Zakres **Usługi Pełnienia Obowiązków Inspektora Ochrony Danych** obejmuje konsultacje i wsparcie merytoryczne oraz przejęcie obowiązków **Inspektora Ochrony Danych** w jednostce organizacyjnej **ZAMAWIAJĄCEGO** w zakresie wynikającym z **Rozporządzenia UE** oraz **Ustawy**, dotyczących zasad przetwarzania danych osobowych oraz ich zabezpieczenia, na które składają się:

1. Realizacja obowiązków **Inspektora Ochrony Danych** w zakresie wynikającym z **Rozporządzenia UE** oraz **Ustawy**;
2. Dostosowanie **Dokumentacji** do wymagań **Rozporządzenia UE** (przez okres pierwszych 6 miesięcy) z uwzględnieniem:
   a/ Opracowania lub aktualizacji **Dokumentacji**;
   b/ Przeprowadzenia analizy zagrożeń i oceny ryzyka;
   c/ Przeprowadzenia oceny skutków przetwarzania, w przypadku występowania takiej konieczności; Wymaga opublikowania przez organ nadzorczy wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.
3. Nadzór nad **Systemem**, z uwzględnieniem bieżącej aktualizacji **Dokumentacji** w odniesieniu do:
   a/ Zmian prawnych;
   b/ Zmian organizacyjnych;
4. Konsultacje merytoryczne telefoniczne i za pośrednictwem poczty elektronicznej, przy czym:
   a/ Czas reakcji na zgłoszony problem/pytanie merytoryczne z zakresu **Systemu** i/lub **Rozporządzenia UE** oraz **Ustawy** nie przekroczy w ramach **Dnia Roboczego**:
      1. 8 godzin w przypadku konsultacji mailowych,
      2. 4 godzin w przypadku konsultacji telefonicznych;
   b/ Problemy/pytania powinny być zgłoszone:
      1. pocztą elektroniczną na adres internetowy wyznaczonego **Inspektora Ochrony Danych** lub jego zastępcy;
      2. telefonicznie na numer telefonu komórkowego wyznaczonego **Inspektora Ochrony Danych** lub jego zastępcy;
   c/ Dane kontaktowe wyznaczonego **Inspektora Ochrony Danych** zostały umieszczone w dokumencie *Koordynatorzy (Załącznik nr 4)*;
   d/ **WYKONAWCA** w trybie roboczym, przekaże **ZAMAWIAJĄCEMU** dodatkowe numery telefonów, faksu oraz adres poczty elektronicznej dedykowane dla celów kontaktu.
   e/ Konsultacje prowadzone będą w ramach **Dnia Roboczego**, zgodnie z jego definicją;
   f/ **ZAMAWIAJĄCY** w trybie roboczym może przekazać **WYKONAWCY** stałą listę osób (nie więcej niż 20 osób), będących pracownikami **ZAMAWIAJĄCEGO**, uprawnionych do przedstawiania i dyskutowania pojawiających się problemów w zakresie **Systemu** i/lub **Rozporządzenia UE** oraz **Ustawy**. Osoby uprawnione powinny posiadać odpowiednie przygotowanie merytoryczne do podjęcia rzeczowej dyskusji o przedstawionym problemie. Zamawiający przekaże również zestawienie telefonów kontaktowych do tych osób i adresy poczty elektronicznej, na który będą przez **WYKONAWCĘ** przekazywane odpowiedzi.
   g/ Ewentualne porady udzielane będą przez **WYKONAWCĘ** na bieżąco, w trakcie rozmowy telefonicznej lub w postaci pisemnej informacji, o ile wymaga tego treść udzielanej porady;
5. Prace, dyżury i konsultacje merytoryczne w siedzibie **ZAMAWIAJĄCEGO (Urząd** lub inna lokalizacja), przy czym:
   a/ Maksymalna liczba wizyt nie przekroczy 12 całodniowych wizyt rocznie oraz 2 wizyt miesięcznie (zbiorczo dla wszystkich Jednostek Organizacyjnych);
   b/ Czas trwania pojedynczej wizyty nie przekroczy 8 godzin;
   c/ Termin wizyt zostanie ustalony przez **Strony** z co najmniej tygodniowym wyprzedzeniem;
   d/ W ramach wizyty możliwe jest przeprowadzenie dla pracowników **ZAMAWIAJĄCEGO** szkoleń z zakresu **Rozporządzenia UE** oraz **Ustawy** i/lub **Systemu**, przy czym szczegółowy zakres i termin przeprowadzenia szkoleń ustalany będzie z wyprzedzeniem co najmniej 10 dni roboczych;

6. Wizyty kontrolne w **Jednostkach Organizacyjnych**, przy czym:
   a/ Maksymalna liczba wizyt nie przekroczy 12 całodniowych wizyt rocznie oraz 1 wizyty miesięcznie (zbiorczo dla wszystkich Jednostek Organizacyjnych);
   b/ Czas trwania pojedynczej wizyty nie przekroczy 8 godzin;
   c/ Termin wizyt zostanie ustalony przez **Strony** z co najmniej tygodniowym wyprzedzeniem;
7. Dodatkowe wizyty:
   a/ W przypadku zajścia potrzeby przeprowadzenia dodatkowych wizyt wykraczających poza określoną powyżej maksymalną liczbę wizyt lub wizyt w lokalizacjach nie uwzględnionych w dokumencie *Lista Miejsc Świadczenia Usługi (Załącznik nr 3)*, **ZAMAWIAJĄCY**:
      1. pokryje koszty przejazdu oraz zakwaterowania według uzgodnionych przed wizytą stawek rzeczywistych;
      2. pokryje koszty dodatkowych wizyt według stawki określonej w § 6.2.
8. Przeprowadzenie audytu weryfikującego w ramach wizyt kontrolnych:
   a/ Zakres audytu obejmie:
      1. Zgodność istniejących zabezpieczeń **Systemu** w zakresie **Rozporządzenia UE**;
      2. Realizacji i spełnienia wymagań **Rozporządzenia UE**.
   b/ Audyt zostanie przeprowadzony po 10 miesiącach obowiązywania **Umowy**;
   c/ Audyt zostanie zakończony raportem poaudytowym w postaci listy pokontrolnej;
   d/ **WYKONAWCA** przekaże Certyfikat Bezpieczeństwa Informacji dla **Systemu**.
9. Przechowywanie, dekretacja i archiwizacja nośników elektronicznych oraz dokumentów papierowych generowanych, przetwarzanych i nadzorowanych w ramach obowiązków **Inspektora Ochrony Danych** będą realizowane w odpowiednio przygotowanym do tego celu pomieszczeniu biurowym wyposażonym w sejf lub zamykaną na klucz szafę w siedzibach **Jednostek Organizacyjnych** przez:
   a/ **Koordynatorów** ze strony **Jednostek Organizacyjnych**;
10. Szczegółowy zakres zadań i obowiązków **Inspektora Ochrony Danych** oraz zakres konsultacji i wsparcia merytorycznego w ramach poszczególnych zadań został przedstawiony w poniższej tabeli:

Legenda:
ADO – Administrator Danych Osobowych
IOD – Inspektor Ochrony Danych (G – Główny, Z – Zastępca)
ASI – Administrator Systemów Informatycznych
KZ – Koordynator Zamawiającego
KW – Koordynator Wykonawcy
RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych wraz z przepisami wykonawczymi
x – realizacja (odpowiedzialność)
w – wsparcie/pomoc
o – opiniowanie

ZADANIA I OBOWIĄZKI IOD	IOD G	IOD Z KW	ASI
Główne zadania i obowiązki			
Przygotowanie planu sprawdzeń (audytu) na określony przez niego okres, nie krótszy niż kwartał i nie dłuższy niż rok, w tym na wniosek organu nadzorczego.	x	w	w
Realizacja sprawdzeń (kontroli) pozaplanowych niezwłocznie po powzięciu informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, w tym na wniosek organu nadzorczego.	x	w	w
Realizacja sprawdzeń (audytów) planowych, w tym na wniosek organu nadzorczego.	x	w	w
Określanie zakresu czynności, które będą podejmowane w toku sprawdzenia oraz sposobu i zakresu dokumentowania czynności podejmowanych w toku sprawdzenia.	x	w	w

ZADANIA I OBOWIĄZKI IOD	IOD G	IOD Z KW	ASI
Sporządzanie programu sprawdzenia przed każdym sprawdzeniem, który określa zakres czynności oraz sposób i zakres ich dokumentowania.	x	w	w
Opracowywanie sprawozdań ze sprawdzeń (audytów).	x	w	w
Nadzorowanie opracowania i aktualizowania dokumentacji systemu ochrony danych osobowych (polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemami informatycznymi), oraz wszelkich późniejszych polityk ochrony danych.	x	w	w
Weryfikacja zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa.	x	w	–
Weryfikacja skuteczności przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych zabezpieczenia rozwiązań dla przeciwdziałania zagrożeniom dla ochrony danych osobowych.	x	w	w
Weryfikacja przestrzegania obowiązków określonych w dokumentacji przetwarzania danych.	x	w	w
W przypadku wykrycia podczas weryfikacji nieprawidłowości, zawiadomienie administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności przedstawianie mu do wdrożenia dokumentów usuwających stan niezgodności.	x	w	w
W przypadku wykrycia podczas weryfikacji nieprawidłowości, zawiadomienie administratora danych o nieaktualności dokumentacji przetwarzania danych oraz przedstawianie administratorowi danych do wdrożenia dokumentów aktualizujących.	x	w	w
W przypadku wykrycia podczas weryfikacji nieprawidłowości, pouczenie lub poinstruowanie osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, z jednoczesnym wskazaniem osoby odpowiedzialnej za naruszenie tych zasad oraz jego zakres.	x	w	w
Informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO UE oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.	x	w	w
Monitorowanie przestrzegania RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.	x	w	w
Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.	x	w	-
Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, dot. oceny skutków, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.	x	w	-
Pozostałe zadania i obowiązki (wsparcie ADO i ASI)			
Opracowanie wymaganej ustawowo dokumentacji systemu ochrony danych osobowych (polityki bezpieczeństwa informacji i instrukcji zarządzania systemami informatycznymi) oraz odpowiednich polityk ochrony danych – jeżeli okaże się to proporcjonalne do występujących po stronie Administratora Danych procesów przetwarzania danych.	x	w	w
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych.	x	w	w
Aktualizacja dokumentacji systemu ochrony danych osobowych (polityki bezpieczeństwa informacji i instrukcji zarządzania systemami informatycznymi) oraz innych ustanowionych polityk ochrony danych.	x	w	w
Kontrola legalności przetwarzania zbiorów danych – okresowe przeglądy i ocena.	x	w	w

ZADANIA I OBOWIĄZKI IOD	IOD G	IOD Z KW	ASI
Prowadzenie Rejestru Czynności Przetwarzania.	x	w	w
Zarządzanie upoważnieniami i klauzulami poufności – gromadzenie pisemnych oświadczeń/klauzul poufności od pracowników i podwykonawców, nadawanie imiennych upoważnień do przetwarzania zbiorów.	x	w	w
Weryfikacja zakresów obowiązków służbowych pracowników, na stanowiskach związanych z przetwarzaniem danych osobowych.	x	w	w
Nadzór i aktualizacja ewidencji osób upoważnionych do przetwarzania danych w zbiorach.	x	w	w
Organizacja formalnych zasad współpracy z podmiotami zewnętrznymi – tworzenie umów powierzenia/poufności, wsparcie podczas negocjacji i podpisania ich przez podmioty posiadające dostęp do danych osobowych.	x	w	w
Reprezentowanie organizacji w kontaktach z organem nadzorczym – prowadzenie kontaktów i korespondencji z organem nadzorczym, zarówno w trybie administracyjnym, jak i podczas kontroli.	x	w	w
Doradztwo w rozprawach i postępowaniach administracyjnych i sądowych dotyczących sporów w zakresie Ochrony Danych Osobowych.	x	w	w
Opiniowanie dokumentów organizacji pod kątem zgodności z wymaganiami RODO – opiniowanie i dostosowanie dokumentacji organizacji do wymagań RODO (np. klauzule zgody, poufności, informacyjne).	x	w	w
Bieżące formułowanie wniosków do Administratora Danych Osobowych (ADO), dotyczących poprawy bezpieczeństwa danych osobowych.	x	w	w
Współpraca z ASI w zakresie wdrażania wymaganych zabezpieczeń informatycznych – wyznaczanie wymaganych ustawowo zabezpieczeń; w przypadku braku, nadzór nad ich wdrożeniem.	x	w	–
Kontrola zgodności oprogramowania – pomoc w dostosowaniu, doborze lub zmianie oprogramowania do przetwarzania danych osobowych, aby spełniało wymagania przepisów wykonawczych do RODO.	x	w	w
Nadzór nad procesem nadawania upoważnień pracownikom przetwarzającym dane osobowe	x	w	w
Nadzór nad przestrzeganiem w bieżącej działalności wymagań dotyczących zasady legalności, celowości, merytorycznej poprawności, adekwatności i czasowości przetwarzania danych osobowych.	x	w	w
Współpraca z kierownikiem komórki organizacyjnej odpowiedzialnej za informatykę w zakresie implementowania zabezpieczeń technicznych i funkcjonalnych.	x	w	w
Nadzorowanie nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych przez użytkowników.	x	w	w
Nadzór nad realizacją wymaganych procedur wynikających z Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych (IZSI).	w	w	x
Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń informatycznych, wspólnie z administratorami systemów informatycznych oraz kierownikiem komórki organizacyjnej odpowiedzialnej za informatykę.	x	w	x
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu, o jakim mowa w art. 33 RODO.	x	w	x
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO.	x	w	x
Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które prowadzą do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.	x	w	w
Monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.	x	w	w

ZADANIA I OBOWIĄZKI IOD	IOD G	IOD Z KW	ASI
Prowadzenie procesu oceny ryzyka oraz oceny skutków i uprzednich konsultacji (kiedy okaże się to konieczne) w kontekście bezpieczeństwa przetwarzanych danych zgodnie z art. 24 i 32 RODO.	x	w	w
Monitorowanie działań Zarządzających Zbiorami Danych Osobowych (Kierowników Komórek Organizacyjnych) w zakresie realizowanych obowiązków dotyczących ochrony danych osobowych w podległych im komórkach, w szczególności w zakresie wnioskowania o nadanie, zmianę i wycofanie uprawnień i upoważnień ich pracowników do przetwarzania danych osobowych.	x	w	w
Organizacja i nadzór nad realizacją obowiązku informacyjnego wynikającego z art. 13 i 14 RODO we współpracy z Zarządzającymi Zbiorami Danych Osobowych.	x	w	w
Organizacja realizacji praw osób, których dane dotyczą oraz obsługa zgłoszeń dotyczących prawa: dostępu do danych, do sprostowania danych, do bycia zapomnianym, do ograniczenia przetwarzania, do przenoszenia danych, do sprzeciwu, do niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu oraz profilowaniu.	x	w	w
Nadzór Administratora Systemów Informatycznych (ASI) nad ewidencjonowaniem i aktualizowaniem zagrożeń i podatności, prowadzeniem analizy tych zagrożeń i podatności oraz dokonywaniem oceny ryzyk występujących w procesie przetwarzania danych osobowych.	w	w	x
Wnioskowanie we współpracy z właściwymi kierownikami komórek organizacyjnych do Administratora Danych o podejmowanie działań zmierzających do ograniczania ryzyk występujących w procesie przetwarzania danych osobowych poprzez stosowanie odpowiednich zabezpieczeń.	x	w	w
Pomoc w sytuacjach wystąpienia incydentów bezpieczeństwa i sporach – wsparcie w opanowaniu kryzysów (np. kradzież, wyciek, upublicznienie danych, skargi), wsparcie prawidłowej komunikacji w kontaktach z policją, organem nadzorczym, prasą, poszkodowanymi i innymi instytucjami zainteresowanymi.	x	w	w
Nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe we współpracy z osobą/osobami odpowiedzialnymi za ochronę fizyczną i techniczną obiektów.	x	w	w
Współpraca z kierownikiem komórki organizacyjnej odpowiedzialnej za archiwizowanie materiałów zawierających dane osobowe, w zakresie sposobu ich kwalifikowania, przekazywania do archiwum zakładowego oraz ich ewentualnego dalszego wykorzystywania po procesie archiwizacji przez osoby uprawnione.	x	w	w
Opracowanie programu szkolenia z zakresu ochrony danych osobowych i zapewnienie jego realizacji przez kierowników komórek organizacyjnych.	x	w	w
Organizacja szkoleń z zasad przestrzegania ochrony danych osobowych.	x	w	w
Opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych.	x	w	w
Opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych.	x	w	w
Wykonywanie kontroli i audytów względem podmiotów przetwarzających w związku z dokonaniem powierzenia danych do przetwarzania.	x	w	w
Prowadzenie centralnego rejestru zbiorów danych osobowych.	x	w	w
Udzielanie organowi nadzorczemu lub innym organom odpowiedzi i wyjaśnień w sprawie zbiorów przetwarzanych danych osobowych.	x	w	w
Udział w kontrolach prowadzonych przez inspektorów organu nadzorczego oraz wyznaczanie Zarządzających Zbiorami Danych Osobowych do uczestniczenia w takim postępowaniu kontrolnym.	x	w	x
Przeprowadzanie kontroli przestrzegania wymagań przepisów prawa przez podmioty, którym Administrator Danych Osobowych powierzył do przetwarzania dane osobowe (tzw. procesorzy).	x	w	w

Przedmiot Umowy będzie realizowany w każdej z **Jednostek Organizacyjnych ZAMAWIAJĄCEGO** wyszczególnionych na poniższej liście.

IDENT. JEDNOSTKI	NAZWA JEDNOSTKI	ADRES	OSOBA KONTAKTOWA / UWAGI
01	Urząd Gminy Gawłuszowice	PL-39-307 Gawłuszowice 5a	Sławomir Kobyra: Inspektor tel.: +48 17 7744282 w.33, tel. kom.: +48 602 899681, e-mail: kobyra@gawluszowice.pl
02	Gminny Ośrodek Pomocy Społecznej w Gawłuszowicach	PL-39-307 Gawłuszowice 6	Małgorzata Staszko: Kierownik tel.: +48 17 250 6430 e-mail: gopsgawluszowice@gawluszowice.pl
03	Gminna Biblioteka Publiczna w Gawłuszowicach	PL-39-307 Gawłuszowice 6	Ewelina Sałek Dyrektor tel. +48 17 7744076, tel.kom. +48 600 324196 e-mail: biblioteka@gawluszowice.pl
04	Szkoła Podstawowa w Gawłuszowicach	PL-39-307 Gawłuszowice 5b	Grzegorz Nelec Dyktor tel.: +48 17 7744284, +48 17 7744285, tel. kom.: +48 660 000 655 e-mail: zsggaw@op.pl