pomiędzy:
....., z siedzibą w (kod:)
przy ulicy, NIP, REGON,
zwany dalej Administratorem danych osobowych lub
Administratorem, reprezentowanym przez :

1)

a

....., z siedzibą w (kod:)
przy ulicy, NIP, REGON,
zwany 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 **Świadczenie usługi asysty technicznej Systemu Zarządzania Ruchem ITS Gminy Lublin wraz z podsystemami oraz Transfer wiedzy dla administratorów** 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

By

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). Jakikolwiek 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 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

B4

✍

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) uczestnicy ruchu drogowego na obszarze objętym monitoringiem wizyjnym
 - b) uczestnicy ruchu drogowego na obszarze objętym Systemem Automatycznego Rozpoznawania Tablic Rejestracyjnych
2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:
 - a) co do uczestników ruchu drogowego na obszarze objętym monitoringiem wizyjnym i Systemem Automatycznego Rozpoznawania Tablic Rejestracyjnych: wizerunek oraz numery rejestracyjne pojazdów

Przetwarzający uprawniony 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.

BY

3

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 serwisowania systemów użytkowanych przez Centrum Sterowania Ruchem Wydziału Zarządzania Ruchem Drogowym i Mobilnością administrowanych przez Wydział Informatyki i Telekomunikacji.
2. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: przeglądanie baz danych w celu określenia źródeł ewentualnych usterek w celu ich usunięcia..
3. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych.
4. Przetwarzający będzie zbierał/otrzymywał dane osobowe zdalnie poprzez połączenie VPN.

§ 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) przekaze 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 przekaze wyniki tej analizy do Administratora ,
 - c) przekaze 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) jakiegokolwiek 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.

Bu

cf

§ 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 przekaze 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 (opisano szczegółowo w umowie głównej)

§ 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)

ZASTĘPCA DYREKTORA
Wydziału Informatyki i Telekomunikacji

Jarosław Buczek

Radca Prawny
Anna Bukowska

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).

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

- a) system kontroli dostępu: czytnik linii papilarnych;
- b) zamykanie drzwi – dostęp z zamkiem elektronicznym;
- c) zdalny domofon – dostęp ograniczony;
- d) urządzenia do nadzoru - system alarmowy oraz monitoring CCTV z nagrywaniem.

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) hasła dostępu do danych współdzielonych: minimalna długość 8 znaków, duża i mała litera, cyfra, znak specjalny, regularna zmiana hasła;
- b) szyfrowanie nośników danych dla urządzeń komputerowych wynoszonych poza siedzibę Podmiotu Przetwarzającego;
- c) regularne testowanie dostępu, ocena środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania

3. Kontrola dostępu do danych

Ryzyko dostępu do danych przez osoby nieuprawnione

Wymagane zabezpieczenia:

- a) zróżnicowane prawa dostępu: grupy uprawnień;
- b) unikalny identyfikator użytkownika;
- c) usuwanie danych po zakończeniu realizacji zlecenia;

4. Kontrola ujawniania

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) Podpis elektroniczny.

5. Zasada rozliczalności wprowadzanych danych

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

Wymagane zabezpieczenia:

- a) kontrola logowania;
- b) dokumentowanie wprowadzania i zmian danych w aplikacjach

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) Replikacja danych, technologia RAID;
- c) Nieprzerwana dostawa zasilania (UPS);
- d) Systemy antywirusowe / firewalle;
- e) Plan odzyskiwania na wypadek katastrofy;
- f) Regularne skanowanie.

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) Instrukcja RODO

Podmiot Przetwarzający
Podpis:

Imię, nazwisko, data

Administrator
Podpis:

Imię, nazwisko, data

ZASTĘPCA DYREKTORA
Wydziału Informatyki i Telekomunikacji
Jarosław Buczek