UMOWA NR UPPDO/WOK/…./2023 POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu _____ 2023 r. we Wrocławiu pomiędzy:
zwaną dalej **„Powierzającym”** którą

reprezentuje:

Gmina Wrocław- Urząd Miejski Wrocławia z siedzibą we Wrocławiu, pl. Nowy Targ 1-8, 50-141 Wrocław, REGON: 931934839

reprezentowaną przez:

Włodzimierz Patalas – Sekretarz Miasta Wrocławia działający na podstawie pełnomocnictwa nr 1/I/18 Prezydenta Wrocławia z dnia 20.11.2018,

a

……. zwaną/-ym dalej **„Przetwarzającym”** którą/-ego reprezentuje[1]:

1. …….

zwani/-e dalej łącznie „**Stronami**”, a każda z osobna „**Stroną**”,

o następującej treści:

§ 1. DEFINICJE

Użyte w niniejszej umowie określenia oznaczają:

1) **administrator** – administrator, w rozumieniu art. 4 pkt 7 RODO;
2) **dane osobowe** – dane osobowe, w rozumieniu art. 4 pkt 1 RODO;
3) **Dane Osobowe** – dane osobowe powierzone do przetwarzania w ramach Umowy;
4) **inspektor ochrony danych** – inspektor ochrony danych, w rozumieniu art. 37-39 RODO;
5) **podmiot przetwarzający** – podmiot przetwarzający, w rozumieniu art. 4 pkt 8 RODO;
6) **przetwarzanie** – przetwarzanie, w rozumieniu art. 4 pkt 2 RODO;
7) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 oraz z 2018 r. Nr 127, str. 2);
8) **Umowa** – niniejsza umowa;
9) **umowa źródłowa** – umowa lub inny dokument, z którego wynika świadczenie przez Przetwarzającego na rzecz Powierzającego usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. g RODO, tj.[2]: **nr WOK/U/……/2023**;
10) **ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781 z późn. zm.).

[1] nie dotyczy osób fizycznych / osób fizycznych prowadzących działalność gospodarczą;
[2] należy wskazać nazwę i datę dokumentu, w którym Przetwarzający zobowiązał się wobec Powierzającego do świadczenia usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. g RODO;

§ 2. WSTĘPNA WERYFIKACJA PRZETWARZAJĄCEGO
(ART. 28 UST. 1 RODO)

Przed powierzeniem przetwarzania Danych Osobowych Przetwarzającemu, Powierzający dokonał wstępnej weryfikacji Przetwarzającego w oparciu o listę kontrolną – kryteria wyboru podmiotu przetwarzającego, któremu Powierzający zamierza powierzyć dane osobowe. Podpisana przez Przetwarzającego lista kontrolna, o której mowa w zdaniu poprzednim, stanowi załącznik nr 2 do Umowy.

§ 3. CEL, CHARAKTER I PRZEDMIOT PRZETWARZANIA DANYCH OSOBOWYCH
(ART. 28 UST. 3 RODO)

1. Powierzający pełni rolę administratora Danych Osobowych / podmiotu przetwarzającego Dane Osobowe / administratora Danych Osobowych i podmiotu przetwarzającego Dane Osobowe [3].
2. Przetwarzający pełni rolę podmiotu przetwarzającego Dane Osobowe.
3. Dane Osobowe przetwarzane będą przez Przetwarzającego w celu realizacji umowy źródłowej.
4. Dane będą przetwarzane w formie papierowej / w sposób zautomatyzowany, w systemach informatycznych [7].
5. W okresie obowiązywania umowy źródłowej Dane przetworzone zostaną jednorazowo / kilkurazowo / dane przetwarzane będą stale (nie-jednorazowo, powtarzalnie) [4].
6. Zakres powierzonych do przetwarzania Przetwarzającemu Danych Osobowych wskazany został w załączniku nr 1 do Umowy, który zawiera w szczególności:
   1) datę sporządzenia załącznika, a w razie konieczności również inne oznaczenie (np. wersję załącznika), tak by w przypadku zmiany załącznika możliwym było jednoznaczne ustalenie jaki zakres Danych Osobowych mógł być przetwarzany w danym okresie przez Przetwarzającego,
   2) informację o nazwie i danych kontaktowych administratora Danych Osobowych [5],
   3) zakres powierzonych Przetwarzającemu Danych Osobowych (w szczególności ich rodzaj) [6],
   4) kategorie osób, których Dane Osobowe dotyczą[7],
   5) rodzaj operacji dokonywanych na Danych Osobowych[8],

[3] niepotrzebne skreślić; w przypadku, gdy Powierzający pełni rolę zarówno administratora Danych Osobowych jak i podmiotu przetwarzającego Dane Osobowe, wskazanie jaką funkcję pełni Powierzający i w stosunku do których Danych Osobowych wynika z treści załącznika nr 1 do Umowy; [7] niepotrzebne skreślić;

[4] niepotrzebne skreślić; jednorazowo (np. zostanie sporządzona lista obecności uczestników szkolenia), kilkurazowo (np. zostanie sporządzony kilka list obecności uczestników z kilku szkoleń odbywających się według ustalonego harmonogramu), stale (np. w przypadku umowy na serwis systemu komputerowego, gdzie podmiot przetwarzający ma dostęp do systemu i poprawia na bieżąco zgłaszane mu przez użytkowników błędy);

[5] w przypadku w którym jako administrator nie został wskazany Powierzający oznacza to, że Powierzający jest podmiotem przetwarzającym dla tych danych, a Przetwarzający dalszym podmiotem przetwarzającym;

[6] rodzaj danych: dane zwykłe lub dane wrażliwe (w rozumieniu motywu 10 preambuły RODO); należy wskazać jakie dane zwykłe (np. imię, nazwisko, adres zamieszkania, NIP, PESEL) oraz jakie dane wrażliwe (np. dane o zdrowiu, o orientacji seksualnej);

[7] należy wskazać czyje dane są zbierane (np. klienci, wykonawcy, pacjenci, studenci, personel, osoby poszukujące pracy);

[8] operacje wykonywane na danych osobowych przez Przetwarzającego mogą obejmować: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie,

6) miejsce przetwarzania Danych Osobowych[9], 7) podpisy Stron.

§ 4. CZAS TRWANIA PRZETWARZANIA
(ART. 28 UST. 3 RODO)

Umowa będzie obowiązywać, a Przetwarzający będzie przetwarzał Dane Osobowe przez okres świadczenia przez Przetwarzającego usług związanych z przetwarzaniem Danych Osobowych w ramach umowy źródłowej, z uwzględnieniem postanowień § 11.

§ 5. POLECENIE PRZETWARZANIA DANYCH
(ART. 28 UST. 3 LIT. A RODO)

1. Powierzający poleca Przetwarzającemu oraz osobom działającym z upoważnienia Przetwarzającego przetwarzanie Danych Osobowych w imieniu administratora Danych Osobowych wyłącznie w zakresie wynikającym z RODO, ustawy o ochronie danych osobowych i Umowy oraz niezbędnym do świadczenia usług związanych z przetwarzaniem na podstawie umowy źródłowej.
2. Powierzający nie wyraża zgody ~~/ wyraża zgodę~~ [10] na przekazywanie Danych Osobowych do Państwa trzeciego lub organizacji międzynarodowej, ~~tj.~~ ____.

§ 6. OBOWIĄZEK ZACHOWANIA TAJEMNICY DANYCH OSOBOWYCH ORAZ SPOSOBÓW ICH ZABEZPIECZENIA
(ART. 28 UST. 3 LIT. B RODO)

Przetwarzający zobowiązuje się do bezterminowego zachowania w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy, oraz zobowiązuje się zapewnić, aby osoby mające dostęp do przetwarzania Danych Osobowych zachowały bezterminowo Dane Osobowe oraz sposoby ich zabezpieczenia w tajemnicy, w tym także po rozwiązaniu Umowy lub ustaniu zatrudnienia u Przetwarzającego. W tym celu Przetwarzający dopuści do przetwarzania Danych Osobowych tylko osoby, które zostały upoważnione do przetwarzania tych danych oraz podpisały stosowne zobowiązanie do zachowania bezterminowo w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia.

§ 7. BEZPIECZEŃSTWO PRZETWARZANIA
(ART. 28 UST. 3 LIT. C RODO)

1. Przetwarzający oświadcza, że stosownie do przepisów art. 32 RODO wdrożył odpowiednie środki techniczne i organizacyjne zabezpieczające Dane Osobowe, oraz stale monitoruje adekwatność tych środków, w świetle wymagań stawianych w rzeczonym artykule RODO.
2. Przetwarzający obowiązany jest do prowadzenia i aktualizacji stosownej dokumentacji opisującej zastosowane środki, o których mowa w ust. 1.

---

wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

[9] należy wskazać miejsce, gdzie dane będą przetwarzane, w tym obowiązkowo, gdzie dane będą przechowywane (np. w siedzibie Przetwarzającego; w oddziale Przetwarzającego w Elblągu, ul. Xyz 1/2, Elbląg; w serwerowni dostawcy poczty elektronicznej tj. XYZ sp. z o.o. z/s w Warszawie, ul. Xyz 1/2, Warszawa);

[10] niepotrzebne skreślić; w przypadku niewskazania przez Przetwarzającego potrzeby przekazania Danych Osobowych do Państwa trzeciego lub organizacji międzynarodowej, Powierzający nie wyraża zgody na przekazywanie danych do takiego Państwa lub Organizacji;

3. Przetwarzający na każde żądanie administratora Danych Osobowych lub Powierzającego:

   1) udzieli mu wszelkich informacji dotyczących stosowanych przez Przetwarzającego środków technicznych i organizacyjnych zabezpieczających Dane Osobowe, 2) umożliwi mu dokonanie przeglądu środków, o których mowa w pkt 1, 3) udostępni mu dokumentację, o której mowa w ust. 2.

§ 8. DALSZE POWIERZENIE PRZETWARZANIA (PODPOWIERZENIE)
(ART. 28 UST. 3 LIT. D / ART. 28 UST. 2 i 4 RODO)

1. Powierzający w imieniu administratora Danych Osobowych nie wyraża zgody / ~~wyraża zgodę~~ na (dalsze) powierzenie (tzw. podpowierzenie) przetwarzania Danych Osobowych przez Przetwarzającego innym podmiotom, z uwzględnieniem treści § 5 ust. 2 [11].
2. Przed podpowierzeniem przetwarzania Danych Osobowych, Przetwarzający jest zobowiązany poinformować pisemnie lub email`owo Powierzającego o zamiarze podpowierzenia przetwarzania Danych Osobowych.
3. Informacja o zamiarze podpowierzenia przetwarzania Danych Osobowych zawiera co najmniej:

   1) dane podmiotu, któremu Przetwarzający zamierza podpowierzyć przetwarzanie Danych Osobowych (imię i nazwisko / firmę oraz dane kontaktowe), 2) informacje o:

   a) charakterze i czasie trwania podpowierzenia,
   b) celu ich przetwarzania przez podmiot, któremu będą podpowierzane,
   c) zakresie podpowierzanych Danych Osobowych (w szczególności ich rodzaju),
   d) kategoriach osób, których Dane Osobowe miałyby być podpowierzone,
   e) miejscu przetwarzania Danych Osobowych przez podmiot, któremu będą podpowierzane.
4. Jeżeli Powierzający w terminie **14 dni** od otrzymania wszystkich powyższych informacji nie wyrazi sprzeciwu wobec zamiaru podpowierzenia przetwarzania wskazanemu podmiotowi, Przetwarzający może podpowierzyć przetwarzanie Danych Osobowych, zgodnie z tymi informacjami.
5. Podpowierzenie przetwarzania Danych Osobowych przez Przetwarzającego jest dopuszczalne tylko na podstawie umowy podpowierzenia.
6. Umowa podpowierzenia zostanie zawarta w formie pisemnej (przez którą rozumie się również formę elektroniczną).
7. Na podstawie umowy podpowierzenia podmiot, któremu podpowierzono przetwarzanie Danych Osobowych zobowiąże się do spełniania tych samych obowiązków i wymogów,
   które na mocy Umowy nałożone są na Przetwarzającego. W szczególności Przetwarzający zapewni, aby podmiot, któremu podpowierzono przetwarzanie Danych Osobowych stosowały co najmniej równorzędny poziom ochrony Danych Osobowych co Przetwarzający.

[11] w przypadku niewyrażenia zgody na (dalsze) powierzenie przetwarzania Danych Osobowych, ust. 2-9 nie mają zastosowania;

8. Administratorowi Danych Osobowych oraz Powierzającemu będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podmiotu, któremu podpowierzono przetwarzanie Danych Osobowych (w szczególności uprawnienia w zakresie audytu i inspekcji, o których mowa w § 12).
9. Jeżeli podmiot, któremu podpowierzono przetwarzanie Danych Osobowych nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora Danych Osobowych i Powierzającego za wypełnienie obowiązków tego podmiotu spoczywa na Przetwarzającym. Przetwarzający zobowiązany jest do powiadomienia Powierzającego o każdym przypadku niewywiązywania się przez podmiot, któremu podpowierzono przetwarzanie Danych Osobowych, z jego zobowiązań umownych.

§ 9. WSPÓŁPRACA W ZAKRESIE ŻĄDAŃ, OSOBY KTÓREJ DANE DOTYCZĄ, WYNIKAJĄCYCH Z ROZDZIAŁU III RODO
(ART. 28 UST. 3 LIT. E RODO)

1. Przetwarzający zobowiązuje się pomagać administratorowi Danych Osobowych i Powierzającemu, poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO.
2. W przypadku, gdy osoba, której dane dotyczą skieruje żądanie realizacji jej praw, o których mowa w art. 15-22 RODO, bezpośrednio do Przetwarzającego, Przetwarzający zobowiązany jest przekazać niezwłocznie treść tego żądania (w szczególności treść sprzeciwu, o którym mowa w art. 21 RODO) do administratora Danych Osobowych i Powierzającego. Ponadto, jeżeli administrator Danych Osobowych lub Powierzający nie będzie mógł zrealizować żądań osoby, której dane dotyczą, bez współdziałania Przetwarzającego, Przetwarzający na polecenie administratora Danych Osobowych lub Powierzającego podejmie wskazane przez administratora Danych Osobowych lub Powierzającego czynności.

§ 10. POMOC W REALIZACJI OBOWIĄZKÓW OKREŚLONYCH W ART. 32-36 RODO
(ART. 28 UST. 3 LIT. F RODO)

1. Przetwarzający zobowiązuje się pomagać administratorowi Danych Osobowych i Powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.
2. W ramach realizacji obowiązków, o których w ust. 1, Przetwarzający ma w szczególności obowiązek:
   1) wyznaczenia osób odpowiedzialnych za podjęcie kroków w celu zaradzenia naruszeniu ochrony Danych Osobowych i podjęcie stosownych działań naprawczych
   w uzgodnieniu z administratorem Danych Osobowych i Powierzającym;
   2) zawiadamiania administratora Danych Osobowych o wszelkich naruszeniach ochrony Danych Osobowych. Zawiadomienie powinno nastąpić niezwłocznie, nie później jednak niż w ciągu **48 godzin** od stwierdzenia przez Przetwarzającego naruszenia ochrony Danych Osobowych. Zawiadomienie powinno zawierać informacje, które pozwolą administratorowi Danych Osobowych na przygotowanie zawiadomienia zgodnie z art. 33 ust. 3 RODO (w zakresie art. 33 ust. 3 lit. b RODO Przetwarzający powinien wskazać dane inspektora ochrony danych Przetwarzającego lub oznaczenie innego punktu kontaktowego Przetwarzającego,

od którego można uzyskać więcej informacji). Jeżeli Przetwarzający napotkałby na przeszkody techniczne po stronie administratora Danych Osobowych, uniemożliwiające zawiadomienie go o naruszeniu bezpieczeństwa Danych Osobowych, powinien o tych przeszkodach niezwłocznie zawiadomić Powierzającego;

3) dokumentowania naruszeń ochrony Danych Osobowych, zgodnie z art. 33 ust. 5 RODO – tj. dokumentowania m.in. okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych, w sposób umożliwiający organowi nadzorczemu zweryfikowanie na podstawie tej dokumentacji przestrzegania przez administratora Danych Osobowych i Przetwarzającego art. 33 RODO;

4) udzielania administratorowi Danych Osobowych i Powierzającemu informacji potrzebnych do dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO;

5) udzielania administratorowi Danych Osobowych i Powierzającemu informacji potrzebnych do konsultacji z organem nadzorczym w zakresie oceny skutków dla ochrony danych, o których mowa w art. 36 RODO.

§ 11. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA
(ART. 28 UST. 3 LIT. G RODO)

1. Niezwłocznie po zakończeniu świadczenia usług związanych z przetwarzaniem przez Przetwarzającego Danych Osobowych, jednakże nie później niż w terminie **14 dni** od zakończenia świadczenia tych usług, Przetwarzający zależnie od decyzji administratora Danych Osobowych lub Powierzającego (działającego w imieniu administratora Danych Osobowych):
   1) usuwa Dane Osobowe albo
   2) zwraca administratorowi Danych Osobowych lub Powierzającemu wszelkie Dane Osobowe oraz usuwa wszelkie ich istniejące kopie.
2. Przetwarzający potwierdzi usunięcie lub zwrot Danych Osobowych oraz ich kopii pisemnym protokołem podpisanym przez osobę uprawnioną do składania oświadczeń woli w imieniu Przetwarzającego i umożliwi przeprowadzenie przez administratora Danych Osobowych lub Powierzającego audytu zgodnie z § 12.
3. Stosownie do treści art. 28 ust. 3 lit. g RODO po zakończeniu świadczenia usług związanych z przetwarzaniem Przetwarzający może jednak przetwarzać Dane Osobowe, w zakresie w jakim prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie Danych Osobowych.

§ 12. UDOSTĘPNIANIE INFORMCJI O POWIERZENIU I WERYFIKACJA PRZESTRZEGANIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH
(ART. 28 UST. 3 LIT. H RODO)

1. Przetwarzający zobowiązuje się udostępnić administratorowi Danych Osobowych i Powierzającemu wszelkie informacje niezbędne do wykazania przez administratora Danych Osobowych oraz Przetwarzającego spełnienia obowiązków, o których mowa w art. 28 RODO.

2. Administrator Danych Osobowych oraz Powierzający są uprawnieni do weryfikacji przestrzegania przez Przetwarzającego zasad przetwarzania Danych Osobowych wynikających z RODO, ustawy o ochronie danych osobowych oraz Umowy, w szczególności poprzez:
   1) prawo żądania udzielenia wszelkich informacji dotyczących powierzonych Danych Osobowych, w tym informacji o lokalizacji, w których Przetwarzający przetwarza Dane Osobowe,
   2) prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową [12].
3. Administrator Danych Osobowych lub Powierzający mają obowiązek poinformowania Przetwarzającego o planowanym audycie na **7 dni** przed jego rozpoczęciem. Audyt nie może trwać dłużej niż miesiąc od jego rozpoczęcia.
4. Audyt lub inspekcja przeprowadzane są przez **upoważnionych audytorów**, przez których w ramach niniejszego paragrafu rozumie się, upoważnionego przez administratora Danych Osobowych lub Powierzającego:
   1) pracownika odpowiednio administratora Danych Osobowych lub Powierzającego lub
   2) audytora zewnętrznego – z tym zastrzeżeniem, że audytorem zewnętrznym nie będzie podmiot prowadzący działalność konkurencyjną wobec Przetwarzającego lub jego pracownik lub podmiot współpracujący bez względu na podstawę zatrudnienia lub współpracy. Przetwarzający musi wykazać obszary konkurencyjności wraz ze wskazaniem ryzyk dla Przetwarzającego w przypadku sprzeciwu Przetwarzającego co do udział w audycie wskazanego przez Powierzającego audytora zewnętrznego.
5. Upoważniony audytor ma prawo w szczególności do:
   1) wstępu i oględzin (zwłaszcza sposobu zabezpieczenia) pomieszczeń, w których przetwarzane są Dane Osobowe,
   2) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania Danych Osobowych,
   3) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z powierzeniem przetwarzania na podstawie Umowy,
   4) żądania złożenia ustnych lub pisemnych wyjaśnień przez Przetwarzającego oraz personel Przetwarzającego (w szczególności pracowników), w zakresie niezbędnym do ustalenia stanu faktycznego.
6. Po zakończeniu audytu upoważniony audytor przedstawia wynik audytu w formie protokołu.
7. W przypadku naruszenia ochrony Danych Osobowych u Przetwarzającego lub rażącego naruszenia przez Przetwarzającego przepisów o ochronie Danych Osobowych, Administrator Danych Osobowych oraz Powierzający mają prawo do przeprowadzenie u Przetwarzającego niezapowiedzianej inspekcji.
8. Powierzający może w szczególności przeprowadzić:
   1) darmowy audyt, na odległość, z wykorzystaniem listy weryfikacyjnej – w przeciągu 3 (trzech) pierwszych miesięcy od powierzenia przetwarzania Danych Osobowych Przetwarzającemu,

[12] sposób audytu będzie uwzględniać specyfikę powierzenia przetwarzania;

2) darmowy audyt, w dowolny sposób – 1 (jeden) raz, w każdym roku obowiązywania Umowy,

3) darmowy audyt, o który mowa w § 11 ust. 2, w dowolny sposób - po zakończeniu Umowy,

4) darmowy audyt lub inspekcję, w dowolny sposób – po każdym naruszeniu, o którym mowa w ust. 7.

9. W razie wątpliwości poczytuje się, że:

1) okoliczności umożliwiające przeprowadzenie audytu lub inspekcji, o których mowa w ust. 8 pkt 1-4 nie wykluczają się wzajemnie [13];

2) darmowy audyt / darmowa inspekcja oznacza, że za podejmowane w ramach audytu lub inspekcji czynności Przetwarzający nie nabywa względem Powierzającego jakichkolwiek wierzytelności (np. o zwrot kosztów czy wynagrodzenie dla pracowników Przetwarzającego biorących udział w audycie lub inspekcji).

10. Jeżeli zdaniem Przetwarzającego wydane mu przez administratora Danych Osobowych lub Powierzającego polecenie stanowi naruszenie przepisów RODO lub innych powszechnie obowiązujących przepisów o ochronie danych Przetwarzający zobowiązuje się niezwłocznie poinformować o tym administratora Danych Osobowych lub Powierzającego (w zależności od tego, który z nich wydał polecenie).

§ 13. REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA (ART. 30 UST. 2 i 3 RODO)

Przetwarzający oświadcza, że w związku z zawarciem Umowy, będzie prowadził rejestr wszystkich kategorii czynności przetwarzania, dokonywanych w imieniu administratora Danych Osobowych, w rozumieniu art. 30 ust. 2 i 3 RODO. Rejestr ten Przetwarzający udostępni na każde żądanie administratora Danych Osobowych lub Powierzającego.

§ 14. WYZNACZENIE INSPEKTORA OCHRONY DANYCH (ART. 37 RODO) 1.

Powierzający wyznaczył inspektora ochrony danych:

imię i nazwisko: Sebastian Sobecki

służbowy adres poczty elektronicznej: iod@um.wroc.pl

służbowy nr telefonu: 71 777 77 24

2. Przetwarzający nie wyznaczył inspektora ochrony danych / osobę kontaktową w sprawach dotyczących Danych Osobowych [14]:

imię i nazwisko: …… służbowy nr telefonu: ……

służbowy adres poczty elektronicznej: ……

3. W przypadku zmiany osób, o których mowa w ust. 1 lub 2, Strona u której doszło do zmiany danych tej osoby, zobowiązana jest do niezwłocznego zawiadomienia o tym drugiej Strony, na adres email wskazany w ust. 1 lub 2 (w zależności od tego czy o

[13] przykład: jeżeli Umowa będzie obowiązywała przez 6 miesięcy danego roku i w trakcie jej obowiązywania zaistniało 1 (jedno) naruszenie ochrony danych: możliwe jest przeprowadzenie czterech audytów po jednym na każdą okoliczność wymienioną w ust. 8 pkt 1-4;

[14] niepotrzebne skreślić

zmianie zawiadamia Przetwarzający czy Powierzający) wraz ze wskazaniem aktualnych danych, o których mowa odpowiednio w ust. 1 lub 2.

§ 15. POSTANOWIENIA DODATKOWE
(ART. 28 UST. 3 RODO)

1. Każda ze Stron zobowiązana jest do poinformowania osób przez siebie upoważnionych do określonych czynności w związku z realizacją Umowy lub umowy źródłowej (w szczególności osób reprezentujących stronę lub osób kontaktowych), o tym, że druga Strona będzie przetwarzała ich dane osobowe jako administrator, w celach, niezbędnych do należytego wykonania Umowy i umowy źródłowej oraz do wypełnienia wynikających z powszechnie obowiązujących przepisów obowiązków prawnych ciążących na Stronach jako administratorach danych. Poinformowanie, o którym mowa w zdaniu poprzednim, będzie zawierać ponadto taką treść, która umożliwi drugiej stronie ewentualne powołanie się na art. 14 ust. 1 lit. a RODO.
2. W celu realizacji obowiązku, o którym mowa w ustępie poprzedzającym zd. 2, Powierzający w załączniku nr 3 do Umowy przekazuje Przetwarzającemu treść obowiązku informacyjnego dla personelu Przetwarzającego. Przetwarzający zobowiązany jest w terminie 7 dni od zawarcia Umowy do przekazania Powierzającemu treści obowiązku informacyjnego, o którym mowa w art. 14 RODO, dla personelu Powierzającego, a po tym terminie, zobowiązany będzie względem tego personelu do samodzielnej realizacji obowiązku informacyjnego, o którym mowa w art. 14 RODO.

§ 16. POSTANOWIENIA KOŃCOWE

1. O ile co innego nie wynika wyraźnie z umowy (np. § 14 ust. 3), wszelkie zmiany Umowy wymagają formy pisemnej (przez którą rozumie się również formę elektroniczną, w rozumieniu kodeksu cywilnego) pod rygorem nieważności.
2. Spory związane z wykonywaniem Umowy rozstrzygane będą przez sąd właściwy dla siedziby Powierzającego (tj. pl. Nowy Targ 1-8, 50-141 Wrocław).
3. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, w tym jeden dla Wykonawcy

§ 17. ZAŁĄCZNIKI

Integralną część Umowy stanowią następujące załączniki:

1) szczegóły powierzenia przetwarzania danych,
2) lista kontrolna - kryteria wyboru podmiotu przetwarzającego, któremu administrator zamierza powierzyć dane osobowe,
3) wzór klauzuli informacyjnej stosowanej przez Powierzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę.

Powierzający **Przetwarzają**

Wrocław, dnia _____ 2023 r.

SZCZEGÓŁY POWIERZENIA (ADMINISTRATORZY, ZBIORY / RODZAJE I ZAKRES DANYCH, KATEGORIE OSÓB, RODZAJ OPERACJI PRZETWARZANIA, LOKALIZACJE PRZETWARZANIA)

L.P.	Nazwa i dane kontaktowe administratora Danych Osobowych	Nazwa zbioru / rodzaj i zakres powierzanych Danych Osobowych[15]	Kategorie osób, których Dane Osobowe dotyczą	Rodzaj operacji przetwarzania[16]	Lokalizacje Przetwarzającego, w których przetwarzane będą dane osobowe
1	Prezydent Wrocławia Gmina Wrocław Plac Nowy Targ 1-8 50-141 Wrocław	Zbiór: Pisma Imiona, nazwisko, imię ojca, imię matki, adres zamieszkania, data urodzenia, miejsce urodzenia, numer PESEL, numer telefonu, seria i numer dowodu osobistego, numer NIP, zawód, miejsce pracy, wykształcenie, numer decyzji, dane zawarte w dokumentacji powstałej i powstającej w związku z działalnością jednostki samorządu terytorialnego, w której zostały utworzone.	Adresaci korespondencji urzędowej	zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie,	

[15] jeżeli Dane Osobowe nie są przetwarzane w nazwanym zbiorze, należy wskazać wyłącznie rodzaj (tj. dane zwykłe oraz – jeżeli są przetwarzane – dane wrażliwe) oraz zakres danych np. dane zwykłe: imię i nazwisko, adres zamieszkania, telefon; dane wrażliwe: dane o zdrowiu;

[16] **operacje wykonywane na danych osobowych przez Przetwarzającego mogą obejmować:** zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

				ograniczanie, usuwanie lub niszczenie	
2	Prezydent Wrocławia Gmina Wrocław Plac Nowy Targ 1-8 50-141 Wrocław	Zbiór: Archiwum Zakładowe Imiona, nazwisko, imię ojca, imię matki, adres zamieszkania, miejsce urodzenia, numer PESEL, seria i numer dowodu osobistego, numer NIP, zawód, miejsce pracy, wykształcenie, przynależność partyjna, nałogi. Szczególne kategorie danych: pochodzenie rasowe lub etniczne, poglądy polityczne, przynależność do związków zawodowych, dane dotyczące zdrowia, wyroki skazujące, czyny zabronione lub związane ze środkami bezpieczeństwa	Osoby, których dotyczą materiały archiwalne powstałe i powstające w związku z działalnością jednostki samorządu terytorialnego, w której zostały utworzone	zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie	

Powierzający **Przetwarzający**

_____ _____

LISTA KONTROLNA - KRYTERIA WYBORU PODMIOTU PRZETWARZAJĄCEGO, KTÓREMU POWIERZAJĄCY ZAMIERZA POWIERZYĆ PRZETWARZANIE DANYCH OSOBOWYCH

Niniejsze kryteria stworzone zostały w celu wstępnej weryfikacji podmiotu przetwarzającego, w zakresie spełniania przez niego podstawowych wymogów RODO.

Kryteria wyboru podmiotu przetwarzającego oparte zostały o:

1) art. 28 ust. 1 RODO, zgodnie z którym *„1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą*" oraz

2) motyw 81 RODO, zgodnie z którym: *„(81) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora*".

DANE PODMIOTU PRZETWARZAJĄCEGO (dalej również **PP**):

(nazwa podmiotu, adres siedziby, KRS/NIP – jeżeli zostały nadane)

DOTYCZY UMOWY / ZAMÓWIENIA:

(w przypadku braku numeru/symbolu należy opisać hasłowo przedmiot umowy)

PLANOWANY OKRES POWIERZENIA PRZETWARZANIA:	01.01.2024-31.12.2024

L.p.	PYTANIE	ODPOWIEDŹ
	SEKCJA I: PYTANIA PODSTAWOWE	
1.	Czy PP będzie wykorzystywać / przetwarzać dane osobowe administratora we własnych celach / na własne potrzeby lub w celach / na potrzeby podmiotów innych niż administrator? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie jakie konkretne rodzaje danych osobowych administratora PP zamierza wykorzystywać/przetwarzać i w jakim i czyim celu / na jakie i czyje potrzeby, w szczególności czy PP zamierza wykorzystywać / przetwarzać we własnych celach / na własne potrzeby dane telemetryczne administratora.)***	
2.	Czy PP zamierza udostępnić dane osobowe administratora odbiorcom, w rozumieniu art. 4 pkt 9 RODO? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie tych odbiorców.)***	
3.	Czy realizując umowę / zamówienie PP korzystał będzie z usług podmiotów zewnętrznych / podwykonawców, którym udostępni/przekaże dane osobowe administratora (uwaga: za takie podmioty uważa się np. podmioty świadczące usługę poczty email na rzecz PP)?	

4.	Czy PP korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? ***(Jeżeli odpowiedź jest twierdząca proszę o wskazanie w jaki sposób PP sprawdził odpowiedni poziom ochrony, np. na podstawie oświadczeń podmiotów zewnętrznych / podwykonawców, na podstawie przedłożonych przez nich certyfikatów, na podstawie audytu przeprowadzonego w tych podmiotach przez PP.)***	
5.	Czy PP w związku ze świadczeniem przez PP usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. h RODO, będzie przetwarzał dane osobowe administratora w krajach Unii Europejskiej? (***Jeżeli odpowiedź jest twierdząca, proszę o wskazanie krajów Unii Europejskiej, w których PP będzie przetwarzał dane osobowe administratora. Uwaga! Jeżeli Przetwarzający przetwarza dane osobowe administratora na terenie Polski należy wskazać również Polskę.)***	
6.	Czy w celu świadczenia przez PP usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. h	

L.p.	**PYTANIE**	**ODPOWIEDŹ**
	RODO, dane osobowe administratora będą przetwarzane w państwie trzecim w szczególności będą przekazywane do państwa trzeciego (np. dostawca poczty email PP przechowujący pocztę email na serwerach w USA / Wielkiej Brytanii) lub organizacji międzynarodowej, w rozumieniu rozdziału V RODO? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie: w których państwach / przez które organizacje międzynarodowe dane administratora miałby być przetwarzane, przez który podmiot – nazwa i siedziba podmiotu (pod)przetwarzającego (jeżeli PP jest również takim podmiotem powinien wymienić również siebie) – oraz wskazanie dla każdego takiego podmiotu podstawy przekazania danych zgodnej z rozdziałem V RODO, np. decyzja komisji, o której mowa w art. 45 RODO, standardowe klauzule umowne, o których mowa w art. 46 ust. 5 zd. 2 RODO, wiążące reguły korporacyjne, o których mowa w art. 47 RODO***	

	itd.)	
7.	Czy do PP (i ewentualnych podmiotów, którym PP (pod)powierzy dane) ma zastosowanie art. 3 ust. 2 RODO, a jeżeli tak czy PP (i ewentualny podmiot któremu PP (pod)powierzył dane) wyznaczył przedstawiciela, o którym mowa w art. 27 RODO? ***(Jeśli odpowiedź jest twierdząca, proszę o wskazanie wszystkich podmiotów (w tym ew. również PP) do których zastosowanie ma art. 3 ust. 2 RODO oraz aktualnych informacji kontaktowych do ww. przedstawiciela, w szczególności proszę wskazać dane dla wszystkich przewidzianych przez PP form kontaktu np. adres korespondencyjny, adres email, numer faxu, numer telefonu itd.)***	
8.	Czy PP stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania, o których mowa w art. 40 RODO? ***(Jeżeli odpowiedź jest przecząca, proszę o wskazanie dlaczego nie stosuje się do takich kodeksów. Jeżeli odpowiedź jest twierdząca proszę o wskazanie do jakich – nazwa - kodeksów się stosuje i przez który organ nadzorczy były przyjęte.)***	

9.	Czy PP objęty jest monitorowaniem przestrzegania kodeksu postępowania, przez akredytowany podmiot monitorujący, o których mowa w art. 41 RODO? ***(Jeżeli odpowiedź jest przecząca proszę o wskazanie dlaczego nie jest objęty. Jeżeli odpowiedź jest twierdząca proszę o wskazanie danych podmiotu monitorującego oraz podmiotu który udzielił mu akredytacji.)***	

L.p.	PYTANIE	ODPOWIEDŹ
10.	Czy PP otrzymał certyfikat zgodności z RODO, o którym mowa w art. 42-43 RODO? ***(Jeżeli odpowiedź jest twierdząca proszę o przekazanie kopii/skanu tego certyfikatu.)***	
11.	Czy PP posiada referencje od innych podmiotów, które obsługuje/obsługiwał i u których w ramach świadczonej obsługi przetwarzał dane osobowe jako podmiot przetwarzający? ***(Jeżeli odpowiedź jest twierdząca proszę o przekazanie kopii/skanu takich referencji.)***	
SEKCJA II: WIEDZA FACHOWA		
12.	Czy przepisy prawa wymagają, aby PP wyznaczył inspektora ochrony danych w rozumieniu art. 37-39 RODO (dalej **IOD**)?	
13.	Czy PP wyznaczył IOD? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie aktualnych informacji kontaktowych do IOD, w szczególności proszę wskazać dane dla wszystkich przewidzianych przez PP form kontaktu z IOD np. adres korespondencyjny, adres email, numer faxu, numer telefonu itd.)***	

14.	Czy PP wyznaczył inną niż IOD osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie aktualnych informacji kontaktowych do tych osób, w szczególności proszę wskazać dane dla wszystkich przewidzianych przez PP form kontaktu z tymi osobami np. adres korespondencyjny, adres email, numer faxu, numer telefonu itd.)***	
15.	Czy osoby po stronie PP dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. świadectwo ze szkolenia, certyfikat ze szkolenia, oświadczenie pracownika o odbyciu szkolenia itp.)***	

L.p.	**PYTANIE**	**ODPOWIEDŹ**
16.	Czy osoby zatrudnione[17] w PP przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych osobowych przez PP? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. świadectwo ze szkolenia, certyfikat ze szkolenia, oświadczenie pracownika o odbyciu szkolenia itp.).***	
17.	Czy osoby zatrudnione w PP przy przetwarzaniu danych zostały przeszkolone w zakresie zasad bezpieczeństwa informacji? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. świadectwo ze szkolenia, certyfikat ze szkolenia, oświadczenie pracownika o odbyciu szkolenia itp.).***	

[17] poprzez „osoby zatrudnione" lub „pracowników" w ramach niniejszej tabeli rozumie się nie tylko pracowników, w rozumieniu Kodeksu pracy, ale także wszystkie osoby, którym PP stosownie – do treści art. 29 RODO – udzielił lub zgodnie z prawem powinien był udzielić upoważnień do przetwarzania danych osobowych (np. praktykantów, stażystów),

18.	Czy PP dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać jakie działania podejmowane są przez PP w celu doskonalenia wiedzy pracowników oraz – w miarę możliwości – częstotliwość tych działań).***	
SEKCJA III: ZASOBY		
19.	Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez PP od tych, które należą do innych podmiotów (np. czy w tym samym pomieszczeniu serwerowni znajdują się serwery zarządzane wyłącznie przez PP czy przez PP i inne podmioty; czy z komputerów z których korzystają osoby zatrudnione przez PP i na których przetwarzane są dane osobowe administratora, korzystają inne osoby nieuprawnione do przetwarzania danych osobowych administratora)? ***(Jeżeli odpowiedź jest przecząca, proszę wskazać/opisać w jakich okolicznościach dochodzi do wspólnego wykorzystywania środków przetwarzania przez PP i inne podmioty.)***	
20.	Czy PP wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii/skanu lub opisu tej procedury).***	
21.	Czy PP przewidział konkretny, maksymalny czas na zawiadomienie administratora o stwierdzeniu naruszenia ochrony danych osobowych, o którym mowa w art. 33 RODO? ***(Jeśli odpowiedź jest twierdząca, proszę wskazać ten czas***	

	np. zawiadomienie administratora następuję nie później niż 48 godzin od stwierdzenia naruszenia przez PP).	
22.	Czy PP dokumentuje wszelkie naruszenia ochrony danych osobowych, zgodnie z art. 33 ust 5 RODO? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii/skanu szablonu takiej dokumentacji).***	
23.	Czy PP prowadzi rejestry czynności przetwarzania danych osobowych (jako administrator oraz jako procesor), o których mowa w art. 30 RODO?	
24.	Czy PP wdrożył następujące zasady zarządzania bezpieczeństwem informacji:	
a)	system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii/ skanu certyfikatu dla tej normy.)***	
b)	zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii/ skanu certyfikatu dla tej normy.)***	
c)	zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?	
25.	Czy PP wdrożył inne, niż wskazane w pozycji 24 tabeli, zasady ochrony informacji): ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii / skanu tych dokumentów.)***	
a)	czy PP wdrożył: Ramy prywatności – PN-ISO/IEC 29100, Praktyczne zasady ochrony informacji o identyfikowalnych osobach – PN-ISO/IEC 29151, wytyczne dotyczące oceny skutków dla prywatności – PN-ISO/IEC 29131? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii / skanu certyfikatu dla tej normy.)***	

b)	czy PP wdrożył inne niż wymienione w lit. a zasady, standardy, regulaminy, procedury, polityki, biblioteki lub zbiory najlepszych praktyk mające znaczenie dla ochrony danych osobowych (np. polityka bezpieczeństwa informacji, polityka ochrony danych osobowych, zbiór najlepszych praktyk dla ochrony danych osobowych)? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii / skanu dokumentów, w których ujęto ww. zasady, standardy, regulaminy itd.)***	
26.	Czy PP dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą?	
27.	Czy PP przeprowadzał szacowanie ryzyka pod kątem ochrony prywatności (w szczególności ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o którym mowa w art. 35 RODO)?	
28.	Czy szacowanie ryzyka pod kątem ochrony prywatności zostało udokumentowane (np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania)? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii / skanu tych dokumentów.)***	

L.p.	**PYTANIE**	**ODPOWIEDŹ**
29.	Czy PP okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie częstotliwości prowadzenia takich działań.)***	
30.	Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników szacowania ryzyka?	

31.	Czy PP wdrożył odpowiednie środki techniczne i organizacyjne, które zapewniają procesowi przetwarzania danych osobowych stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, w tym:	
a)	pseudonimizację i szyfrowanie danych osobowych,	
b)	zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,	
c)	zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	
d)	procedury odtwarzania systemu po awarii, procedury ich testowania oraz czy stosuje je praktycznie?	
32.	Czy w przypadku wykorzystywania przez administratora szyfrowania, wdrożonego przez PP, PP ma dostęp lub może uzyskać dostęp (np. resetując hasło i ustanawiając własne) do zaszyfrowanych przez administratora treści?	
33.	Czy PP prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie częstotliwości prowadzenia audytów.)***	

L.p.	**PYTANIE**	**ODPOWIEDŹ**

34.	Czy PP poddawał audytom prowadzonym przez niezależnych audytorów zewnętrznych funkcjonujący w jego organizacji system ochrony danych osobowych? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie ile takich audytów zostało przeprowadzonych w okresie ostatnich dwóch lat).***	
35.	Czy wnioski z audytów, o których mowa w pozycji 33 i 34 tabeli, zostały udokumentowane? ***(Jeżeli odpowiedź jest twierdząca, proszę o przekazanie kopii/skanu dokumentu z takiego audytu.)***	
36.	Czy PP jest podda się audytowi przetwarzania danych osobowych przeprowadzonemu / inspekcji przetwarzania danych osobowych przeprowadzanej przez administratora lub audytora upoważnionego przez administratora?	
37.	Czy w związku z realizacją prawa administratora do audytu/inspekcji, o którym mowa w art. 28 ust. 3 lit. h RODO administrator zobowiązany jest do zapłaty jakichkolwiek kwot na rzecz PP (np. zapłaty wynagrodzenia za udział pracowników PP w audycie)?	
38.	Czy w przypadku braku ustaleń co do wysokości wynagrodzenia dla PP za przeprowadzenie audytu lub inspekcji, PP umożliwi administratorowi przeprowadzenie takiego audytu lub inspekcji? **(tak – pomimo braku płatności audyt lub inspekcja będą możliwe; nie – brak płatności uniemożliwi audyt lub inspekcję)**	
39.	Czy osoby delegowane przez PP do obsługi administratora posiadają nadane upoważnienia do przetwarzania danych osobowych? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP potwierdzających powyższe okoliczności, np. samodzielne pisemne oświadczenie PP o upoważnieniu pracownika do przetwarzania danych; upoważnienie do przetwarzania zawarte w umowie o pracę.)***	

L.p.	PYTANIE	ODPOWIEDŹ
40.	Czy wszystkie osoby upoważnione do przetwarzania danych osobowych przez PP w ramach obsługi administratora zostały obowiązane do zachowania tych danych, jak i sposobów ich zabezpieczenia, w tajemnicy? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP potwierdzających powyższe okoliczności, np. pisemne oświadczenie pracownika o zachowaniu poufności, zawarte w umowie o pracę.)*** Czy obowiązek ten rozciąga się również na okres po ustaniu zatrudnienia tych osób?	
41.	Czy, po godzinach pracy organizacji, osoby inne niż uprawnione do przetwarzania danych (np. firma sprzątająca, ochrona), mają za zgodą lub wiedzą PP dostęp do pomieszczeń, w których ma miejsce przetwarzanie danych osobowych? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać jakie podmioty mogą mieć za wiedzą lub zgodą PP dostęp do pomieszczeń, w których przetwarzane są dane osobowe.)*** Czy osoby takie zostały zobowiązane do zachowania poufności (np. w stosownej umowie)?	
SEKCJA IV: RETENCJA I USUWANIE DANYCH		
42.	Czy dane osobowe przetwarzane są wyłącznie przez czas niezbędny do realizacji celu przetwarzania?	
43.	W jaki sposób PP ustala czy nie minął już okres przechowywania danych osobowych?	

44.	Czy dane osobowe administratora, dla których nie istnieją dla PP postawy do przetwarzania są bezpowrotnie usuwane? ***(Jeżeli odpowiedź jest twierdząca, proszę wskazać w jaki sposób usuwane są dane np. dane w formie papierowej niszczone są w niszczarkach, dane w formie elektronicznej usuwane są z systemu za pomocą specjalistycznego oprogramowania do usuwania danych uniemożliwiającego ich odtworzenie.)***	

SEKCJA V: BEZPIECZEŃSTWO

L.p.	PYTANIE	ODPOWIEDŹ
45.	W jaki sposób PP informuje pracowników o obowiązujących wewnętrznych procedurach bezpieczeństwa informacji i ochrony danych osobowych?	
46.	Czy pracownicy PP pozwalaną na przebywanie w obszarze przetwarzania danych osób nieuprawnionych bez nadzoru?	
47.	Czy pracownicy PP przechowują, korzystają i transportują dokumenty zawierające powierzone PP dane osobowe w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby postronne? W szczególności czy dane osobowe gromadzone w formie papierowej, w sytuacji, gdy nie ma konieczności ich wykorzystania w bieżącej pracy (w tym po zakończeniu pracy), przechowywane są w zamykanych na zamek szafach / szafkach / szufladach, do których nie mają dostępu osoby nieupoważnione?	
48.	Czy pracownicy PP niszczą dokumenty papierowe zawierające dane osobowe przy użyciu niszczarki dokumentów zapewniającej odpowiedni poziom bezpieczeństwa niszczonych dokumentów?	

L.p.	PYTANIE	ODPOWIEDŹ
54.	Czy PP doświadczył naruszenia ochrony danych osobowych, dla którego konieczne było poinformowanie osób, których ono dotyczyło? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie ile takich naruszeń miało miejsce w okresie ostatnich dwóch lat).***	
49.	Czy programy, w których przetwarzane są powierzone dane odnotowują, kto i kiedy dane wprowadzał, zmieniał, usuwał?	
50.	W jaki sposób zabezpieczany jest dostęp do systemów informatycznych, w których przetwarzane są powierzone dane?	
51.	Czy w przypadku przenoszenia powierzonych danych na nośnikach elektronicznych/optycznych ich zawartość jest szyfrowana?	
SEKCJA VI: NEGATYWNE DOŚWIADCZENIA PODMIOTU		
53.	Czy PP doświadczył naruszenia ochrony danych osobowych, dla którego konieczne było poinformowanie organu nadzorczego? ***(Jeżeli odpowiedź jest twierdząca, proszę o wskazanie ile takich naruszeń miało miejsce w okresie ostatnich dwóch lat).***	

55.	Czy stwierdzono prawomocną decyzją UODO/innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez PP? ***(Jeśli odpowiedź jest twierdząca, proszę wskazać dla wszystkich dotychczasowych naruszeń z okresu ostatnich dwóch lat: miesiąc i rok w którym nastąpiło naruszenie, podmiot, który wydał decyzję/wyrok oraz sygnaturę sprawy. Jeżeli naruszenie miało miejsce przed dwoma laty proszę o zawarcie takiej informacji)*** Czy UODO/organ nadzorczy nakazał/zalecił PP podjęcie określonych działań naprawczych? ***(Jeśli odpowiedź jest twierdząca, proszę o wskazanie czy te nakazy / zalecenia zostały w pełni zrealizowane).***	

Oświadczam, że wszystkie informacje zawarte w niniejszej liście kontrolnej są zgodne z prawdą.

data: _____

podpis: _____
(imię i nazwisko osoby uprawnionej do reprezentowania Przetwarzającego)

Załączniki:
1) Załącznik

Załącznik do ankiety – Standardowe środki techniczne i organizacyjne

Niniejszy załącznik przedstawia ogólny opis standardowych środków technicznych i organizacyjnych stosowanych przy świadczeniu dla klientów usług związanych z przetwarzaniem danych osobowych. Umowa główna może określać dodatkowe lub inne środki techniczne i organizacyjne uzgodnione przez Strony i w tym zakresie postanowienia Umowy głównej będą miały pierwszeństwo przed postanowieniami niniejszego załącznika.

I. Środki organizacyjne - Procedury i polityki obowiązujące w grupie Comarch

1. W spółkach z grupy Comarch wdrażane są niezbędne procedury i polityki służące m.in. zapewnieniu bezpieczeństwa, poufności, integralności i dostępności danych klientów (w tym danych osobowych, w stosunku do których administratorami są klienci), do których w ramach świadczonych usług uzyskują dostęp pracownicy lub współpracownicy spółek z grupy Comarch.
2. Spółka Comarch S.A. posiada certyfikat ISO 27001 i wdrożyła procedury i powiązane z nimi instrukcje określające w szczególności:

a) Politykę bezpieczeństwa
b) Politykę zarządzania siecią informatyczną Comarch
c) Zasady administracji systemami i aplikacjami
d) Zasady przebywania na terenie Comarch i dostępu do pomieszczeń Comarch
e) Zasady użytkowania aktywów i wynoszenie sprzętu
f) Zasady zabezpieczenia komputerów osobistych
g) Zasady korzystania z nośników informacji
h) Zasady dostępu zdalnego
i) Zasady bezpieczeństwa poczty elektronicznej
j) Politykę haseł
k) Politykę ciągłości działania
l) Politykę antywirusową

3. W pozostałych spółkach z grupy Comarch wdraża się niezbędne procedury i polityki co do zasady oparte na procedurach obowiązujących w głównej spółce w grupie, w zakresie uwzględniającym specyfikę i działalność tych spółek.
4. Wdrażane są ponadto dedykowane procedury służące zapewnieniu prawidłowego wykonania wynikających z RODO obowiązków spółek Comarch jako administratorów oraz obowiązków spółek Comarch jako podmiotów przetwarzających (w stosunku do danych klientów).
5. Spółki z grupy Comarch współpracują w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniając tym samym odpowiedni standard bezpieczeństwa dla klientów grupy Comarch.

II. Środki techniczne i organizacyjne – kontrola dostępu

1. W spółkach z grupy Comarch wdrażane są odpowiednie środki techniczne i organizacyjne zapewniające ograniczenie dostępu do budynków, systemów, środowisk i zbiorów danych wyłącznie dla osób upoważnionych.
2. W budynkach Comarch wydzielane są strefy publicznie dostępne oraz strefy z dostępem zastrzeżonym dla osób upoważnionych.
3. Pracownicy lub współpracownicy korzystają z kart dostępowych lub stosowane są inne metody kontroli fizycznego dostępu do nieruchomości, budynków lub pomieszczeń Comarch, zapewniające kontrolę dostępu poszczególnych osób odpowiednią do zakresu ich uprawnień.
4. Nadawanie uprawnień poszczególnym pracownikom lub współpracownikom w zakresie dostępu do systemów wewnętrznych Comarch oraz środowisk klienta podlega procedurze umożliwiającej kilkustopniową weryfikację wniosku o nadanie uprawnień.
5. Dostęp do systemów wewnętrznych i środowisk oraz danych klientów możliwy jest tylko dla upoważnionych pracowników lub współpracowników po zalogowaniu na indywidualne konto i przy użyciu indywidualnego hasła zgodnego z Polityką haseł.
6. Zdalny dostęp pracowników lub współpracowników do sieci grupy Comarch i późniejsza wymiana informacji odbywają się po uwierzytelnieniu przy wykorzystaniu bezpiecznych mechanizmów, zapewniających poufność i integralność (np. VPN IPSec).
7. W celu zapewnienia bezpieczeństwa, tam gdzie jest to uzasadnione oraz zgodne z prawem, Comarch stosuje monitoring i współpracuje z firmami ochroniarskimi.

III. Środki techniczne i organizacyjne – Comarch Data Center

1. Comarch oferuje klientom korzystanie z Comarch Data Center, tj. data center zarządzanych przez jedną ze spółek z grupy Comarch.
2. Comarch Data Center bazuje na praktykach ITIL v3. w zakresie następujących procesów: zarządzanie zmianą (change management), zarządzanie incydentem (incident management), zarządzanie problemem (problem management), service level management oraz zarządzanie konfiguracją (configuration management). Ponadto, wdrożone są odpowiednie procesy w zakresie : zarządzania aktualizacjami i łatkami (patch management), zarządzanie ryzykiem, procedury backupowe i odtworzeniowe, zarządzanie ciągłością biznesu (business continuity management), raportowania, DRP, przeglądów logów oraz przeglądy dostępów i uprawnień.
3. Backup systemów wewnętrznych podlega centralnemu systemowi backupów zgodnie z Procedurą Backup serwerów.
4. Backup systemów klientów oraz backup danych klientów podlegają zasadom określonym w umowach z klientami. Standardowe procedury Comarch Data Center przewidują maksymalny okres retencji backupów

do 3 miesięcy), przy czym okres retencji może zostać wydłużony na żądanie klienta zgodnie z postanowieniami Umowy Głównej.

5. Wstęp do Comarch Data Center mają jedynie inżynierowie Comarch Data Center oraz działy bezpieczeństwa. Inne osoby mogą przebywać na terenie Comarch Data Center tylko w uzasadnionych przypadkach oraz wyłącznie w obecności przedstawiciela Comarch. Dostęp do poszczególnych pomieszczeń na terenie Comarch Data Center może podlegać dalszym ograniczeniom.
6. Stosowana jest logiczna bądź fizyczna separacja środowisk poszczególnych Klientów (VLANy, VMy itp.)
7. Do poszczególnych środowisk mają dostęp jedynie pracownicy lub współpracownicy odpowiedzialni za obsługę poszczególnych klientów i ich działania na systemach klientów są logowane.
8. Wymogowi „segregation of duties" podlegają również inżynierowie Comarch Data Center. W związku z tym , tworzone są dedykowane zespoły dla:

a) systemów Linux/Unix,
b) systemów Windows,
c) baz danych,
d) systemów FireWall (wewnętrznych) oraz Load Balancerów.
e) infrastruktury sieciowej w Data Center oraz FireWalli zewnętrznych

9. Każdy ośrodek Data Center wyposażony jest w dwie linie klastrów systemów FireWall od dwóch czołowych, niezależnych producentów.

a) Klaster zewnętrzny chroniący dostępu do DMZ,
b) Klaster wewnętrzny kontrolujący przepływy danych pomiędzy DMZ a strefą Bazodanową.

10. W Comarch Data Center stosuje się kilka niezależnych łączy internetowych dywersyfikując media (np. miedź, światło, radio, uruchomiony protokół BGP).
11. Komunikacja pomiędzy siecią Klienta a Comarch Data Center jest szyfrowana (np. IPSec, SSL VPN).
12. Comarch Data Center stosuje:

a) niezależne i redundantne obiegi klimatyzacji z jednym aktywnym obiegiem;
b) redundantne linie energetycznie z jedną aktywną ścieżką;
c) systemy zasilania awaryjnego (UPS'y lub generatory prądotwórcze);
d) wielostrefową ochronę przeciwpożarową;
e) system gaśniczy oparty o gaz neutralny lub gaz chemiczny;
f) alarm przeciwpożarowy oraz automatyczna notyfikacja.

13. W przypadku decyzji Klienta o wyborze innego data center, stosowane środki techniczne i organizacyjne określa wybrany dostawca usług. W przypadku, gdy Comarch korzysta z podwykonawcy w zakresie świadczenia usług hostingowych dla Klienta, podwykonawca zobowiązany jest do wdrożenia

odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO oraz Umowy powierzenia zawartej przez Comarch z Klientem.

IV. Środki techniczne i organizacyjne – usługi serwisowe

1. W spółkach z grupy Comarch wdraża się niezbędne środki techniczne i organizacyjne mające na celu zapewnienie ograniczenia dostępu do systemów obsługi zgłoszeń serwisowych oraz systemów, środowisk i zbiorów danych klienta dostępnych zdalnie wyłącznie dla osób upoważnionych przy zagwarantowaniu bezpieczeństwa, poufności, integralności i dostępności danych.
2. Komunikacja z systemami obsługi zgłoszeń jest szyfrowana (SSL).
3. Nadawanie uprawnień poszczególnym pracownikom, współpracownikom lub upoważnionym przedstawicielom klienta w zakresie dostępu do systemów obsługi zgłoszeń oraz kontrola dostępu do tych systemów podlega ogólnym procedurom kontroli dostępu wdrożonym w spółkach z grupy Comarch.
4. Dla systemów obsługi zgłoszeń wdrożone są odpowiednie procesy w zakresie : zarządzanie aktualizacjami i łatkami (patch management), procedury backupowe i odtworzeniowe, okresowe przeglądy logów oraz przeglądy dostępów i uprawnień.
5. Serwery hostujące systemy obsługi zgłoszeń są zainstalowane w serwerowniach z ograniczonym dostępem dla uprawnionych, wymienionych z imienia i nazwiska pracowników Comarch. Serwerownie wyposażone są systemy zasilania awaryjnego (UPS).
6. Dostęp pracowników lub współpracowników do dostępnych zdalnie środowisk Klienta i późniejsza wymiana informacji odbywają się po uwierzytelnieniu przy wykorzystaniu bezpiecznych mechanizmów, zapewniających poufność i integralność (np. VPN IPSec).

V. Zarządzanie incydentami bezpieczeństwa

W Comarch wdrożono procedurę zarządzania incydentami naruszenia bezpieczeństwa
i nałożono na wszystkich pracowników obowiązek zgłaszania wszelkiego rodzaju incydentów naruszenia bezpieczeństwa, w tym incydentów dotyczących naruszenia ochrony danych osobowych.

VI. Szkolenia i audyty

1. W Comarch wdrożono procedurę zapewniającą okresowe szkolenia pracowników
   z zakresu obowiązującej polityki i procedur bezpieczeństwa oraz przepisów i procedur dotyczących ochrony danych osobowych.
2. Audyty bezpieczeństwa systemów wewnętrznych grupy Comarch przeprowadzane są okresowo przez Dział Bezpieczeństwa Wewnętrznego Comarch S.A.

3. Comarch S.A. okresowo przechodzi audyty realizowane przez jednostki certyfikujące.
4. Audyty systemów klientów podlegają zasadom określonym w umowach z klientami. Comarch współpracuje z klientami w zakresie kontroli i audytów przeprowadzanych przez klientów lub wyznaczonych audytorów zewnętrznych w zakresie uzgodnionym przez strony w umowie, przy zachowaniu procedur bezpieczeństwa obowiązujących w grupie Comarch oraz przy uwzględnieniu tajemnicy przedsiębiorstwa oraz obowiązku zachowania w poufności danych i warunków współpracy z innymi klientami.

KLAUZULA INFORMACYJNA
INFORMACJE DOTYCZĄCE PRZETWARZANIA TWOICH DANYCH OSOBOWYCH

Niniejszą informację otrzymałeś w związku z obowiązkami określonymi w art. 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 (ogólne rozporządzenie o ochronie danych) (Dziennik Urzędowy Unii Europejskiej z dnia 4 maja 2016 r. L 119/1).

*** w zależności od źródła danych z art. 13 i/lub 14 RODO**

Administrator danych

Administratorem Pani/Pana danych osobowych jest Prezydent Wrocławia. Można się z nami skontaktować w następujący sposób:

- listownie na adres: Prezydent Wrocławia, Urząd Miejski Wrocławia, pl. Nowy Targ 1-8, 50-141 Wrocław,
- przez e-mail: *kum@um.wroc.pl*
- telefonicznie: *+48 71 777 87 88*

Cele przetwarzania danych

Będziemy przetwarzać Pani/Pana dane osobowe, w celu:
realizacji postanowień wynikających z Umowy zawartej przez administratora, z Twoim pracodawcą/zleceniodawcą/podmiotem, w którym odbywasz staż/praktykę (w tym w celach kontaktowych).

Podstawy prawne przetwarzania

Będziemy przetwarzać Pani/Pana dane osobowe na podstawie[•].
gdyż jest to niezbędne do wykonania zadania realizowanego w interesie publicznym w związku z umową zawartą przez administratora z Pani/Pana pracodawcą/zleceniodawcą/podmiotem, w którym odbywasz staż/praktykę.

Kategorie danych
***art. 14 RODO**

Będziemy przetwarzać Pani/ Pana służbowe dane kontaktowe (np. imię, nazwisko adres e-mail, telefon, dane komunikatora internetowego), które niezbędne są do należytej realizacji umowy zawartej przez administratora z Twoim pracodawcą/zleceniodawcą/podmiotem, w którym odbywasz staż/praktykę.

Będziemy przetwarzać następujące kategorie Pani/Pana danych osobowych:

Źródło pochodzenia danych
***art. 14 RODO**

Pani/Pana dane osobowe pozyskane zostały:
od Pani/Pana pracodawcy/zleceniodawcy w związku z Pani/Pana udziałem w realizacji umowy zawartej przez administratora z Twoim pracodawcą/zleceniodawcą.

Okres przechowywania danych

Będziemy przechowywać Pani/Pana dane do czasu[•].
Twoje dane osobowe będą przetwarzane przez 10 lat od stycznia kolejnego roku po zakończeniu realizacji umowy administratora z Pani/Pana pracodawcą/zleceniodawcą/podmiotem, w którym odbywasz staż/praktykę.

Odbiorcy danych

Będziemy przekazywać Pani/Pana dane osobowe[•].podmiotom upoważnionym na podstawie przepisów prawa. Dodatkowo dane mogą być dostępne dla usługodawców wykonujących zadania na zlecenie administratora w ramach świadczenia usług serwisu, rozwoju i utrzymania systemów informatycznych.

Prawa związane z przetwarzaniem danych osobowych

Przysługują Pani/Panu następujące prawa związane z przetwarzaniem danych osobowych:
- prawo dostępu do Pani/Pana danych osobowych,
- prawo żądania sprostowania Pani/Pana danych osobowych,
- prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych,
- prawo do żądania usunięcia Pani/Pana danych osobowych,
- prawo do sprzeciwu wobec przetwarzania Twoich danych osobowych.

Aby skorzystać z powyższych praw, skontaktuj się z IOD (dane kontaktowe powyżej).

Inspektor Ochrony Danych

W Urzędzie wyznaczony został Inspektor Ochrony Danych – Sebastian Sobecki. Jest to osoba, z którą można się kontaktować w sprawach dotyczących przetwarzania Pani/Pana danych osobowych oraz korzystania z przysługujących Pani/Panu praw związanych z przetwarzaniem danych.

Z Inspektorem można kontaktować się w następujący sposób:
- listownie na adres: ul. G. Zapolskiej 4, 50-032 Wrocław
- przez e-mail: iod@um.wroc.pl
- telefonicznie: 71 777 77 24.

Prawo wniesienia skargi do organu

Przysługuje Pani/Panu także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.