Umowa powierzenia przetwarzania danych osobowych

(zwana dalej „Umową")

zawarta ..... roku między:

.....

- z siedzibą w ..... pod adresem: .....,
- reprezentowaną przez .....,
- zwaną dalej **„Podmiotem przetwarzającym"**

a

Prezesem Prokuratorii Generalnej Rzeczypospolitej Polskiej

- z siedzibą pod adresem: Urząd Prokuratorii Generalnej Rzeczypospolitej Polskiej, 00-682 Warszawa, ul. Hoża 76/78,
- w imieniu którego, na podstawie upoważnienia nr .../.... z .... miesiąca .... roku, działa Pan ....., ...,
- zwanym dalej **„Administratorem"**,

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 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 (ogólne rozporządzenie o ochronie danych)(Dz. Urz. UE L 119, s. 1)(zwanego w dalszej części „Rozporządzeniem"), dane osobowe do przetwarzania, na zasadach i w celu określonym w Umowie.
2. Podmiot przetwarzający zobowiązuje się nieodpłatnie przetwarzać powierzone mu dane osobowe zgodnie z Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Cel i zakres przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji zawartej między Stronami umowy nr ..... z ..... miesiąca ..... roku, której przedmiotem są usługi w zakresie utrzymania eksploatowanego przez Zamawiającego systemu finansowo-księgowego QNTemida.
2. Podmiot przetwarzający będzie przetwarzał powierzone dane osobowe zawarte w modułach systemu finansowo-księgowego QNTemida, których rodzaj oraz kategorie określają przepisy prawa. Podmiot przetwarzający będzie przetwarzał następujące dane osobowe:

.....

(kategoria i rodzaj)

.....

(kategoria i rodzaj)

§3

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności dołożenia wynikającej z zawodowego charakteru prowadzonej działalności oraz z wysokich gwarancji ochrony danych osobowych przy przetwarzaniu powierzonych danych osobowych. Szczegółowy opis technicznych i organizacyjnych środków ochrony danych osobowych wprowadzonych przez Podmiot przetwarzający znajduje się w załączniku nr 1 do Umowy.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 lit. b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym lub współpracy z Podmiotem, jak i po ustaniu łączącego ich stosunku prawnego.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem:
   1) usuwa*/ ~~zwraca~~* Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo polskie nakazują przechowywanie danych osobowych;
   2) w ciągu 30 dni przesyła Administratorowi protokół lub inny dokument potwierdzający fakt usunięcia*/~~zwrócenia~~* danych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. W przypadku stwierdzenia incydentu bezpieczeństwa, którego następstwem może być naruszenie ochrony powierzonych do przetwarzania danych osobowych Podmiot przetwarzający zgłasza go Administratorowi bez zbędnej zwłoki, nie później niż 24 h od incydentu.

§4

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy, w szczególności:
   1) Administrator lub upoważniony przez niego audytor ma prawo przeprowadzania audytów, w tym inspekcji; uprawnienie to obejmuje prawo wejścia do pomieszczeń w których przetwarzane są dane lub w których znajdują się urządzenia służące do przetwarzania danych;

2) Administrator ma prawo wglądu do rejestru kategorii czynności przetwarzania dokonywanych w jego imieniu oraz niezwłocznego otrzymania wypisu z takiego rejestru;
3) Administrator ma prawo do żądania od Podmiotu przetwarzającego niezwłocznego wykonania czynności niezbędnych do kontroli, o ile nie wymaga to szczególnego nakładu pracy; w przeciwnym przypadku Podmiot przetwarzający wykonuje te czynności w uzgodnionym przez Strony terminie.

2. Administrator przeprowadza kontrolę w uzgodnionym z Podmiotem przetwarzającym terminie oraz miejscu. W przypadku braku takich uzgodnień Administrator przeprowadza kontrolę za minimum 7-dniowym uprzedzeniem, w dni robocze, w godzinach 9:00-17:00, w siedzibie Podmiotu przetwarzającego lub miejscach przetwarzania danych.
3. Z przeprowadzonej kontroli Strony sporządzają w protokół. W przypadku stwierdzenia uchybień, w protokole zamieszcza się ich opis oraz ewentualny, ustalony termin ich usunięcia.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie ustalonym przez Strony, a w przypadku braku takiego uzgodnienia w terminie wskazanym przez Administratora, nie dłuższym niż 7 dni, chyba, że w oczywisty sposób usunięcie uchybień wymaga dłuższego terminu.
5. W przypadku zgłoszenia przez Podmiot przetwarzający incydentu bezpieczeństwa, którego następstwem może być naruszenie ochrony powierzonych do przetwarzania danych osobowych terminy, o których mowa w ust. 2 i 4 ulegają skróceniu do 1 dnia.
6. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia. Obejmuje to także obowiązek niezwłocznego poinformowania Administratora, jeżeli zdaniem Podmiotu przetwarzającego wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii Europejskiej lub polskich o ochronie danych osobowych.

§5

Podpowierzenie

1. Podmiot przetwarzający może powierzyć dane osobowe objęte Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo polskie. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy (art. 31 Rozporządzenia). Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§7

Czas obowiązywania Umowy

1. Umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania umowy, o której mowa w § 2 ust. 1.
2. Odstąpienie od umowy, o której mowa w § 2 ust. 1 wywołuje taki sam skutek prawny w stosunku do tej Umowy.

§8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Zmiana Umowy wymaga formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy będzie sąd właściwy Administratora.

....

Administrator Podmiot przetwarzający

Załącznik do Umowy

OPIS TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW OCHRONY DANYCH OSOBOWYCH WPROWADZONYCH PRZEZ PODMIOT PRZETWARZAJĄCY

(do ustalenia z podmiotem przetwarzającym)

Środki techniczne

1. Miejsce zainstalowania serwerów, na których przetwarzane są dane osobowe znajduje się na terytorium Rzeczypospolitej Polskiej / innego państwa należącego do Europejskiego Obszaru Gospodarczego.
2. Służba ochrony prowadzi całodobową, fizyczną ochronę budynku, w którym są przetwarzane dane osobowe.
3. Hol główny i teren wokół budynku, w który przetwarzane są dane osobowe jest objęty monitoringiem wizyjnym.
4. Dokumenty zawierające dane osobowe są przechowywane w szafach zamykanych na klucz.
5. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów o właściwych parametrach niszczenia.
6. Zastosowano urządzenia typu: UPS, generator prądu lub wydzielona sieć elektroenergetyczna, chroniące system teleinformatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
7. Dostęp do systemu operacyjnego komputera lub serwera, w którym przetwarzane są dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
8. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych, przetwarzanych przy użyciu systemów teleinformatycznych.
9. Zastosowano systemowe mechanizmy wymuszające na osobach przetwarzających dane osobowe okresową zmianę haseł uwierzytelniających. Dostęp do danych mają tylko wyznaczone osoby.
10. Zastosowano system rejestracji dostępu do danych osobowych.
11. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji a dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
12. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej (sprzętowy RAID .....).
13. Aktualizacja systemów operacyjnych oraz kluczowego dla przetwarzania danych osobowych oprogramowania jest dokonywana niezwłocznie po jej wydaniu przez producentów.
14. Zastosowano środki ochrony przed oprogramowaniem zawierającym wirusy komputerowe, niechcianą korespondencją (spamem) oraz złośliwym oprogramowaniem (malware) m.in. takim jak robaki, wirusy, konie trojańskie, rootkity.
15. Zastosowano rozwiązanie zapory ogniowej (firewall) do ochrony dostępu do sieci teleinformatycznej.
16. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
17. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

18. Zastosowano mechanizm automatycznej blokady dostępu do systemu teleinformatycznego służącego do przetwarzania danych osobowych w przypadku braku dłuższej aktywności użytkownika.

Środki organizacyjne

1. Wyznaczono inspektora danych osobowych, z którym można skontaktować się telefonicznie pod numerem: ....., za pomocą poczty elektronicznej pod adres e-mail: ....., korespondencyjnie pod adres: .....
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest ograniczony zasadami zarządzania dostępem do kluczy do pomieszczeń.
3. Osoby pracujące przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
4. Osoby pracujące przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie zabezpieczeń systemu teleinformatycznego w zakresie ich właściwości.
5. Osoby pracujące przy przetwarzaniu danych osobowych zostały obowiązane do zachowania ich w tajemnicy, także po ustaniu zatrudnienia lub innej podstawy prawnej współpracy.