**Załącznik nr 5 do Warunków Zamówienia**

**Umowa powierzenia przetwarzania danych osobowych  
stanowiąca uzupełnienie Umowy ....................**

zawarta w dniu .................... w ...................., pomiędzy:

pomiędzy

Starostą Otwockim – Panem Tomaszem Laskusem, zwanym w dalszej części umowy „Administratorem"

a

…………………………………………..……………….., z siedzibą ……………………..………, przy ul. ………………………………………………………….…………, NIP: ………………….., reprezentowana przez ……………………………………………………………………………………

zwany w dalszej części „Podmiotem Przetwarzającym” lub „Przetwarzającym”

zwanymi dalej łącznie „Stronami" lub każda z osobna „Stroną”.

Mając na uwadze, że:

1. Strony zawarły umowę nr CRU/……../KT/2024 z dnia …………….., na usuwanie pojazdów oraz ich elementów z drogi i umieszczanie ich na parkingu strzeżonym   
   w Zarządzie Dróg Powiatowych w Otwocku z/s w Karczewie, ul. Bohaterów Westerplatte 36 w przypadkach określonych w art. 130a ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (tekst jedn. Dz. U. z 2024 r., poz. 1251) na obszarze powiatu otwockiego, dalej „**Umowa Podstawowa**”, w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;
2. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;
3. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1) – dalej **RODO**.

Strony postanowiły zawrzeć Umowę o następującej treści:

**§ 1** **Opis Przetwarzania**

1. Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.
2. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
3. Charakter i cel przetwarzania wynikają z Umowy Podstawowej.
4. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób: właścicieli pojazdów, w szczególności w następującym zakresie:
5. imiona i nazwiska,
6. dane usuniętych pojazdów:
7. rodzaj pojazdu,
8. markę i model pojazdu,
9. numer rejestracyjny pojazdu,
10. numer dyspozycji usunięcia pojazdu,
11. datę i godzinę usunięcia pojazdu,
12. datę i godzinę umieszczenia pojazdu na parkingu,

do których dostęp jest wymagany celem wykonania Umowy Podstawowej.

**§ 2 Podpowierzenie**

Przetwarzający nie jest upoważniony do powierzenia jakiejkolwiek operacji na danych innemu podmiotowi.

**§ 3 Obowiązki Przetwarzającego**

* 1. Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.
  2. Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.
  3. Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.
  4. Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).
  5. Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

**Zasady zachowania poufności**

1. Podmiot 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 („dane poufne”).
2. Podmiot Przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania   
   w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane   
   bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy Głównej,   
   chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy Głównej.

Do wykonywania zobowiązań wynikających z postanowień Umowy Głównej powierzenia mogą być dopuszczone wyłącznie osoby, które podpisały klauzulę poufności w zakresie określonym w ust. 1 i 2 lub są zobowiązane do zachowania ich w tajemnicy na mocy odrębnych przepisów, w szczególności przepisów dotyczących tajemnicy zawodowej.

**§ 4 Obowiązki Administratora**

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

**§ 5 Powiadomienie o Naruszeniach Danych Osobowych**

1. Przetwarzający niezwłocznie powiadamia Inspektora Ochrony Danych działającego u Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych, jednak w miarę możliwości nie później niż w ciągu 24 godzin od wykrycia naruszenia, umożliwia Administratorowi oraz Inspektorowi Ochrony Danych uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
2. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.
3. Powiadomienie powinno zawierać co do zasady wszystkie dostępne informacje o okolicznościach naruszenia, niezbędne do dokonania jego oceny m.in.:
   1. datę i godzinę zdarzenia (jeśli jest znana; w razie potrzeby możliwe jest określenie w przybliżeniu),
   2. datę i godzinę, kiedy Podmiot Przetwarzający powziął informację o zdarzeniu;
   3. opis charakteru i okoliczności naruszenia (w tym wskazanie, na czym polegało naruszenie, określenie miejsca, w którym fizycznie doszło do naruszenia, wskazanie nośników,   
      na których znajdowały się dane będące przedmiotem naruszenia),
   4. kategorie i przybliżoną liczbę wpisów (rekordów), których dotyczyło naruszenie,
   5. kategorie i przybliżoną liczbę osób, których dotyczyło naruszenie,
   6. opis potencjalnych konsekwencji i niekorzystnych skutków naruszenia dla osób, których dane dotyczą,
   7. opis środków technicznych i organizacyjnych, które zostały lub mają być zastosowane   
      w celu złagodzenia potencjalnych niekorzystnych skutków naruszenia,
   8. imię, nazwisko i dane kontaktowe do osoby, od której można uzyskać więcej informacji na temat zgłoszonego naruszenia.

**§ 6 Nadzór**

Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do (i) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz (ii) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

**§ 7 Oświadczenia Stron**

* 1. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
  2. Przetwarzający oświadcza, że w związku z powierzeniem przetwarzania danych zobowiązuję się do przestrzegania zasad związanych z ochroną danych osobowych, w tym przyjętą u Administratora Polityką Bezpieczeństwa Informacji, a także na polecenie Administratora do uczestniczenia w szkoleniach dotyczących ochrony danych osobowych.

**§ 8 Odpowiedzialność**

1. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.
2. Podmiot Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy Głównej, a w szczególności za udostępnienie powierzonych do przetwarzania danych nieuprawnionym osobom trzecim. W takim przypadku Administrator jest uprawniony do nałożenia kary umownej w wysokości 5.000,00 zł (słownie: pięć tysięcy złotych). Kara będzie należna Administratorowi bez konieczności wykazywania wysokości poniesionej szkody przez Administratora.
3. Administrator zastrzega sobie prawo do żądania od Podmiotu Przetwarzającego odszkodowania przenoszącego wysokość kary umownej.

**§ 9 Postanowienia Końcowe**

* 1. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

1. Umowa została zawarta na czas obowiązywania Umowy Podstawowej.
   1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
   2. Umowa podlega prawu polskiemu oraz RODO.

ADMINISTARTOR PRZETWARZAJĄCY

**ZAŁĄCZNIK A DO UMOWY POWIERZENIA DANYCH OSOBOWYCH**

**Ankieta z informacjami dotyczącymi zabezpieczeń**

Wyjaśnienie: (podstawa prawna) Zgodnie z art. 28 ust. 1 Rozporządzenia, Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich Podmiotów Przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”.

|  |  |
| --- | --- |
| **Podmiot Przetwarzający:** |  |
| **Imię i nazwisko osoby wypełniającej** |  |
| **Stanowisko** |  |
| **Adres e-mail i nr telefonu** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PYTANIA DOTYCZĄCE WIARYGODNOŚCI I WIEDZY FACHOWEJ** | | **TAK** | **NIE** | **NIE DOTYCZY** | **OCENA\*** |
| 1 | Cz*y* w Państwa Firmie wyznaczono Inspektor Ochrony Danych (dalej: IOD)? |  |  |  |  |
| Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe IOD. |  |  |  |  |
| 2 | W przypadku braku konieczności powołania IOD - *Czy* w Państwa Firmie wyznaczono osobę odpowiedzialną za ochronę danych osobowych? |  |  |  |  |
| Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe osoby, która w Państwa Firmie jest odpowiedzialna za ochronę danych osobowych. |  |  |  |  |
| 3 | Czy w Państwa Firmie opracowano politykę bezpieczeństwa lub inną dokumentację opisującą zasady ochrony danych osobowych w organizacji? |  |  |  |  |
| 4 | Czy w ciągu ostatnich dwóch lat przeprowadzono w Państwa Firmie kompleksowy audyt zgodności z przepisami o ochronie danych osobowych? |  |  |  |  |
| 5 | Czy w Państwa Firmie zostały wypracowane zasady usuwania powierzonych danych osobowych z chwilą rozwiązania umowy o współpracę? |  |  |  |  |
| 6 | Czy w Państwa Firmie zostały wypracowane zasady realizacji praw jednostki w zakresie ochrony danych osobowych, o którym mowa w art. 15-22 RODO\*\* w ramach, których Państwa Firma będzie wspierała Administratora |  |  |  |  |
| 7 | Czy Państwa Firma dokonała oceny skutków dla ochrony danych osobowych dla czynności przetwarzania (o których mowa w art. 35 RODO\*\* i w wykazie rodzajów operacji przetwarzania danych wymagających oceny skutków dla ochrony ich danych, opublikowanym w komunikacie Prezesa Urzędu Ochrony Danych Osobowych), a które wchodzą w zakres planowanej współpracy z Administratorem |  |  |  |  |
| **PYTANIA DOTYCZĄCE DOSTĘPU DO DANYCH PRZEZ PODMIOTY TRZECIE** | |  |  |  |  |
| 9 | Czy Państwa Firma zawiera umowy powierzenia danych  osobowych zgodnie z art. 28 RODO ze wszystkimi  podmiotami przetwarzającymi? |  |  |  |  |
| **PYTANIA DOTYCZĄCE BEZPIECZEŃSTWA FIZYCZNEGO** | |  |  |  |  |
| 10 | Czy w Państwa Firmie obowiązują procedury dotyczące  nadawania fizycznego dostępu do pomieszczeń, w których przechowywana jest dokumentacja zawierająca dane osobowe, zapewniające weryfikację tożsamości i zakresu nadawanego dostępu? |  |  |  |  |
| 11 | Czy w Państwa Firmie istnieją mechanizmy kontroli dostępu to tych pomieszczeń? |  |  |  |  |
| 12 | Czy Państwa Firma posiada działający system alarmowy oraz system monitoringu przemysłowego obejmujący miejsca, gdzie przechowywana jest dokumentacja zawierająca dane osobowe oraz inne dane osób fizycznych? |  |  |  |  |
| **PYTANIE DOTYCZĄCE STSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA W ŚRODOWISKU INFORMATYCZNYM** | |  |  |  |  |
| 13 | Czy Państwa Firma zabezpiecza komputery osobiste oraz  inne urządzenia (np. tablety, smartfony), na których przetwarzane są dane osób fizycznych? |  |  |  |  |
| 14 | Czy Państwa Firma zapewnia jednoznaczną identyfikację działań w systemach informatycznych za pomocą  unikalnego ID Użytkownika? |  |  |  |  |
| 15 | Czy system, w którym miałyby być przetwarzane dane  osobowe, posiada funkcjonalności pozwalające na jednoznaczne wskazanie i odtworzenie działań użytkownika o konkretnym ID, w określonym czasie? |  |  |  |  |
| 16 | Czy Państwa Firma posiada formalne zasady zarządzania  hasłami (minimalna długość, złożoność, częstotliwość zmiany, możliwość powtórnego użycia hasła, szyfrowanie przechowywanych haseł), które są wdrożone? |  |  |  |  |
| 17 | Czy urządzenia (np. tablety, smartfony), i komputery  osobiste, na których przetwarzane są dane osób fizycznych, mają włączoną automatyczne blokowanie ekranu po okresie bezczynności użytkownika? |  |  |  |  |
| 18 | Czy Państwa Firma prowadzi monitorowanie nieudanych  prób zalogowania się do systemu oraz blokowanie konta po określonej nieudanej liczbie prób zalogowania? |  |  |  |  |
| 19 | Czy Państwa Firma jest właścicielem infrastruktury fizycznej (serwerownia, serwery) na której funkcjonują systemy IT, w których będą przetwarzane dane osobowe oraz inne dane? |  |  |  |  |
| 20 | Czy Państwa Firma wykonywała testy bezpieczeństwa swojego środowiska informatycznego? Jeśli tak, uprzejmie prosimy o udostępnienie wyników. |  |  |  |  |
| 21 | Czy w Państwa Firmie została wyznaczona osoba odpowiedzialna za bezpieczeństwo IT? |  |  |  |  |
| Jeśli tak, proszę podać dane kontaktowe tej osoby (imię, nazwisko, nr telefonu, adres e-mail). |  |  |  |  |
| 22 | Czy w Państwa firmie stosowane są rozwiązania chmury publicznej (cloud computing)? |  |  |  |  |
| Jeżeli tak, to jakie? |  |  |  |  |
| 23 | Czy rozwiązanie chmurowe pozwala na przetwarzanie danych zgodnie z obowiązującymi regulacjami? |  |  |  |  |
| 24 | W przypadku stosowania rozwiązań w chmurze, czy stosowane są metody ograniczające dostęp do danych dla osób nieuprawnionych np. szyfrowanie danych? |  |  |  |  |
| 25 | Czy systemy IT w Państwa Firmie, w których są przetwarzane dane osobowe, zarządzane są przez podmiot zewnętrzny? |  |  |  |  |
| 26 | Jeśli administratorem systemu IT lub dostawcą utrzymującym system w Państwa Firmie jest podmiot zewnętrzny, proszę wskazać, czy posiada on zdalny dostęp do środowiska IT? |  |  |  |  |
| 27 | Czy użytkownicy mają dostęp zdalny do zasobów?  Jeśli tak, to w jaki sposób zabezpieczony jest kanał  Komunikacji? |  |  |  |  |

……………………………………………….………………..

(data, pieczątka, podpis osoby wypełniającej ankietę)