

GCI.DZP.261.2.1.2025.KM

Gdynia, dnia 27 stycznia 2025 r.

WYJAŚNIENIE I ZMIANA TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA w postępowaniu na asystę techniczną i konserwację systemu KSAT200i (ogłoszenie o zamówieniu zostało zamieszczone w Biuletynie Zamówień Publicznych pod numerem 2025/BZP 00053287/01 z dnia 21 stycznia 2025 r.)

Zamawiający na podstawie art. 284 ust. 2 i 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r., poz. 1320 z późn. zm.) – dalej „Pzp” – udziela wyjaśnień treści specyfikacji warunków zamówienia – dalej „SWZ” – oraz udostępnia treść zapytania z dnia 27.01.2025 r. złożonego w przedmiotowym postępowaniu wraz z wyjaśnieniem, bez ujawniania źródła zapytania.

Pytanie nr 1:

Dzień dobry,

proszę o wyjaśnienie jak należy wypełnić formularz cenowy: w pozycji asysta techniczna skreślona jest ilość zaś cena netto dotyczy ceny jednostkowej, więc nie da się wyjść na wartość brutto z rachunku kolumna 3 razy kolumna 6? Co rzutuje na dalsze wyliczenia....

Dodatkowo zwracam uwagę na zapisy w zał. nr 3 projekt umowy dot. par. 8 ust. 2: "Łączna wysokość kar umownych, dla wszystkich zdarzeń, przez cały okres obowiązywania Umowy, nie może przekroczyć 20 % kwoty netto, o której mowa w § 6 ust. 1 Umowy.", gdzie powinno być par. 6 ust. 2.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że w pozycji nr 1 tj. „Asysta techniczna i konserwacja system KSAT2000i”, kolumna nr 3 jest przekreślona, ponieważ w tej pozycji w kolumnie nr 4 wpisują Państwo cenę netto za całą usługę asysty technicznej i konserwacji systemu KSAT2000i na okres 8 miesięcy. Tym samym w pozycji nr 1 w kolumnie nr 6 i nr 7 cena brutto będzie taka sama.

Dodatkowo Zamawiający w *Załączniku nr 3 do SWZ (Projekt Umowy)* w § 8 ust. 2 dopatrył się omyłki pisarskiej. W związku z powyższym Zamawiający na podstawie art. 286 ust. 1 Pzp w § 8 ust. 2 Załącznika nr 3 do SWZ (Projekt umowy) wprowadza następujące zmiany:

„2. Łączna wysokość kar umownych, dla wszystkich zdarzeń, przez cały okres obowiązywania Umowy, nie może przekroczyć 20 % kwoty netto, o której mowa w § 6 ust. 2 pkt 1 Umowy.”

Zmieniony Załącznik nr 3 do SWZ (Projekt umowy) zawierający wprowadzone zmiany stanowi Załącznik nr 1 do niniejszego pisma.

Zamawiający nie przedłuża terminu składania ofert.

Zgodnie z art. 513 pkt 1 Pzp mają Państwo prawo wnieść odwołanie.

Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej, zgodnie z art. 514 ust. 1 Pzp. Odwołujący jest zobowiązany przekazać zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej przed upływem terminu do wniesienia odwołania, w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu, zgodnie z art. 514 ust. 2 i 3 Pzp.

Jako że wyjaśnienia treści SWZ zostały przekazane przy użyciu środków komunikacji elektronicznej i zamieszczone na stronie internetowej prowadzonego postępowania, to termin wniesienia odwołania do Prezesa Krajowej Izby Odwoławczej oraz przesłania kopii odwołania do Zamawiającego upływa w dniu 3.02.2025 r., czyli po 5 dniach od przekazania wykonawcom treści zapytań wraz z wyjaśnieniem treści SWZ, zgodnie z art. 515 ust. 1 pkt 2 lit. a Pzp.

Załączniki:

1. Załącznik nr 3 – Projekt umowy

PROJEKT UMOWY

zawarta pomiędzy:

Gminą Miasta Gdyni, z siedzibą w Gdyni, 81-382, przy Al. Marszałka Piłsudskiego 52/54, NIP 5862312326, REGON 191675557, **Gdyńskie Centrum Informatyki jednostka budżetowa**, 81-310, Gdynia, ul. Śląska 35-37, NIP 5862363714, REGON 387844850 reprezentowaną przez:

.....,
zwanym w dalszej części umowy „**Zamawiającym**”,

a

.....,
zwaną dalej „**Wykonawcą**”,

zwanymi dalej „**Stronami**”, a każda z osobna „**Stroną**”,

po przeprowadzeniu postępowania o udzielenie zamówienia publicznego nr GCI.DZP.261.2.1.2025.KM prowadzonego na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2011 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r., poz. 1320 z późn. zm.) w trybie w trybie podstawowym z możliwością prowadzenia negocjacji w celu ulepszenia treści ofert, w ramach przewidzianych w SWZ kryteriów oceny została zawarta umowa serwisowa nr, zwana dalej „**Umową**”, o następującej treści:

§ 1.

Dla potrzeb realizacji niniejszej Umowy Strony przyjmują następujące definicje:

1. **System** – Systemem KSAT2000i do którego całość autorskich praw majątkowych posiada COIG S.A.;
2. **Moduł/Submoduł** – część Systemu realizującą grupę powiązanych tematycznie funkcji;
3. **Błąd** – stan Systemu, rozumiany jako ograniczenie możliwości przetwarzania; Wyróżnia się następujące rodzaje błędów: Błąd krytyczny, Błąd wysoki, Błąd średni;
4. **Błąd krytyczny** – stan Systemu, rozumiany jako brak możliwości przetwarzania, charakteryzujący się całkowitym brakiem możliwości uzyskania efektów jego pracy, odpowiadających ustalonym przez Wykonawcę założeniom funkcjonalnym Systemu, w postaci rejestracji zdarzeń, wyszukiwania i edycji danych, dokonywania obliczeń, generowania zestawień i raportów;

5. **Błąd wysoki** – stan Systemu, rozumiany jako ograniczona możliwość przetwarzania, w którym uzyskanie efektów jego pracy, odpowiadających ustalonym przez Wykonawcę założeniom funkcjonalnym Systemu, w postaci rejestracji zdarzeń, wyszukiwania i edycji danych, dokonywania obliczeń, generowania zestawień i raportów jest możliwe dopiero po zastosowaniu odpowiednich procedur wskazanych przez Wykonawcę;
6. **Błąd średni** – stan Systemu, w którym nie występuje ograniczenie możliwości realizacji zakładanych przez Wykonawcę funkcjonalności Systemu, występuje jednak obniżenie jakości warunków pracy w zakresie obsługiwanej funkcjonalności Systemu;
7. **Interwencja Serwisowa** – działania Wykonawcy podjęte w wyniku zgłoszenia przez Zamawiającego Błędów w działaniu Systemu, mające na celu przywrócenie ciągłości i poprawności funkcjonowania Systemu;
8. **Dzień roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej;
9. **Procedura zastępcza** - zaproponowane przez Wykonawcę rozwiązanie tymczasowe mające na celu zmniejszenie uciążliwości Błędu i zapewnienie realizacji funkcji Systemu do czasu naprawienia Błędu;
10. **Użytkownik Systemu** – pracownik jednostki obsługiwanej przez Zamawiającego korzystający z Systemu, który zapoznał się z dokumentacją Systemu, posiada podstawową wiedzę dotyczącą obsługi komputera i posiada wiedzę na temat zasad działania Systemu;
11. **Powierzający** – Gdyńskie Centrum Informatyki – powierzające dane w imieniu i na rzecz jednostki obsługiwanej – Urzędu Miasta Gdyni, w rzeczywistości podpowierzający dane osobowe, o których mowa w niniejszej umowie.

§ 2.

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę usług serwisu i bieżącej konserwacji nad wdrożonym w jednostce obsługiwanej przez Zamawiającego Systemem w zakresie niżej wymienionych Modułów i funkcjonalności:
 - 1) Administrator Systemów Aplikacji (ASA),
 - 2) Centralna Kartoteka Kontrahentów (CKK);
 - 3) Egzekucja (EGZ);
 - 4) Ewidencja Koncesji Alkoholowych (ALK);
 - 5) Fakturowanie (FA);
 - 6) Gospodarka Mieniem Komunalnym (GMK);
 - 7) Gospodarka Odpadami (GOP);
 - 8) Księga Główna (KG);
 - 9) Należności i Zobowiązania (NZ);
 - 10) Organizacja Pracy Urzędu (ORG);
 - 11) Repozytorium Systemu (RS);
 - 12) Sprawozdawczość Budżetowa (SPR);
 - 13) Podatki (POD).

2. W ramach Umowy Wykonawca zobowiązuje się do zapewnienia ciągłości funkcjonowania Systemu, poprzez realizację następujących świadczeń:

- 1) dostosowanie Systemu do zmian prawnych wynikających ze zmiany powszechnie obowiązujących przepisów prawa z wyłączeniem aktów prawa miejscowego w rozumieniu art. 87 ust. 2 oraz art. 94 Konstytucji Rzeczypospolitej Polskiej. Terminy realizacji prac ustala się na:
 - a) 7 dni przed dniem wejścia w życie przepisu prawa, dla którego ustalono *vacatio legis*,
 - b) 21 dni od dnia ogłoszenia zmiany przepisów prawa w przypadku przepisów, dla których nie ustalono *vacatio legis*, lub dla których *vacatio legis* jest krótsze niż 7 dni, z zastrzeżeniem, że termin na dostosowanie Systemu w żadnym z powyższych przypadków nie będzie krótszy niż 21 dni,
- 2) dostosowanie Systemu według procedur Wykonawcy i zapewnienie jego działania na aktualnych wersjach LTS (Long Term Support) systemów operacyjnych. Przyjmuje się, że czas obowiązywania danej wersji systemu operacyjnego jest tożsamy z terminem zakończenia otrzymywania przez niego wsparcia technicznego,
- 3) usuwanie zgłoszonych Błędów Systemu,
- 4) w przypadku aktualizacji Systemu, przekazywania Zamawiającemu drogą elektroniczną wykazu wprowadzonych zmian w stosunku do poprzedniej wersji Systemu wraz z ich opisem oraz instrukcji użytkownika, w terminie 14 dni od daty wprowadzenia aktualizacji Systemu,
- 5) udzielanie Użytkownikom Systemu telefonicznej pomocy konsultacyjnej i doradczej („hot-line”) związanej z funkcjonowaniem Systemu, w zakresie obejmującym uprzednio przesłane zgłoszenia serwisowe lub wynikającym ze zgłoszonych Błędów Systemu, która realizowana będzie w Dni robocze, w godzinach od 8:00 do 16:00,
- 6) aktualizacje Systemu/Modułu do najnowszej wersji, zgodnie z przyjętą przez Wykonawcę polityką wersjonowania. O możliwości aktualizacji Systemu/Modułu Zamawiający zostanie poinformowany z 3-dniowym wyprzedzeniem lub krótszym, jeśli Strony na to wyrażą zgodę. Zamawiający ma prawo do korzystania z pełnej funkcjonalności nowej wersji Systemu/Modułu,
- 7) pomocy w formie konsultacji, w usuwaniu problemów w funkcjonowaniu Systemu powstałych z przyczyn niezależnych od Systemu wynikających z niewłaściwej obsługi Systemu przez Użytkownika.

§ 3.

1. Świadczenia, o których mowa w § 2 ust. 2 pkt 1 Umowy, odnoszą się wyłącznie do zakresu funkcjonalnego Systemu, wskazanego w § 2 ust. 1 Umowy i nie obejmują one adaptacji Systemu do uregulowań prawnych wykraczających poza aktualny zakres funkcjonalny Systemu
2. W sytuacji, gdy z przyczyn obiektywnych lub leżących po stronie Zamawiającego albo konieczności wprowadzenia istotnych zmian funkcjonalnych Systemu dochowanie terminów, o których mowa w § 2 ust. 2 pkt 1 Umowy, będzie niemożliwe lub wprowadzenie zmian w Systemie we wskazanych terminach nie będzie konieczne, Strony przewidują możliwość przedłużenia tych terminów lub wprowadzenia harmonogramu dostosowania. W takiej sytuacji, przed upływem wskazanych w § 2 ust. 2 pkt. 1 Umowy,

Wykonawca zwróci się do Zamawiającego z wnioskiem o wydłużenie terminu, wskazując proponowaną datę wykonania prac. W przypadku braku zgody Zamawiającego na zaproponowane przez Wykonawcę terminy, prace zostaną wykonane zgodnie z Umową.

3. Realizacja usług określonych § 2 ust. 2 pkt 1 i 3 niniejszego paragrafu, odbywać się będzie w szczególności poprzez aktualizację Systemu lub Modułu Systemu. O sposobie realizacji usług decyduje Wykonawca.
4. W przypadku Błędów krytycznych Wykonawca może wdrożyć procedurę zastępczą, która umożliwi przywrócenie ciągłości funkcjonowania Systemu, informując o tym fakcie Zamawiającego. Zastosowanie procedury zastępczej skutkuje zmianą kategorii Błędu z kategorii krytyczny na wysoki.
5. Zamawiającemu przysługuje prawo do stworzenia listy zmian usprawniających działanie systemu (tzw. „prac rozwojowych”), które Wykonawca przeanalizuje pod kątem możliwości realizacji, o ile ich pracochłonność nie przekracza 100 roboczogodzin. Warunkiem realizacji prac rozwojowych, o których mowa w zdaniu poprzednim, jest stwierdzenie i uzasadnienie przez Wykonawcę wnioskowanych przez Zamawiającego zgłoszeń za nie naruszające dotychczasowej koncepcji architektonicznej systemu. Wykonawca ma prawo odmówić realizacji wnioskowanych funkcji programowych wraz z pełnym uzasadnieniem odmowy w sytuacji, w której wymagałyby one zmian w architekturze systemu tzn.:
 - 1) naruszałyby integralność danych w systemie,
 - 2) zmieniałyby przeznaczenie atrybutów w bazie danych,
 - 3) zmieniałyby algorytmy stosowane w systemie w sposób taki, że odbiegałyby od ogólnie przyjętych zasad, tj. ogólnej koncepcji systemu
6. Świadczone w ramach Umowy usługi nie obejmują oprogramowania systemu wirtualizacyjnego, systemu operacyjnego, serwera bazodanowego oraz serwera aplikacyjnego oraz wadliwego funkcjonowania Systemu spowodowanego nieprawidłową pracą tego oprogramowania.
7. Zamawiający jest uprawniony do złożenia zamówienia opcjonalnego a Wykonawca zobowiązany jest do jego wykonania tj. usługi obejmującej zwiększenie liczby godzin rozwojowych, o których mowa w ust. 5 niniejszego paragrafu, do 30 godzin w stosunku do pierwotnie określonej liczby godzin rozwojowych.
8. Realizacja zamówienia opcjonalnego odbędzie się na podstawie informacji (Zlecenia opcji), którą Zamawiający przekaze Wykonawcy w formie pisemnej pod rygorem nieważności lub w formie elektronicznej. Zamawiający może złożyć więcej niż jedno Zawiadomienie w ramach Prawa Opcji do wyczerpania liczby godzin wskazanych w ust. 7 niniejszego paragrafu. Wzór zlecenia opcji stanowi Załącznik nr 5 do Umowy.
9. Zamawiający skorzysta z prawa opcji o ile będzie posiadał środki finansowe na jego zrealizowanie i uzasadnioną potrzebę zakupu. Zamówienie opcjonalne nie stanowi zobowiązania Zamawiającego do jego udzielenia, jak również nie stanowi podstawy do dochodzenia przez Wykonawcę roszczeń odszkodowawczych z tytułu niezłożenia tego zamówienia.
10. Decyzja o realizacji lub rezygnacji z Zamówienia opcjonalnego jest wyłącznym uprawnieniem Zamawiającego, przy czym Zamawiający ma prawo skorzystać z możliwości udzielenia zamówienia opcjonalnego w terminie do dnia 30.09.2025 r. Brak decyzji w tym terminie oznacza, że Zamówienie opcjonalne nie będzie realizowane.
11. Wykonawca zrealizuje przedmiot zamówienia opcjonalnego w terminie do dnia 31 października 2025 r.

12. Zasady odbiorów, rozliczenia dot. zamówienia podstawowego stosuje się odpowiednio do zamówienia opcjonalnego.

§ 4.

1. Obsługa zgłoszeń serwisowych odbywać się będzie zgodnie z procedurą opisaną w **Załączniku nr 1** do Umowy pn. „**Procedura Zapewnienia Ciągłości Funkcjonowania Systemu (CFS)**”.
2. Zgłoszenia serwisowe realizowane będą wyłącznie przez osoby upoważnione przez Zamawiającego, wymienione w **Załączniku nr 2** do Umowy „**Lista Przedstawicieli Zamawiającego**”, zwanych dalej „Przedstawicielami Zamawiającego”. Zmiana Załącznika nr 2 nie stanowi zmiany Umowy. O każdorazowej zmianie Załącznika nr 2 Zamawiający jest zobowiązany powiadomić pisemnie, niezwłocznie Wykonawcę przedkładając mu aktualizację Załącznika nr 2. Wykonawca nie ponosi jakiejkolwiek odpowiedzialności za niedopełnienie przez Zamawiającego obowiązku, o którym mowa w zdaniu poprzednim, w szczególności za niezrealizowanie zgłoszeń serwisowych wykonanych przez osoby nie wskazane w Załączniku nr 2.
3. Strony ustalają, że wszelkie zgłoszenia Zamawiającego, co do sposobu działania Systemu, niespełniające kryteriów Błędu, zawartych w § 1 pkt 3 – 6 Umowy, traktowane będą jako funkcjonalności dodatkowe i realizowane będą dopiero na mocy odrębnych zmian lub ustaleń z puli godzin rozwojowych, o których mowa w § 3 ust. 5 i 7 Umowy, z jednoczesnym ich zamknięciem na portalu zgłoszeń serwisowych przez Wykonawcę.
4. Wszelkie zgłoszenia Zamawiającego, z wyjątkiem zgłoszeń Interwencji Serwisowych realizowanych na podstawie Umowy, powinny być dokonywane na adres mailowy Wykonawcy: lub poprzez zgłoszenie jako Zlecenie usługi w portalu zgłoszeń serwisowych pod adresem
5. W zakresie wprowadzonych zmian Systemu, o których mowa w § 2 ust. 2 pkt 1-4 i pkt 6 Umowy, Zamawiający uzyskuje uprawnienia do korzystania z Systemu na warunkach określonych w ramach udzielonych licencji na System.

§ 5.

1. Zamawiający dopuszcza realizację umowy zdalnie. W tym celu Zamawiający zapewni Wykonawcy zdalny dostęp do Systemu dla celów serwisowych o przepustowości min. 10Mb/s. Zdalny dostęp realizowany będzie w ramach kanału VPN.
2. Kanał VPN, o którym mowa w ust. 1 niniejszego paragrafu uruchamiany będzie każdorazowo na żądanie Wykonawcy w dni robocze w godzinach 8:00-16:00. W przypadku konieczności połączenia poza godzinami wskazanymi w zdaniu poprzednim, Wykonawca zgłasza taką konieczność Zamawiającemu najpóźniej do godz. 14:00 dnia roboczego przed planowanym rozpoczęciem prac. Zamawiający nie przewiduje włączania kanału VPN na czas nieokreślony. Wykonawca przedstawi Zamawiającemu listę osób uprawnionych do otrzymania zdalnego dostępu. Wykonawca jest zobowiązany do aktualizacji tej listy w przypadku zaistnienia zmian.
3. W przypadku braku możliwości zdalnego dostępu, o którym mowa w ust. 1 i 2, wynikającego z przyczyn leżących po stronie Zamawiającego, Wykonawca zobowiązuje się do podjęcia próby realizacji usługi zdalnie przy użyciu oprogramowania przeznaczonego do zdalnego sterowania systemem operacyjnym

poprzez Internet bez konieczności instalacji serwera lub klienta w pamięci masowej komputera, niezależnych od działania kanału VPN. Jeśli próba zdalna, o której mowa w zdaniu poprzednim nie przyniesie oczekiwanych rezultatów, Wykonawca zobowiązany jest do wykonania usługi w siedzibie Zamawiającego, po uprzednim uzgodnieniu terminu wizyty oraz zakresu usługi.

4. W przypadku braku możliwości zdalnego dostępu, o którym mowa w ust. 1 i 2, z przyczyn losowych niezależnych od Zamawiającego, Strony dołożą wszelkich starań, aby przywrócić zdalny dostęp w możliwie najkrótszym czasie. Do momentu przywrócenia dostępu czas reakcji i przywrócenia ciągłości pracy Systemu mogą ulec odpowiedniemu wydłużeniu.
5. Zamawiający zobowiązuje się do zapewnienia niezbędnego współdziałania przy wykonaniu Umowy, a w szczególności zobowiązuje się do:
 - 1) dochowania terminów wszelkich obustronnie ustalanych kontaktów roboczych oraz zaplanowanych prac;
 - 2) uzgadniania z Wykonawcą wszelkich planowanych zmian sprzętowych i systemowych mogących mieć znaczenie dla poprawności i efektywności pracy Systemu;
 - 3) czynnej współpracy z Wykonawcą w zakresie realizacji postanowień § 3 Umowy. W sytuacji tego wymagającej Zamawiający zobowiązuje się do wprowadzenia wszelkich niezbędnych uzupełnień do baz danych, modułów Systemu oraz weryfikacji ich poprawności w porozumieniu z Wykonawcą;
 - 4) umożliwienia wykorzystania oprogramowania TeamViewer udostępnionego przez Wykonawcę w celu realizacji prac serwisowych bezpośrednio na stacjach roboczych Użytkownika pod nadzorem Zamawiającego;
 - 5) terminowego regulowania zobowiązań wynikających z § 6 Umowy.
6. Wszelkie zgłoszenia Interwencji Serwisowej powinny być kierowane za pośrednictwem portalu zgłoszeń serwisowych pod adresem w sposób określony w rozdziale I Załącznika nr 1 do Umowy. W przypadku braku możliwości wykonania zgłoszenia na portalu zgłoszeń serwisowych z przyczyn technicznych leżących po stronie Zamawiającego lub Wykonawcy, Zamawiający będzie mógł dokonać zgłoszenia za pomocą telefonu pod numerem 32 757 44 44 lub e-mail: Wykonawca zastrzega, że zgłoszenia serwisowe kierowane w inny sposób niż określone powyżej mogą zostać niezrealizowane, za co Wykonawca nie ponosi odpowiedzialności.

§ 6.

1. Wysokość miesięcznego wynagrodzenia za usługi stanowiące przedmiot Umowy zamówienia podstawowego wynosi **zł netto** (słownie złotych:) tj. wraz z 23% podatkiem VAT (słownie złotych:).
2. Całkowita wartość Umowy wynosi:
 - 1) w ramach zamówienia podstawowego **zł netto** (słownie złotych... tj. wraz z 23% podatkiem VAT **zł brutto** (słownie złotych.....),
 - 2) w ramach zamówienia opcjonalnego **zł netto** (słownie złotych... tj. wraz z 23% podatkiem VAT **zł brutto** (słownie złotych.....).

3. Wynagrodzenie określone w ust. 1 płatne jest z dołu przelewem na rachunek bankowy wskazany w fakturze VAT wystawionej przez Wykonawcę, w terminie do 14 dni od daty otrzymania prawidłowo wystawionej faktury przez Zamawiającego.
4. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany na fakturze jest rachunkiem, dla którego zgodnie z rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (tj. Dz. U. z 2024 poz.1646) prowadzony jest rachunek VAT. Płatności realizowane będą w trybie podzielonej płatności, tzw. split payment.
5. Dniem zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego.
6. W przypadku opóźnienia Zamawiającego w zapłacie wynagrodzenia, o którym mowa w ust. 1 niniejszego paragrafu Wykonawcy przysługują odsetki ustawowe za opóźnienie.
7. Faktury opisywane będą w następujący sposób:
Nabywca: Gmina Miasta Gdyni, Al. Marsz. Piłsudskiego 52/54, 81-382 Gdynia, NIP 5862312326
Odbiorca: Gdyńskie Centrum Informatyki ul. Ślaska 35-37, 81-310 Gdynia.
8. Zamawiający dopuszcza przesyłanie faktur w formacie .pdf na adres: faktury@gci.gdynia.pl

§ 7.

1. Strony są zwolnione od odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy, jeżeli na realizację jej postanowień miała wpływ siła wyższa.
2. Przez pojęcie siły wyższej Strony zgodnie rozumieją zdarzenie nagle, zewnętrzne, niemożliwe do przewidzenia i niezależne od Stron, któremu nie można zapobiec, ani przeciwdziałać przy zachowaniu należytej staranności, a w szczególności:
 - 1) klęski żywiołowe np. pożar, powódź, susza, trzęsienie ziemi, huragany, itd.;
 - 2) niezapowiedziane przerwy w dostawie energii elektrycznej;
 - 3) strajki o zasięgu krajowym;
 - 4) akty władzy państwowej np. stan wojenny, stan wyjątkowy;
 - 5) działania wojenne, akty sabotażu i terroryzmu;
 - 6) blokady i embarga niezależnie od ich statusu prawnego.
3. 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.
4. 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.

§ 8.

1. W przypadku zwłoki Wykonawcy w usunięciu Błędu powstałej z przyczyn leżących wyłącznie po stronie Wykonawcy, Zamawiający ma prawo do naliczania kar umownych w wysokości 0,2% wartości

wynagrodzenia netto, o którym mowa w § 6 ust. 1 Umowy, za każdą pełną dobę zwłoki w stosunku do terminów określonych pkt. II ppkt 1 i 2 Załącznika nr 1 do Umowy.

2. Łączna wysokość kar umownych, dla wszystkich zdarzeń, przez cały okres obowiązywania Umowy, nie może przekroczyć 20 % kwoty netto, o której mowa w § 6 ust. 2 pkt 1 Umowy.
3. Kary umowne, o których mowa w ust. 1, płatne będą na wezwanie Zamawiającego, w terminie przez niego wskazanym, nie krótszym jednak niż 14 dni od dnia otrzymania wezwania przez Wykonawcę.
4. Wykonawca wyraża zgodę na potrącenie naliczonych kar umownych z należnego mu wynagrodzenia po uprzednim poinformowaniu przez Zamawiającego o naliczonej wysokości kary umownej. Naliczenie kary umownej będzie przez Zamawiającego udokumentowane odpowiednią notą księgową i przesłane na adres e-mail Wykonawcy albo listem poleconym za potwierdzeniem odbioru.
5. Strony zastrzegają sobie prawo dochodzenia odszkodowań przewyższających kary umowne na zasadach ogólnych.

§ 9.

1. Wykonawca nie ponosi odpowiedzialności za:
 - 1) treść i integralność danych, otrzymywanych i przechowywanych w Systemie;
 - 2) jakiegokolwiek szkody wynikłe z nieprawidłowego działania lub zaprzestania funkcjonowania Systemu związane z nieprawidłowym korzystaniem z Systemu przez użytkownika Systemu i Zamawiającego;
 - 3) korzystanie z Systemu przez osoby nieupoważnione, z winy Zamawiającego,
 - 4) udostępnienie hasła lub jakichkolwiek innych informacji identyfikujących Zamawiającego względem Wykonawcy, włącznie z treścią wiadomości przekazywanych przez Zamawiającego lub przez niego odbieranych, osobom upoważnionym na podstawie właściwych przepisów prawa lub umów z podmiotami trzecimi, które biorą udział w świadczeniu usług,
 - 5) niewykonanie albo nienależyte wykonanie Umowy w przypadku Błędów Systemu spowodowanych nieprawidłowym działaniem oprogramowania wirtualizacyjnego, operacyjnego, bazodanowego oraz innego oprogramowania firm trzecich.
2. Odpowiedzialność Wykonawcy nie obejmuje w szczególności:
 - 1) uszkodzeń spowodowanych nieprawidłowym użytkowaniem lub naprawami Systemu dokonanymi przez Zamawiającego lub osobę trzecią nieuprawnioną przez Wykonawcę,
 - 2) uszkodzeń mechanicznych, termicznych, chemicznych, przepięć elektrycznych, itp., wywołanych przyczyną zewnętrzną lub przez Zamawiającego, lub przez osobę trzecią nieuprawnioną przez Wykonawcę,
 - 3) błędów wynikających z używania przez Zamawiającego oprogramowania osób trzecich lub sprzętu, w szczególności niezgodnego z wymaganiami Systemu,
 - 4) braku funkcjonalności Systemu nie zapisanych w specyfikacji Systemu lub dokumentacji,
 - 5) nieprawidłowości w działaniu Systemu wynikających z nieuprawnionej ingerencji w kod źródłowy lub wynikowy Systemu,
 - 6) problemów wynikłych ze zmian w konfiguracji sprzętowej lub systemowej Systemu dokonanych bez autoryzacji Wykonawcy,

- 7) utraconych korzyści Zamawiającego.
3. Wykonawca zobowiązuje się informować Zamawiającego na bieżąco o wymaganej przez System konfiguracji sprzętowej, programowej i systemowej oraz o planowanych zmianach w tym zakresie, z co najmniej trzy miesięcznym wyprzedzeniem.
 4. Wykonawca nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy, które spowodowane było okolicznościami, za które odpowiada Zamawiający lub osoby trzecie, zależne od Zamawiającego oraz wynikających z działania siły wyższej.
 5. Wykonawca nie ponosi odpowiedzialności za gromadzone w Systemie treści oraz dane i nie wykonuje jakiegokolwiek kontroli działań Użytkowników Systemu w tym zakresie. Wykonawca nie ponosi odpowiedzialności za szkody polegające na utracie danych, kosztach związanych z ich odtworzeniem oraz niemożnością korzystania z danych utraconych przez Zamawiającego w trakcie wykonywania Umowy. Obowiązek sporządzenia kopii zapasowych danych aktualnych i archiwalnych oraz odtwarzania utraconych lub zmienionych danych obciąża wyłącznie Zamawiającego.
 6. Łączna odpowiedzialność Wykonawcy z jakiegokolwiek tytułu związanego z Umową ograniczona jest do kwoty stanowiącej pełne wynagrodzenie netto, określonego § 6 ust. 2 Umowy, z zastrzeżeniem ograniczeń ustalonych w § 8 ust. 2 i 5 Umowy oraz z zastrzeżeniem bezwzględnie obowiązujących przepisów prawa.

§ 10.

1. Każda ze Stron zobowiązuje się traktować jako informacje poufne, wszelkie informacje dotyczące drugiej Strony, uzyskane w związku z zawarciem i realizacją Umowy niezależnie od sposobu ich wyrażenia (ustne, pisemne, elektroniczne itd.) oraz nośnika, na którym zostały zapisane (Informacje Poufne).
2. Informacjami Poufnymi będą w szczególności informacje i dokumenty przekazywane przez Zamawiającego w celu wykonywania Umowy, jak również informacje i dokumenty, które znalazły się w posiadaniu drugiej Strony w związku z zawarciem oraz wykonywaniem Umowy. Informacjami Poufnymi są w szczególności dane finansowe, informacje organizacyjne, informacje dotyczące produktów informatycznych oraz inne informacje o działalności każdej ze Stron, jak też treść rezultatów prac powstałych w wyniku realizacji Umowy.
3. Strony zobowiązane są w szczególności do:
 - 1) nieujawniania i nierozpowszechniania Informacji Poufnych drugiej Strony oraz niewykorzystywania ich do celów innych niż realizacja Umowy,
 - 2) przechowywania Informacji Poufnych drugiej Strony w sposób uniemożliwiający dostęp do nich osób nieuprawnionych oraz zabezpieczenia Informacji Poufnych drugiej Strony w taki sposób, w jaki Strona zabezpiecza własne Informacje Poufne.
4. Informacje Poufne nie będą przez żadną ze Stron ujawniane, rozpowszechniane i udostępniane w jakikolwiek sposób osobom trzecim, bez wyraźnej pisemnej zgody drugiej Strony. Nie dotyczy to jednakże ujawniania Informacji Poufnych podmiotom współpracującym ze Stroną przy realizacji Umowy – w zakresie niezbędnym do realizacji Umowy oraz audytorom i doradcom prawnym Stron, o ile

zobowiążą się oni do zachowania poufności przekazywanych informacji na warunkach nie gorszych niż wynikające z Umowy.

5. Strony uprawnione są do przekazywania Informacji Poufnych swoim pracownikom oraz podwykonawcom, gdy jest to konieczne do wykonania Umowy. W takim przypadku ponoszą odpowiedzialność za naruszenie zasad poufności przez pracowników i podwykonawców, jak za własne działania bądź zaniechania.
6. Informacji poufnych nie stanowią informacje, które:
 - 1) są powszechnie znane,
 - 2) zostały uzyskane przez Stronę we własnym zakresie, w sposób nie naruszający postanowień Umowy oraz obowiązujących przepisów prawa i Strona jest uprawniona do dysponowania nimi,
 - 3) ujawniane są na podstawie bezwzględnie obowiązujących przepisów prawa, na podstawie decyzji albo orzeczenia uprawnionego organu publicznego.
7. W wypadku, gdy Strona zostanie zobowiązana nakazem sądu bądź organu publicznego do ujawnienia Informacji Poufnych albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie drugą Stronę oraz poinformować odbiorcę Informacji Poufnych o ich poufnym charakterze.
8. Osoby, za pomocą których Wykonawca wykonuje zobowiązania wynikające z Umowy, zobowiązane są do podpisania oświadczenia o zachowaniu poufności.
9. Obowiązek poufności, o którym mowa wyżej, wiąże Strony również przez okres 5 lat od wygaśnięcia lub rozwiązania Umowy.

§ 11.

1. Zamawiający jako Powierzający i Podpowierzający – na podstawie Porozumienia SOO.031.6.2021 w sprawie powierzenia przetwarzania danych osobowych zawartego w dniu 1 kwietnia 2021 r. między Urzędem Miasta Gdyni a Gdynskim Centrum Informatyki (dalej „**Powierzający**”), powierza Wykonawcy (w roli **Podmiotu Przetwarzającego**), na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (DZ.Urz.UE.L.nr 119) (dalej „**RODO**”), przetwarzanie danych osobowych wyłącznie w zakresie określonym Umową, związanym z serwisem i aktualizacją Systemu.
2. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie odczytu danych i ich usuwanie, w rozumieniu art. 4 pkt. 2 RODO (dalej „**Przetwarzanie Danych Osobowych**”).
3. Powierzający powierza Wykonawcy do Przetwarzania Dane Osobowe zawarte w **Załączniku nr 3** do Umowy („**Kategorie osób, rodzaj i zakres danych osobowych powierzonych do przetwarzania**”).
4. Powierzający powierza Wykonawcy Przetwarzanie Danych Osobowych, w celu o którym mowa w ust. 1 i w zakresie, o którym mowa w ust. 3.

5. Wykonawca będzie Przetwarzał Dane Osobowe w ramach powierzenia Przetwarzania Danych Osobowych wyłącznie w celu i w zakresie niezbędnym do wykonania Umowy. Wykonawca nie może zmieniać celu ani zakresu danych osobowych powierzonych do przetwarzania.
6. Wykonawca oświadcza, że dysponuje środkami umożliwiającymi prawidłowe Przetwarzanie Danych Osobowych powierzonych przez Powierzającego, w zakresie i celu określonym Umową.
7. Wykonawca zobowiązuje się, że będzie Przetwarzał Dane Osobowe, w tym uzyskiwał do nich dostęp, w ramach Infrastruktury Informatycznej, z zastrzeżeniem ust. 8. Przez Infrastrukturę Informatyczną rozumie się całokształt rozwiązań sprzętowo-programowych i organizacyjnych stanowiących podstawę wdrożenia i eksploatacji systemów informatycznych. Wykonawca oświadcza, iż Infrastruktura Informatyczna znajduje się na terenie Rzeczypospolitej Polskiej.
8. Wykonawca może Przetwarzać Dane Osobowe, o których mowa w ust. 2 Umowy także w postaci papierowej, o ile będzie to uzasadnione wykonaniem Umowy.
9. W przypadku planowania zmian w sposobie przetwarzania danych, Wykonawca zobowiązuje się do stosowania wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i zobowiązuje się do informowania Powierzającego z wyprzedzeniem o planowanych zmianach, a wyprzedzenie to ma umożliwić Powierzającemu realną możliwość reagowania, jeżeli planowane zmiany w opinii Powierzającego zagrażają bezpieczeństwu danych lub zwiększają ryzyko naruszenia praw i wolności osób fizycznych.
10. Na wniosek Powierzającego lub osoby, której dane dotyczą, Wykonawca wskaże dokładne miejsca, w których przetwarza powierzone dane.
11. Wykonawca zobowiązuje się:
 - 1) podejmować wszelkie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa, w tym środki o których mowa w art. 32 RODO;
 - 2) umożliwić Powierzającemu na każde żądanie dokonania oceny stosowanych środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z prawem, a także uaktualniać te środki, o ile są one niewystarczające do tego, aby zapewnić zgodne z prawem przetwarzanie powierzonych danych osobowych;
 - 3) pomagać Powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. W szczególności Wykonawca zobowiązuje się przekazywać Powierzającemu informacje oraz wykonywać jego polecenia dotyczące stosowanych środków zabezpieczenia danych osobowych, przypadków naruszenia ochrony danych osobowych oraz zawiadamiania o tym organu nadzorczego lub osób, których dane osobowe dotyczą, przeprowadzenia oceny skutków dla ochrony danych oraz uprzednich konsultacji z organem nadzorczym i wdrożenia zaleceń organu;
 - 4) po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłaszać je pisemnie Powierzającemu na adres: gci@gci.gdynia.pl. Informacja o naruszeniu powinna zawierać wszystkie elementy określone w art. 33 ust.3 RODO, niezbędne Powierzającemu do reagowania na naruszenie. Informacje te w różnym zakresie mogą być dosyłane sukcesywnie, ale niezwłocznie po ich ustaleniu;
 - 5) pomagać Powierzającemu, poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądanie osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 15-22 RODO;

- 6) umożliwić przeprowadzenie audytów lub inspekcji w zakresie zgodności operacji przetwarzania danych osobowych z prawem i Umową. Audyty lub inspekcje o których mowa powyżej mogą być przeprowadzone przez podmioty trzecie upoważnione przez Powierzającego;
 - 7) zwrócić lub usunąć po zakończeniu Umowy, zależnie od decyzji Powierzającego, wszelkie dane osobowe oraz usunąć wszelkie ich kopie;
 - 8) informować niezwłocznie Powierzającego, jeżeli zdaniem Wykonawcy wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych;
 - 9) stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, po uprzednim poinformowaniu Powierzającego, dotyczących Przetwarzania Danych Osobowych, w szczególności w zakresie stosowania RODO.
12. Wykonawca nie jest zobowiązany do wykonania polecenia Powierzającego dotyczącego stosowanych środków zabezpieczenia danych osobowych, w sytuacji gdyby ich zastosowanie mogło spowodować zagrożenie bezpieczeństwa danych osobowych.
 13. Wykonawca zobowiązuje się Przetwarzać Dane Osobowe zgodnie z udokumentowanymi poleceniami Powierzającego. Poprzez zawarcie niniejszej Umowy Powierzający poleca Przetwarzanie Danych Osobowych Wykonawcy, a także każdej osobie działającej z upoważnienia Wykonawcy mającej dostęp do tych danych. Niniejsze postanowienie Strony zgodnie uznają za udokumentowane polecenie Powierzającego, w rozumieniu art. 28 ust. 3 lit. a w związku z art. 29 RODO.
 14. Powierzający upoważnia Wykonawcę do nadawania upoważnień do Przetwarzania Danych Osobowych wyłącznie osobom o odpowiednich kwalifikacjach i odpowiednio przeszkolonych do prawidłowego wykonania Umowy oraz jednocześnie osobom, które zapewnią zachowanie poufności Powierzonych Danych Osobowych oraz sposobów ich zabezpieczania. Wykonawca we własnym zakresie prowadzi wykaz upoważnionych osób. Wykonawca jest zobowiązany na żądanie Powierzającego w terminie 7 dni od daty jego otrzymania, przekazać informacje o osobach, które dopuścił do Przetwarzania Danych Osobowych, wskazując imię, nazwisko oraz adres e-mail osób upoważnionych.
 15. Wykonawca oświadcza, że osoby zatrudnione przy Przetwarzaniu Danych Osobowych zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy Przetwarzanych Danych Osobowych i sposobów ich zabezpieczenia, na potwierdzenie czego odebrał od ww. osób stosowne oświadczenia.
 16. Powierzający nie udziela Wykonawcy ogólnej pisemnej zgody na Podpowierzenie Przetwarzania Danych Osobowych.
 17. Powierzającemu przysługuje prawo kontroli, czy środki zastosowane przez Wykonawcę i jego podwykonawców przy przetwarzaniu i zabezpieczaniu danych osobowych powierzonych do Przetwarzania, spełniają wymagania dotyczące ochrony danych osobowych, wynikające z bezwzględnie obowiązujących przepisów prawa, w tym przepisów Ustawy i RODO.
 18. Wykonawca zobowiązuje się do ścisłej współpracy podczas kontroli i udzielania Powierzającemu wszelkich informacji dotyczących sposobu przetwarzania i zabezpieczenia danych osobowych.

Powierzający będzie korzystał z prawa kontroli w dni robocze, w godzinach pracy Wykonawcy. Kontrola może zostać wykonana w formie:

- 1) wizji lokalnej miejsca Przetwarzania Danych Osobowych – w tym przypadku Strony uzgodnią termin kontroli jednak nie później niż 10 dni roboczych od powiadomienia Wykonawcy przez Powierzającego o zamiarze przeprowadzenia kontroli. Wizja lokalna na terenie siedziby Wykonawcy odbywać się będzie zgodnie z regulaminami wewnętrznymi obowiązującymi u Wykonawcy;
 - 2) pisemnego żądania przedstawienia określonych informacji dotyczących przetwarzania i zabezpieczenia danych osobowych;
19. Wykonawca zobowiązany jest udzielić niezwłocznie pisemnej odpowiedzi, na żądanie Powierzającego, w szczególności w przypadkach konieczności:
- 1) wyjaśniania okoliczności incydentów bezpieczeństwa;
 - 2) udzielenia przez Powierzającego odpowiedzi organom uprawnionym z mocy prawa do żądania informacji.
20. Powierzający może przekazać Wykonawcy w formie pisemnej istotne zalecenia pokontrolne Zamawiającego, a Wykonawca zobowiązuje się je zrealizować, o ile ich realizacja nie będzie niezgodna z bezwzględnie obowiązującymi przepisami prawa, w tym przepisami RODO oraz Umowy.
21. Wykonawca zobowiązuje się do niezwłocznego informowania Powierzającego:
- 1) o kontrolach, jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Wykonawcę danych osobowych na podstawie Umowy;
 - 2) o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym Przetwarzania Danych Osobowych, o których mowa powyżej, skierowanych do Wykonawcy,
 - 3) o wszelkich planowanych, o ile Wykonawcy są wiadome, lub realizowanych kontrolach dotyczących przetwarzania u Wykonawcy Danych Osobowych, o których mowa powyżej, w szczególności prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych.
22. W przypadku, gdy Powierzający zamierza uczestniczyć w postępowaniach i kontrolach, o których mowa w ust. 20, Wykonawca zobowiązany jest umożliwić Powierzającemu lub upoważnionej przez Powierzającego osobie uczestnictwo w takich czynnościach.
23. W ramach, w czasie i w zakresie świadczonych usług Wykonawca zobowiązuje się do zapoznania i przestrzegania Procedury bezpieczeństwa informacji w Urzędzie Miasta Gdyni w relacjach z podmiotami zewnętrznymi. Wyżej wymieniony dokument stanowi załącznik nr 6 do niniejszej Umowy.

§ 12.

1. Niniejsza Umowa obowiązuje przez osiem miesięcy począwszy od dnia 1 marca 2025 r. do dnia 31 października 2025 r.
2. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności, chyba że Umowa wyraźnie stanowi inaczej.

3. W razie rozbieżności między treścią Umowy, a innymi ustaleniami Stron wiążące są postanowienia Umowy.
4. Wszystkie załączniki stanowią integralną część Umowy.
5. W przypadku jakichkolwiek sporów wynikłych pomiędzy Stronami odnośnie zawarcia, interpretacji, wykonania i skutków prawnych Umowy, Strony w dobrej wierze podejmą negocjacje w celu polubownego rozstrzygnięcia sporu. W razie braku rozwiązania sporu na drodze polubownej Strony oddadzą spór pod rozstrzygnięcie polskiemu sądowi powszechnemu właściwemu dla siedziby Zamawiającego.
6. Za datę zawarcia niniejszej Umowy Strony uznają dzień złożenia kwalifikowanego podpisu elektronicznego przez z ostatnią z osób podpisujących w imieniu ostatniej ze Stron.
7. Umowa została sporządzona w formie elektronicznej i podpisana przez każdą ze Stron kwalifikowanym podpisem elektronicznym.

Załączniki:

- 1) *Procedura Zapewnienia Ciągłości Funkcjonowania Systemu (CFS),*
- 2) *Lista Przedstawicieli Zamawiającego,*
- 3) *Kategorie osób, rodzaj i zakres danych osobowych powierzonych do przetwarzania*
- 4) *Informacja o przetwarzaniu danych osobowych reprezentantów, w tym pełnomocników oraz osób wskazanych do kontaktu i współpracy przez Wykonawcę,*
- 5) *Procedura bezpieczeństwa informacji Gdyńskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi,*
- 6) *Procedura bezpieczeństwa informacji w Urzędzie Miasta Gdyni w relacjach z podmiotami zewnętrznymi.*
- 7) *Wzór zlecenia opcji*

ZAMAWIAJĄCY

WYKONAWCA

Procedura Zapewnienia Ciągłości Funkcjonowania Systemu (CFS)

I. Zgłoszenie Interwencji Serwisowej.

1. Zgłoszenie Interwencji Serwisowej przez Zamawiającego następuje za pośrednictwem portalu zgłoszeń serwisowych. Zarejestrowanie zgłoszenia jest jednoznaczne z przyjęciem do realizacji i nie wymaga dodatkowego potwierdzenia przez Wykonawcę.
2. Zgłoszenie Interwencji Serwisowej dokonane w Dni robocze po godzinie 16.00, w soboty oraz w dni ustawowo wolne od pracy, traktowane będzie jako przyjęte o godz. 8.00 następnego Dnia Roboczego.
3. Zgłoszenie Interwencji Serwisowej powinno zawierać: unikalny identyfikator, opis przypadku stanowiącego podstawę Interwencji Serwisowej, jeżeli to możliwe załącznik obrazujący zaistniały błąd, kategorię błędu, datę zgłoszenia, nazwę Modułu oraz dane pracownika Zamawiającego dokującego zgłoszenia. Zgłoszenie dotyczy pojedynczego problemu związanego z funkcjonowaniem Systemu/Modułu.
4. Osoba zgłaszająca Interwencję Serwisową jest zobowiązana do zachowania należytej staranności przy określaniu kategorii Błędu. Wykonawca na każdym etapie realizacji zgłoszenia Interwencji Serwisowej ma prawo do zmiany kategorii Błędu. W przypadku zakwestionowania przez Wykonawcę kategorii Błędu dokonanej przez Zamawiającego, Wykonawcy przysługuje prawo do zmiany kategorii Błędu. Stanowisko Wykonawcy dotyczące zmiany kategorii Błędu jest ostateczne.
5. Status Błąd krytyczny nadaje się następującym kategoriom zgłoszeń:
 - 1) zgłoszenia dotyczące błędów ujawnionych po aktualizacji Systemu i zarejestrowane do dwóch dni roboczych po aktualizacji;
 - 2) zgłoszenie błędów w działaniu modułu FKT ujawnionych w okresach: 10-15 dzień, 20-25 dzień każdego miesiąca;
 - 3) zgłoszenia dotyczące błędów w działaniu modułu NZ w zakresie sporządzenia deklaracji VAT ujawnionych w okresie 10-20 dzień każdego miesiąca;
 - 4) zgłoszenia dotyczące błędów w działaniu modułu NZ i KG w zakresie sporządzania sprawozdań finansowych miesięcznych i kwartalnych oraz zestawienia obrotów i sald i dziennika w okresie 5-15 dzień każdego miesiąca.
6. Wykonawca może złożyć protest w stosunku do zgłoszenia Interwencji Serwisowej w przypadku:
 - 1) dokonania zgłoszenia przez osoby inne niż wskazane w Załączniku nr 2 do Umowy;
 - 2) gdy zgłoszeniem objęto większą ilość Błędów, gdy do każdego z nich można przydzielić inną kategorię;
 - 3) brak jest uzasadnienia dla Interwencji Serwisowej, w szczególności określonego zgłoszeniem zdarzenia, nie można zakwalifikować jako Błąd Systemu,
 - 4) gdy zgłoszenie dotyczy Błędów objętych jeszcze nierozwiązanym zgłoszeniem Interwencji Serwisowej,
 - 5) gdy zgłoszenie dotyczy Błędów objętych jeszcze nieukończonym postępowaniem reklamacyjnym, o którym mowa w pkt. II ppkt. 3 poniżej.
7. Wykonawca może złożyć protest niezwłocznie, nie później jednak niż w terminie 2 Dni roboczych od daty zarejestrowania zgłoszenia Interwencji Serwisowej. Zgłoszenie protestu przez Wykonawcę skutkuje odrzuceniem zgłoszenia Interwencji Serwisowej, o czym Wykonawca powiadamia niezwłocznie Zamawiającego.
8. Do czasu rozpatrzenia protestu, o którym mowa w pkt. 6 powyżej, wstrzymywane są terminy realizacji zgłoszenia Interwencji Serwisowej, w stosunku do którego zgłoszono protest.

II. Realizacja Interwencji Serwisowej.

1. W przypadku Błędu krytycznego Interwencje Serwisowe podejmowane będą z czasem reakcji do ... godzin od momentu zarejestrowania zgłoszenia, zaś usunięcie Błędu Krytycznego powinno nastąpić w terminie ... godzin od zarejestrowania zgłoszenia.
2. W przypadkach Błędu wysokiego i średniego realizacja zgłoszeń Interwencji Serwisowych nastąpi w terminach:
 - 1) do ... Dni roboczych od zarejestrowania zgłoszenia – w przypadku Błędu kategorii wysoki,
 - 2) do ... Dni roboczych od zarejestrowania zgłoszenia – w przypadku Błędu kategorii średni.
3. Zamawiającemu przysługuje prawo zgłoszenie jednej reklamacji w stosunku do przeprowadzonej i rozwiązywanej Interwencji Serwisowej. Brak zgłoszenia reklamacji ze strony Zamawiającego w odniesieniu do przeprowadzonej Interwencji Serwisowej, oznacza skuteczne przywrócenie ciągłości funkcjonowania Systemu i usunięcie Błędu. Termin na zgłoszenie reklamacji upływa na koniec następnego Dnia roboczego liczonego od momentu rozwiązania zgłoszenia przez Wykonawcę.
4. W ramach zgłoszenia reklamacji nie jest dopuszczalne zgłoszenie przez Zamawiającego nowej Interwencji Serwisowej. Wszelkie Błędy, inne niż wynikające z Interwencji Serwisowej objętej reklamacją, powinny zostać objęte nowym zgłoszeniem serwisowym, na zasadach określonych w pkt. I powyżej. W przypadku zgłoszenia przez Zamawiającego reklamacji, Wykonawca ma prawo złożyć protest na zasadach obowiązujących dla Interwencji Serwisowej.
5. W przypadku zgłoszenia przez Zamawiającego reklamacji, Wykonawca zobowiązany jest ponownie podjąć czynności serwisowe, jednakże termin na usunięcie Błędu w ramach procedury reklamacji w żadnym razie nie będzie krótszy niż:
 - 1) 1 Dzień roboczy liczony od dnia zarejestrowania reklamacji - w przypadku reklamacji na usunięcie Błędu krytycznego,
 - 2) 10 Dni roboczych liczony od dnia zarejestrowania reklamacji - w przypadku reklamacji na usunięcie Błędu wysokiego,
 - 3) 14 Dni roboczych liczony od dnia zarejestrowania reklamacji - w przypadku reklamacji na usunięcie Błędu średniego.
6. Usunięcie Błędów objętych reklamacją, w terminach wskazanych w pkt. 5 powyżej, traktowane będzie jako należyta realizacja Interwencji Serwisowej i nie uprawnia Zamawiającego do nałożenia na Wykonawcę kar umownych. Na czynności serwisowe Wykonawcy, podjęte w wyniku zgłoszonej przez Zamawiającego reklamacji, reklamacja nie przysługuje.
7. Strony dopuszczają możliwość przedłużenia terminów realizacji Interwencji Serwisowych o których mowa w pkt. 1, 2 i 5 powyżej, w sytuacji, gdy z przyczyn nie leżących po Stronie Wykonawcy, dochowanie tych terminów nie będzie możliwe. W takiej sytuacji, przed upływem wskazanych powyżej terminów, Wykonawca zwróci się do Zamawiającego z wnioskiem o akceptację przedłużenia terminu realizacji zgłoszenia, wskazując datę jego wykonania. Akceptacja wniosku o przedłużenie terminu realizacji zgłoszenia powoduje, iż Wykonawca nie pozostaje w zwłoce w realizacji zgłoszenia i w konsekwencji Zamawiający nie jest uprawniony do nałożenia kary umownej na Wykonawcę. W przypadku niedotrzymania przedłużonego terminu realizacji zgłoszenia, Zamawiający uprawniony będzie do naliczenia Wykonawcy kary umownej za zwłokę liczoną od następnego dnia po upływie przedłużonego terminu.
8. W przypadku utraty ciągłości działania Systemu z winy infrastruktury Zamawiającego oraz oprogramowania firm trzecich, nie będących przedmiotem Umowy, Wykonawca doloży wszelkich starań, aby pomóc Zamawiającemu w rozwiązaniu problemu. W takim przypadku nie mają zastosowania terminy wskazane w pkt 1,2 i 5 niniejszego Załącznika.

Lista Przedstawicieli Zamawiającego

L.p .	Imię i Nazwisko	Adres email	Telefon
1			
2			
3			
4			

I Dane kontrahentów (CKK - CKK_KLIENCI)

1. Nazwa kontrahenta - pole scalone
2. Typ kontrahenta
3. Numer PESEL osoby fizycznej
4. Numer REGON osoby prawnej
5. Numer Ewidencji Podatkowej
6. Pierwsze imię osoby fizycznej
7. Drugie imię osoby fizycznej
8. Nazwisko osoby fizycznej - człón I
9. Nazwisko osoby fizycznej - człón II
10. Stan dokumentacji
11. Rodzaj kontrahenta
12. Kod kontrahenta
13. Imię ojca osoby fizycznej
14. Imię matki osoby fizycznej
15. Data urodzenia osoby fizycznej
16. Typ dokumentu tożsamości osoby fizycznej
17. Numer dokumentu tożsamości osoby fizycznej

Dane powiązane:

1. Adresy kontrahentów (CKK - CKK_ADRESY)
2. Cechy kontrahenta (CKK - CKK_CECHY)
3. Geografie urzędów skarbowych (CKK - CKK_GEOGRAFIE_US)
4. Podstawowe dane o kontrahencie (CKK - CKK_KLIENCI)
5. Powiązania kontrahentów z kodami Polskiej Klasyfikacji Działalności (CKK - CKK_KLIENCI_PKD)
6. Dane powiązań pomiędzy klientami (CKK - CKK_KLIENCI_POWIAZANIE)
7. Rachunki bankowe kontrahentów (CKK - CKK_KONTA)
8. Informacja zdefiniowana dla przedstawiciela i/lub kontrahenta. (CKK - CKK_KONTAKTY)
9. Notatki dotyczące kontrahentów (CKK - CKK_NOTATNIK)
10. Powiązanie pomiędzy parametrami a kontrahentami (CKK - CKK_PARAMETRY_KLIENTA)
11. Tabela pełnomocników klienta (CKK - CKK_PELNOMOCNICY)
12. Osoby fizyczne reprezentująca klienta (CKK - CKK_PRZEDSTAWICIELE)
13. Zgody klientów (CKK - CKK_ZGODY)
14. Rejestr vat sprzedaży (BUD - BUD_REJESTR_VAT_SPRZEDAZY)
15. Rejestr vat sprzedaży v17 (BUD - BUD_REJESTR_VAT_SPRZEDAZY_V17)
16. Firmy, sprzedaż alkoholu (ALK - EDG_ALK_FIRMY)
17. Opłaty dodatkowe – sprzedaż alkoholu (ALK - EDG_ALK_OPL_DOD)

18. Zmiany dotyczące aktualności punktów - sprzedaż alkoholu (ALK - EDG_ALK_WLAS)
19. Kontrahenci prowadzący punkty na sprzedaż alkoholu (ALK - EDG_KLIENT_ALK)
20. Dokumenty księgowe - sprzedaż alkoholu (ALK - EDG_NZ_KG)
21. Dane dotyczące organizatora targowiska (ALK - EDG_ORGANIZ_TARG)
22. Dokumenty dot. punktów i zdarzeń (ALK - EDG_PKT_CKK_NZ)
23. Dokumenty dot. punktów i zdarzeń, terminy płatności, raty (ALK - EDG_ZEZ_CKK_NZ)
24. Czynności (EGZ - EGZ_CZYNNOSCI)
25. Operacje wyciągów (EGZ - EGZ_OPERACJE_WYCIAGOW)
26. Pisma (EGZ - EGZ_PISMA)
27. Pobrania (EGZ - EGZ_POBRANIA)
28. Pozycje tytułu (EGZ - EGZ_POZYCJE_TYTULU)
29. Pozycje wyciągu (EGZ - EGZ_POZYCJE_WYCIAGU)
30. Przelewy (EGZ - EGZ_PRZELEWY)
31. Tytuły wykonawcze (EGZ - EGZ_TYTULY_WYKONAWCZE)
32. Zajęcia (EGZ - EGZ_ZAJECIA)
33. Zobowiązani tytuły wykonawcze (EGZ - EGZ_ZOBOWIAZANI_TW)
34. Dokumenty (GM - GM_DOKUMENTY)
35. Zamówienia potrzeb (GM - GM_POTRZEBY_ZAMOWIENIA)
36. Rezerwacje (GM - GM_REZERWACJE)
37. Stany na magazynie (GM - GM_STANY_NA_MAGAZYNIE)
38. Zamówienia zbiorcze (GM - GM_ZAMOWIENIA_ZBIORCZE)
39. Dane opisujące deklarację/naliczenie/decyzję (GOP - GOP_DEKLARACJE)
40. Obsługa dokumentów elektronicznych z EPUAP - elementy dokumentu (GOP - GOP_EPUAP_DOK_ELEMENTY)
41. Ewidencja klientów obiektów (GOP - GOP_KLIENCI_OBIEKTY)
42. Dekrety uzupełniające (KG - KG_DEKRETY_UZUPELNIAJACE)
43. wygenerowany plik dokumentu oraz jego dane nagłówkowe (KG - KG_JPK_FORMULARZE)
44. Klucze wyjściowe (KG - KG_KLUCZE_WYJ)
45. Ewidencja potwierdzeń sald (KG - KG_POTWIERDZENIA_SALD)
46. Pozycje automatów (KG - KG_POZYCJE_AUTOMATOW)
47. Przejściowe dekrety uzupełniające (KG - KG_PRZEJSCIOWE_DEKRETY_UZ)
48. Wzorce dokumentów (KG - KG_WZORCE_DOKUMENTOW)
49. Druki rejestracja (MD - MD_DRUKI)
50. Mandaty rejestracja (MD - MD_MANDATY)
51. Pracownicy dane (MD - MD_PRACOWNICY)
52. Zatrudnienia dane (MD - MD_ZATRUDNIENIA)
53. Dane wiarytelności przekazywanej do big (NZ - NZ_BIG_WIERZYTELNOSCI)
54. Rejestr biletów (NZ - NZ_BILETY)
55. Decyzje ratalne/odroczenia (NZ - NZ_DECYZJE)
56. Informacja o dekrétach dokumentów NZ (NZ - NZ_DEKRETY)
57. Dekrety BO (NZ - NZ_DEKRETY_BO)
58. Dekrety, polecenia księgowania (NZ - NZ_DEKRETY_PK_ZM)

59. Ewidencja deklaracji VAT7 (NZ - NZ_DEK_VAT7)
60. Powiązanie klientów solidarnie zobowiązanych z dokumentami (NZ - NZ_DOK_KL)
61. Główna tabela modułu NZ - zawiera informacje o dokumentach (przypisy, odpisy, wpłaty, zwroty, inne dokumenty) (NZ - NZ_DOKUMENTY)
62. Błoczki druków ścisłego zarachowania (NZ - NZ_DR_BLOCZKI)
63. Druki błoczka ścisłego zarachowania (NZ - NZ_DR_DRUKI)
64. Operacje na drukach (NZ - NZ_DR_OPERACJE)
65. Dziennik operacji dokumentu NZ (NZ - NZ_DZIENNIK)
66. Konfiguracja automatycznego tworzenia faktur/paragonów z zapłat (NZ - NZ_FAZ_KONF_FA)
67. Ewidencja hipotek (NZ - NZ_HIPOTEKI)
68. Ewidencja inkasentów – konto kwitariusze (NZ - NZ_IK_KONTOKWITARIUSZE)
69. Ewidencja inkasentów powiązanie z dokumentem (NZ - NZ_IK_KONTOKWIT_DOK)
70. Lista dla inkasentów pow. z CKK (NZ - NZ_IK_LISTY)
71. Pozycje listy inkasenci (NZ - NZ_IK_POZYCJE_LISTY)
72. Dane z importu z system. zewnętrznych (NZ - NZ_IMPORT_DOKUMENTY)
73. Ewidencja inkasentów punkty poboru opłat (NZ - NZ_INK_PUNKTY_POBORU)
74. Inkasencie wnioski - zwroty (NZ - NZ_INK_WNIOSKI_ZWROT)
75. Zasady definiowania limitów kwot wypłat (NZ - NZ_KWOTY_DO_LIMITOW)
76. Konfiguracja kartotek w ramach ewidencji należności płatnych cyklicznie (NZ - NZ_NALEZNOSCI_CYKL)
77. Ewidencja osób wykorzystywana w należnościach generowanych cyklicznie (NZ - NZ_NAL_KLIENT_CYKL)
78. Ewidencja współwłaścicieli (klientów) dla należności generowanych cyklicznie (NZ - NZ_NAL_WSPOL_CYKL)
79. Noty korygujące dokumentów NZ (NZ - NZ_NOTY_KORYGUJACE)
80. Dane komorników - w ramach funkcjonalności NZ_OBIEKTY (NZ - NZ_OB_KOMORNIK)
81. Powiązanie obiektów z klientami CKK (NZ - NZ_OB_OBIEKTY_KLIENCI)
82. Rejestr opłat - w ramach funkcjonalności NZ_OBIEKTY (NZ - NZ_OB_REJESTR_OPLAT)
83. Tytuły wykonawcze - w ramach funkcjonalności NZ_OBIEKTY (NZ - NZ_OB_TW)
84. Rejestr wierzyciela - w ramach funkcjonalności NZ_OBIEKTY (NZ - NZ_OB_WIERZ_REJESTR)
85. Zestawienie operacji z elektronicznego wyciągu bankowego - dane pobierane z plików bankowych (NZ - NZ_OPERACJE_WYCIAGOW)
86. Rejestr opłat parkingowych - funkcjonalność dedykowana (NZ - NZ_OPLATY_PARKINGOWE)
87. Główna encja - pismo (NZ - NZ_PISMA)
88. Słownik rodzajów pism (NZ - NZ_PIS_RODZAJE_PISM)
89. Strony pisma (NZ - NZ_PIS_STRONY)
90. Ewidencja zmian terminów w dokumencie PK-Przeksięgowania zapłat (NZ - NZ_PK_TPL)
91. Ewidencja terminów związanych z wyksięgowanie dokumentów zapłat innych (NZ - NZ_PK_TPL_INN)
92. Ewidencja pomocy publicznej w NZ (NZ - NZ_POMOC_PUBLICZNA)
93. Sprawozdanie z pomocy publicznej (NZ - NZ_POM_PUB_SPR)
94. Ewidencja postanowień o zarachowaniu zapłat/przedpłat/innych dokumentów (NZ - NZ_POSTANOWIENIA)
95. Pozycje postanowienia o zarachowaniu zapłaty (NZ - NZ_POZYCJE_POST)

96. Ewidencja punktów rejestracji spraw (słownik wydziałów sądów) (NZ - NZ_ROS_PUNKTY_REJESTRACJI)
97. Rozliczenie OT (NZ - NZ_ROZLICZENIE_OT)
98. Tabela przechowująca powiązania tytułów wykonawczych (NZ - NZ_TW_POWIAZANIA)
99. Tabela przechowuje informację o wystawionych tytułach wykonawczych (NZ - NZ_TYTULY_WYKONAWCZE)
100. Ewidencja upomnień (NZ - NZ_UPOMNIENIA)
101. Strony upomnienia (NZ - NZ_UPOMNIENIA_STRONY)
102. Dane powiązane z wirtualnym kontem (NZ - NZ_WK_DANE)
103. Wzorce dokumentów (NZ - NZ_WZORCE_DOK)
104. Ewidencja zabezpieczeń (NZ - NZ_ZABEZPIECZENIA)
105. Informacje o zmianach na dokumentach (NZ - NZ_ZM_KLRDDOK)
106. Osoby zobowiązane w hipotekach (NZ - NZ_ZOBOWIAZANI_HIP)
107. Osoby zobowiązane na tytułach wykonawczych (NZ - NZ_ZOBOWIAZANI_TW)
108. Osoby zobowiązane na zabezpieczeniach (NZ - NZ_ZOBOWIAZANI_ZAB)
109. Podmioty związane z obiektem (OPL - OPL_OBK_POD)
110. Podmioty związane z nieruchomością (OPL - OPL_PODMIOTY)
111. Centralny rejestr umów (CRU - ORG_UMOWY)
112. Powiązanie dodatkowych klientów z fakturę (FKT - RS_DOK_KL)
113. Główny rejestr faktur w systemie KSAT (FKT - RS_FAKTURY)
114. Rejestr dokumentów (FKT - RS_REJESTR_DOKUMENTOW)
115. Generowanie pozycji paczki powiadomień (RSD -SD_KORESPONDENCJA_GEN_KP)
116. Korespondencja wychodząca (RSD - RSD_KORESPONDENCJA_WYCHODZACA)
117. Decyzje – zwrot podatku akcyzowego (ZPA - ZPA_DECYZJE)
118. Pozycje list wypłat ZPA (ZPA - ZPA_POZYCJE_LISTY_WYPLAT)
119. Składniki do wypłaty- zwrot podatku akcyzowego (ZPA - ZPA_SKLADNIKI_WYPLATY)
120. Plan wypłat z ZPA (ZPA - ZPA_SKUMULOWANA_WYPLATA)
121. Wnioski— zwrot podatku akcyzowego (ZPA - ZPA_WNIOSKI)
122. Współposiadacze z wniosku (ZPA - ZPA_WSPOLPOSIADACZE)
123. Wydruki ZPA (ZPA - ZPA_WYDRUKI)
124. Wykonane wypłaty ZPA (ZPA - ZPA_WYPLATY)

III Dane klientów w zakresie zezwoleń na sprzedaż alkoholu (ALK)

1. Nazwa kontrahenta
2. Numer Identyfikacji Podatkowej kontrahenta
3. Nazwisko człón I
4. Nazwisko człón II
5. Pierwsze imię kontrahenta
6. Drugie imię kontrahenta
7. Numer identyfikacyjny PESEL kontrahenta
8. Kod pocztowy kontrahenta
9. Numer domu

10. Numer lokalu

11. Kod klienta

IV Użytkownicy systemu (ADM_USERS)

1. Nazwa użytkownika bazy danych
2. Lokalizacja użytkownika (informacja opisowa)
3. Nazwisko użytkownika
4. Imię użytkownika
5. Tytuł (informacja opisowa, np. tytuł naukowy lub inny)
6. Stanowisko służbowe
7. Miejsce zatrudnienia
8. Telefon kontaktowy
9. Lokalizacja użytkownika (adres, itp.)
10. Pokój użytkownika
11. Adres poczty elektronicznej e-mail
12. Opis/charakterystyka użytkownika

Informacja o przetwarzaniu danych osobowych reprezentantów, w tym pełnomocników oraz osób wskazanych do kontaktu i współpracy przez Wykonawcę

Działając na podstawie art. 13 i 14 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, dalej RODO, informujemy, że:

- 1) Administratorem Pani/Pana danych osobowych jest Gmina Miasta Gdyni – jednostka budżetowa Gdyńskie Centrum Informatyki, z siedzibą przy ul. Śląskiej 35-37, 81-310 Gdynia, e-mail: gci@gci.gdynia.pl tel: +48 58-527-85-00
- 2) Administrator powołał inspektora ochrony danych, z którym kontakt jest możliwy poprzez e-mail: iod@gci.gdynia.pl lub adres pocztowy: jak wyżej
- 3) Przetwarzamy dane osobowe przekazane przez Wykonawcę lub wskazane w dokumentach przekazywanych przez Wykonawcę, w szczególności dane identyfikacyjne (m.in. imię i nazwisko, stanowisko), kontaktowe (m.in. służbowy adres e-mail, służbowy numer telefonu, miejsce wykonywania pracy) oraz dane identyfikujące podmiot, w imieniu którego Pani/Pan występuje. Wobec członków organów możemy również przetwarzać numer PESEL, a w przypadku pełnomocników również inne dane widoczne w pełnomocnictwie.
- 4) Pani/Pana dane osobowe zostały nam przekazane przez podmiot, który Pani/Pan reprezentuje lub który wskazał Panią/Pana jako osobę do współpracy w związku z zawarciem/wykonywaniem zawartej z nami umowy.
- 5) Pani/Pana dane osobowe będą przetwarzane w celach:
 - a) zawarcia i realizacji, w tym rozliczenia umowy (podstawa prawna z art. 6 ust. 1 lit. b RODO),
 - b) związanych z koniecznością wypełnienia ciążącego na nas obowiązku prawnego zgodnie z obowiązującymi przepisami prawa, w szczególności udokumentowania zawartej umowy i jej rozliczenia, wynikających z przepisów podatkowych i o rachunkowości, w tym wystawiania zaświadczeń do celów podatkowych, prowadzenie ksiąg rachunkowych i dokumentacji podatkowej (podstawa prawna z art. 6 ust. 1 lit. c RODO),
 - c) wynikających z prawnie uzasadnionych interesów Administratora, jakim jest m.in. umożliwienie prowadzenia komunikacji związanej z zawarciem i realizacją umowy, ustalenie, obrona i dochodzenie roszczeń (podstawa prawna z art. 6 ust. 1 lit. f RODO)
- 6) Odbiorcami Pani/Pana danych osobowych mogą być:
 - a) podmioty publiczne, sądy i inni odbiorcy na podstawie przepisów powszechnie obowiązującego prawa;
 - b) firmy świadczące usługi z zakresu serwisu i asysty technicznej systemów informatycznych oraz programów dziedzicznych Administratora,
 - c) operator pocztowy, z którym Administrator zawarł umowę na świadczenie usług pocztowych i kurierskich,
 - d) dostawcy usług audytorskich i doradczych oraz wspierających Administratora.W przypadku ujawnienia się konieczności przekazania danych odbiorcom innym niż w zdaniu poprzedzającym, zostanie Pani/Pan odrębnie poinformowana/y.
- 7) Administrator nie przewiduje zautomatyzowanego podejmowania decyzji ani profilowania w oparciu o otrzymane dane osobowe.
- 8) Dane osobowe będą przechowywane przez okres upoważniający do ich zachowania i archiwizacji zgodnie z przepisami prawa powszechnie obowiązującego; dane osobowe są przetwarzane przez okres przygotowania umowy do jej zawarcia, jej realizacji i rozliczenia, a w przypadku wystąpienia roszczeń przez okres ustalania i dochodzenia roszczeń oraz obrony przed roszczeniami. W odniesieniu do pozostałych celów opartych na naszym uzasadnionym interesie Pani/Pana dane przetwarzane będą przez okres ważności tych celów albo do czasu, aż zgłosi Pan/Pani swój sprzeciw.
- 9) Zgodnie z RODO ma Pani/Pan prawo do:
 - a) uzyskania kopii danych osobowych, lub ich udostępnienia w siedzibie administratora;

- b) żądania sprostowania danych osobowych;
 - c) usunięcia danych lub ograniczenia ich przetwarzania, w przypadkach przewidzianych prawem,
 - d) wniesienia w dowolnym momencie sprzeciwu wobec przetwarzania Pani/Pana danych osobowych, w zakresie w jakim podstawą przetwarzania danych osobowych jest nasz prawnie usprawiedliwiony interes, w tym ze względu na Pani/Pana szczególną sytuację,
 - e) wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.
- 10) Podanie danych osobowych jest dobrowolne, ale niezbędne dla doprowadzenia do zawarcia umowy, jej zawarcia, następnie prawidłowego wykonania jej postanowień a także rozliczenia.

	Procedura bezpieczeństwa informacji Gdyńskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 1/6

§1

Cel procedury

Celem niniejszej procedury jest zapewnienie ochrony aktywów informacyjnych Gdyńskiego Centrum Informatyki udostępnianych osobom trzecim.

§2

Zakres stosowania

Procedura obowiązuje wszystkie osoby trzecie świadczące na rzecz Gdyńskiego Centrum Informatyki usługi związane z realizacją celów i zadań statutowych Gdyńskiego Centrum Informatyki.

§3

Definicje pojęć i skrótów użytych w procedurze

W niniejszej procedurze obowiązuje terminologia i definicje zawarte w Polityce Bezpieczeństwa Informacji Gdyńskiego Centrum Informatyki.

1. **Aktywa informacyjne** - wszelkie urządzenia, oprogramowanie, informacje czy elementy infrastruktury, które mają znaczenie dla Gdyńskiego Centrum Informatyki i wpływają na bezpieczeństwo informacji.
2. **Katastrofa** - zdarzenia, które uniemożliwiają świadczenie usług przez Gdyńskie Centrum Informatyki.

§4

Przyznawanie dostępu do aktywów informacyjnych Gdyńskiego Centrum Informatyki

1. Osoby trzecie realizujące określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych GCI, w tym do:
 - 1) informacji sklasyfikowanych w poszczególnych grupach:
 - a) informacji publicznych jawnych,
 - b) informacji prawnie chronionych,

	Procedura bezpieczeństwa informacji Gdyńskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 2/6

- c) informacji wewnętrznych Urzędu,
- d) danych osobowych;
- 2) aktywów wspierających przetwarzanie ww. informacji:
 - a) sprzęt (w tym komputery, nośniki informacji),
 - b) oprogramowanie,
 - c) sieć,
 - d) personel (w tym pracownicy Gdyńskiego Centrum Informatyki),
 - e) lokalizacja/siedziba (w tym pomieszczenia biurowe GCI),
 - f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych GCI),w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.
- 2. Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za realizację umowy lub porozumienia, lub osoby przez niego upoważnionej, na zasadach i w trybie określonym w podpisywanych indywidualnych umowach lub porozumieniach.
- 3. Przyznawanie rozszerzonych uprawnień nie przewidzianych w umowie możliwe jest po przedłożeniu stosownego uzasadnienia przez właściwego kierownika komórki organizacyjnej, odpowiedzialnego za realizację umowy lub porozumienia, lub osoby przez niego upoważnionej, i po formalnym odnotowaniu przedmiotowej zmiany. Przyznanie tych uprawnień musi zostać zaakceptowane przez Najwyższe kierownictwo GCI.
- 4. Dostęp zdalny osób trzecich do aktywów informacyjnych GCI, w związku z wykonywaniem prac objętych umową lub porozumieniem, przyznawany jest w zakresie niezbędnym do realizacji zadań i jest monitorowany.
- 5. Dostęp fizyczny do budynków i pomieszczeń GCI dla osób trzecich następuje na wniosek skierowany do osoby odpowiedzialnej za realizację umowy lub porozumienia, lub osoby przez niego upoważnionej.

	Procedura bezpieczeństwa informacji Gdynskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 3/6

6. W strefach bezpieczeństwa osoby trzecie mogą przebywać tylko pod nadzorem uprawnionych pracowników Gdynskiego Centrum Informatyki.

§5

Podstawowe zasady bezpieczeństwa w zakresie współpracy z podmiotami zewnętrznymi

1. W przypadku korzystania z budynków i pomieszczeń GCI osoby trzecie zobowiązane są do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.
2. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla osób trzecich z zakresu bezpieczeństwa informacji przez pracowników SSC lub/i ochrony danych osobowych przez IOD GCI.
3. Osoby trzecie zobowiązane są stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń.
4. Szczegółowe wymagania w zakresie stosowanych zabezpieczeń aktywów informacyjnych GCI oraz sposobów komunikacji stanowią część umowy lub porozumienia.
5. W ramach zapewnienia poufności przetwarzanych informacji, osoby trzecie zobowiązane są zachować w tajemnicy przez czas określony w umowie lub porozumieniu, informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnieniem osobom nieuprawnionym.
6. Wymóg zachowania poufności, o którym mowa w ust. 5 obejmuje wszelkie informacje chronione, których ujawnienie mogłoby narazić Gdynskie Centrum Informatyki na szkodę.

§6

Treść umów i porozumień z podmiotami zewnętrznymi

1. W celu ograniczenia ryzyka związanego z dostępem osób trzecich do aktywów GCI, w treści zawieranych umów lub porozumień wprowadza się niezbędne

	Procedura bezpieczeństwa informacji Gdynskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 4/6

wymogi dot. bezpieczeństwa aktywów informacyjnych i/lub utrzymania ciągłości świadczonych usług, do których przestrzegania w trakcie i po zakończeniu umowy lub porozumienia zobowiązana jest osoba trzecia.

2. Podstawowy zakres wymogów, o których mowa w ust. 1 wynika wprost z obowiązujących przepisów prawa oraz dokumentacji bezpieczeństwa, w szczególności Polityki bezpieczeństwa informacji Gdynskiego Centrum Informatyki.
3. Właściwy kierownik komórki organizacyjnej odpowiedzialnej za realizację umowy lub porozumienia, w konsultacji z Samodzielnym Stanowiskiem ds. Bezpieczeństwa Informacji i Cyberbezpieczeństwa przygotowuje projektowane postanowienia umowne dotyczące bezpieczeństwa informacji.
4. Zakres oraz stopień szczegółowości zapisów dotyczących bezpieczeństwa informacji w treści umowy lub porozumienia zależy od przedmiotu i specyfiki podejmowanej współpracy oraz zidentyfikowanych zagrożeń.
5. Poza standardowymi wymogami, wprost określonymi w obowiązujących przepisach prawa oraz dokumentacji bezpieczeństwa, dodatkowe zapisy dotyczące bezpieczeństwa informacji mogą uwzględniać np.:
 - 1) cel i zakres przetwarzanych informacji,
 - 2) wykaz osób upoważnionych do wymiany informacji i listę zatwierdzonych narzędzi do komunikacji,
 - 3) zakres i poziom świadczonych usług,
 - 4) zasady i tryb postępowania w przypadku awarii lub katastrofy (maksymalny czas reakcji, maksymalny czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,
 - 5) akceptowalny poziom dostępności świadczonych usług (umowy SLA),
 - 6) ochronę własności intelektualnej i praw autorskich.
6. W przypadku korzystania przez osobę trzecią z usług podwykonawców wymogi bezpieczeństwa informacji dotyczą również podwykonawców.
7. W przypadku powierzenia osobom trzecim przetwarzania danych osobowych, kierownik właściwej komórki organizacyjnej GCI przygotowuje stosowne zapisy

	Procedura bezpieczeństwa informacji Gdyńskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 5/6

dotyczące ochrony danych osobowych (umowa powierzenia), zgodnie z art. 28 RODO..

8. Każda umowa wiążąca się z dostępem do pomieszczeń i zasobów informacyjnych Gdyńskiego Centrum Informatyki, musi zawierać zobowiązanie następującej treści:

Wykonawca zobowiązuje się do zapoznania i przestrzegania zasad bezpieczeństwa informacji określonych w Procedurze bezpieczeństwa informacji Gdyńskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi, opartej o Politykę Bezpieczeństwa Informacji w Gdyńskim Centrum Informatyki.

Wykonawca zobowiązuje się do zapoznania z aktualną instrukcją przeciwpożarową i aktualnymi przepisami BHP obowiązującymi w budynkach, do których wykonawca będzie miał dostęp.

§7

Monitorowanie i przegląd usług świadczonych przez osoby trzecie

1. Dostęp i korzystanie z aktywów informacyjnych GCI przez osoby trzecie są nadzorowane i monitorowane.
2. Bieżący nadzór nad udostępnianiem i korzystaniem przez osoby trzecie z aktywów informacyjnych GCI prowadzi właściwy kierownik komórki organizacyjnej lub osoba/osoby przez niego wyznaczone.

§8

Zgłaszanie przypadków naruszenia bezpieczeństwa informacji

1. Osoby trzecie wykonujące czynności w imieniu i na rzecz GCI i/lub mające dostęp do aktywów informacyjnych GCI, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w GCI, zobowiązane są niezwłocznie poinformować o szczegółach i charakterze zdarzenia Samodzielne Stanowisko ds. Bezpieczeństwa Informacji i Cyberbezpieczeństwa.

	Procedura bezpieczeństwa informacji Gdynskiego Centrum Informatyki w relacjach z podmiotami zewnętrznymi		
	Obowiązuje od:	Wersja: I	Strona: 6/6

2. Zgłoszenie, o którym mowa w ust. 1, należy przestać drogą mailową na adres incydenty@gci.gdynia.pl, podając dane kontaktowe, okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia.
3. Osobom trzecim świadczących usługi na rzecz GCI zabrania się podejmowania prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych.
4. Próby/przypadki nieautoryzowanego dostępu do aktywów informacyjnych GCI są identyfikowane jako incydenty związane z bezpieczeństwem informacji.
5. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązującej dokumentacji bezpieczeństwa przez osoby trzecie stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.
6. Z tytułu działań osób trzecich i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dotyczących niewłaściwego przetwarzania danych osobowych), grożą odrębne kary określone w odpowiednich przepisach prawa.

Podpis jest prawidłowy

Dokument podpisany przez
MARTA BARBARA
KITTEL
Data: 2022.11.23 11:01:42
CET

Samodzielne Stanowisko
ds. bezpieczeństwa informacji
i cyberbezpieczeństwa
dr Małgorzata Groch-Bobrowska

**PROCEDURA BEZPIECZEŃSTWA INFORMACJI
W URZĘDZIE MIASTA GDYNI W RELACJACH
Z PODMIOTAMI ZEWNĘTRZNYMI**

¹ Dodany przez § 1 pkt 6 zarządzenia nr 5763/22/VIII/S z dnia 22.11.2022 r.

PRYZNAWANIE DOSTĘPU DO AKTYWÓW INFORMACYJNYCH URZĘDU.

§ 1.1. Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych Urzędu, w tym do:

- 1) informacji sklasyfikowanych w poszczególnych grupach:
 - a) informacji publicznych jawnych,
 - b) informacji prawnie chronionych,
 - c) informacji wewnętrznych Urzędu,
 - d) danych osobowych;
- 2) aktywów wspierających przetwarzanie ww. informacji:
 - a) sprzętu (w tym komputerów, nośników informacji),
 - b) oprogramowania,
 - c) sieci,
 - d) personelu (w tym pracownicy Urzędu),
 - e) lokalizacji/siedziby (w tym pomieszczeń biurowych Urzędu),
 - f) organizacji (w tym procedur wewnętrznych określających zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Urzędu),

w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

2. Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie i/lub realizację umowy lub porozumienia, na zasadach i w trybie określonym w podpisywanych indywidualnych umowach.

3. Przyznawanie rozszerzonych uprawnień możliwe jest po przedłożeniu stosownego uzasadnienia przez kierownika, o którym mowa w ust. 2 i po formalnym odnotowaniu przedmiotowej zmiany.

4. Dostęp zdalny podmiotów zewnętrznych do aktywów informacyjnych Urzędu, w związku z wykonywaniem prac serwisowych i aktualizacji oprogramowania, przyznawany jest w zakresie niezbędnym do realizacji zadań i jest monitorowany.

5. Dostęp fizyczny do budynków i pomieszczeń Urzędu dla pracowników podmiotów zewnętrznych następuje na wniosek skierowany do kierownika, o którym mowa w ust. 2.

6. W strefach bezpieczeństwa pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem uprawnionych pracowników Urzędu lub miejskich jednostek organizacyjnych. Dostęp do stref bezpieczeństwa jest ewidencjonowany.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA W ZAKRESIE WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI

§ 2.1. W przypadku korzystania z budynków i pomieszczeń administrowanych przez Urząd, pracownicy podmiotów zewnętrznych zobowiązani są do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.

2. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla pracowników podmiotów zewnętrznych z zakresu bezpieczeństwa informacji lub/i ochrony danych osobowych.

3. Pracownicy podmiotów zewnętrznych zobowiązani są stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń.

4. Szczegółowe wymagania w zakresie stosowanych zabezpieczeń aktywów informacyjnych Urzędu oraz sposobów komunikacji stanowią część umowy lub porozumienia.

5. W ramach zapewnienia poufności przetwarzanych informacji, pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas określony w umowie lub porozumieniu, informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnieniem osobom nieuprawnionym.

6. Wymóg zachowania poufności, o którym mowa w ust. 5 obejmuje wszelkie informacje prawnie chronione.

TREŚĆ UMÓW I POROZUMIEŃ Z PODMIOTAMI ZEWNĘTRZNYMI

§ 3.1. Kierownik, o którym mowa w § 1 ust. 2, przygotowuje i zamieszcza w umowie lub porozumieniu adekwatne zapisy dotyczące bezpieczeństwa informacji.

2. W treści zawieranych umów lub porozumień wprowadza się niezbędne wymagania dotyczące bezpieczeństwa aktywów informacyjnych i/lub utrzymania ciągłości świadczonych usług, do których przestrzegania w trakcie i po zakończeniu umowy lub porozumienia zobowiązany jest podmiot zewnętrzny.

3. Podstawowy zakres wymogów, o których mowa w ust. 2 wynika wprost z obowiązujących przepisów prawa oraz dokumentacji bezpieczeństwa, w szczególności Polityki Bezpieczeństwa Informacji w Urzędzie Miasta Gdyni.

4. Zakres oraz stopień szczegółowości zapisów dotyczących bezpieczeństwa informacji w treści umowy lub porozumienia zależy od przedmiotu i specyfiki podejmowanej współpracy oraz zidentyfikowanych zagrożeń.

5. Poza standardowymi wymogami, wprost określonymi w obowiązujących przepisach prawa oraz dokumentacji bezpieczeństwa, dodatkowe zapisy dotyczące bezpieczeństwa informacji mogą uwzględniać np.:

- 1) cel i zakres przetwarzanych informacji,
- 2) wykaz osób upoważnionych do wymiany informacji i listę zatwierdzonych narzędzi do komunikacji,

- 3) zakres i poziom świadczonych usług,
 - 4) zasady i tryb postępowania w przypadku awarii lub katastrofy (maksymalny czas reakcji, maksymalny czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,
 - 5) akceptowalny poziom dostępności świadczonych usług (umowy SLA),
 - 6) ochronę własności intelektualnej i praw autorskich.
6. W przypadku korzystania przez dostawcę z usług podwykonawców wymogi bezpieczeństwa informacji dotyczą również podwykonawców.
7. W przypadku powierzenia podmiotom zewnętrznym przetwarzania danych osobowych, kierownik, o którym mowa w § 1 ust. 2, przygotowuje stosowne zapisy dotyczące ochrony danych osobowych (umowa powierzenia), zgodnie z art. 28 RODO.
9. Każda umowa wiążąca się z dostępem do pomieszczeń i zasobów informacyjnych Urzędu, musi zawierać zobowiązanie następującej treści:
- Wykonawca zobowiązuje się do zapoznania i przestrzegania zasad bezpieczeństwa informacji określonych w Procedurze Bezpieczeństwa Informacji w Urzędzie Miasta Gdyni w relacjach z podmiotami zewnętrznymi, opartej o Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Gdyni.*

MONITOROWANIE I PRZEGLĄD USŁUG ŚWIADCZONYCH PRZEZ PODMIOTY ZEWNĘTRZNE

- § 4. 1. Dostęp podmiotów zewnętrznych i korzystanie z aktywów informacyjnych Urzędu przez ich pracowników są nadzorowane i monitorowane.
2. Bieżący nadzór nad udostępnianiem i korzystaniem przez podmioty zewnętrzne z aktywów informacyjnych Urzędu prowadzi kierownik, o którym mowa w § 1 ust. 2 lub osoba/osoby przez niego wyznaczone.

ZGŁASZANIE PRZYPADKÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI PRZEZ PODMIOTY ZEWNĘTRZNE

- § 5. 1. Osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UM i/lub mające dostęp do aktywów informacyjnych Urzędu, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w UM, zobowiązane są niezwłocznie poinformować o szczegółach i charakterze zdarzenia Pełnomocnika Prezydenta ds. Bezpieczeństwa Informacji.
2. Zgłoszenie, o którym mowa w ust. 1, należy przesłać pocztą elektroniczną na adres incydenty@gdynia.pl, podając dane kontaktowe, okoliczności oraz czas wystąpienia zdarzenia wskazującego na naruszenie lub próbę naruszenia.
3. Próby/przypadki nieautoryzowanego dostępu do aktywów informacyjnych Urzędu są identyfikowane jako incydenty związane z bezpieczeństwem informacji.
4. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązującej dokumentacji bezpieczeństwa przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.

O BOWIĄZKI W ZAKRESIE DYSTRYBUCJI

§ 6

Niniejszy dokument udostępnia się podmiotom zewnętrznym, realizującym usługi na rzecz Urzędu Miasta Gdyni.

ZLECENIE OPCJI NR

do Umowy..... z dnia

1. Zamawiający zleca Wykonawcy realizację zamówienia opcjonalnego tj. usługę roboczogodzin w liczbie godzin w zakresie i na warunkach określonych w Umowie, SWZ oraz w Ofercie Wykonawcy stanowiącej Załącznik nr do Umowy w terminie do dnia 31 grudnia 2025 r.
2. Wartość wynagrodzenia brutto z tytułu realizacji Prawa opcji wyniesie zł (słownie: złotych), w tym podatek VAT.
3. Pozostałe warunki realizacji zamówienia opcjonalnego określa Umowa.

.....

Zamawiający