Załącznik nr 2. Powierzenie przetwarzania danych osobowych

Definicje[1]:
Administrator danych - zgodnie z art. 4 pkt 7 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych - RODO)(zwanego w dalszej części „Rozporządzeniem" lub "RODO") pojęcie administrator danych osobowych oznacza osobę prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W tym przypadku Zamawiający.
Podmiot przetwarzający - Open Nexus, który przetwarza dane osobowe w imieniu administratora danych.
Pozostałe definicje są uregulowane w art. 4 RODO

§ 1 Powierzenie przetwarzania danych osobowych w systemie

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia, **przetwarzanie danych osobowych** na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, którym jest niniejszy załącznik (zwany dalej w niniejszym załączniku jako: "umowa") do Umowy na usługi świadczone przez Podmiot Przetwarzający (dalej jako: "Umowa główna"), chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane
4. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia oraz norm bezpieczeństwa zawartych w wymaganiach normy PN-EN ISO/IEC 27001:2017-06 dotyczących zarządzania bezpieczeństwem informacji. Spełnienie przez podmiot przetwarzający tych wymagań zostało potwierdzone certyfikatem Systemu Zarządzania Bezpieczeństwem Informacji.

§2 Opis przetwarzania - zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, na podstawie niniejszej umowy dane następujących **kategorii osób**:
    a. pracowników Administratora/Zamawiającego,
    b. wykonawców oraz osób uprawnionych do ich reprezentowania,
    c. Pracownicy Wykonawców
    d. Podwykonawcy w tym osoby umocowane do reprezentacji Podwykonawców oraz ich pracownicy
2. Kategorie przetwarzanych danych
    a. **platformazakupowa.pl**
        i. dane zwykłe imię i nazwisko,
        ii. Firma (nazwa), adres siedziby,
        iii. NIP,
        iv. stanowisko służbowe,
        v. adres poczty elektronicznej,
        vi. numer telefonu,
        vii. podpis w tym podpis wymagany przepisami prawa zamówień publicznych,
        viii. pozostałe informacje pozwalające zidentyfikować konkretną osobę fizyczną a wprowadzone przez Administratora w związku z obsługą systemów, o których mowa w art 10. RODO.

[1] Na potrzeby niniejszej umowy Strony przyjmują pozostałe definicje wynikające z art. 4 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych - RODO.

b. **przetargOS.pl**
   i. pracowników Administratora/Zamawiającego,
   ii. wykonawców oraz osób uprawnionych do ich reprezentowania,
   iii. Pracownicy Wykonawców.
c. **asystentOS.pl -** jeżeli system będzie wykorzystywany zgodnie z przeznaczeniem to nie będzie w nim danych osobowych.

3. Dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie **w celu** i zakresie koniecznym do prawidłowej realizacji zadań związanych z realizacją umowy głównej - prawidłowym działaniem systemów, wsparciem technicznym dla Administratora w celu utrzymania ciągłości działania systemów i jej niezawodności oraz archiwizacji danych.
4. **Charakter przetwarzania** - przetwarzanie danych osobowych przez Podmiot Przetwarzający będzie polegało na przeglądaniu, przesyłaniu, zapisywaniu, szyfrowaniu, przechowywaniu i usuwaniu danych osobowych zawartych w dokumentach elektronicznych.

§3 Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu danych osobowych w oparciu o niniejszą umowę, 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. Podmiot Przetwarzający informuje o nich Administratora na każde jego żądanie. **Podmiot przetwarzający stosuje przy przetwarzaniu danych osobowych techniczne i organizacyjne środki bezpieczeństwa opisane w tabeli:**

Kategoria środka techniczno-organizacyjnego	**Opis środków**
Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych	- stosowanie zabezpieczeń kryptograficznych do ochrony informacji poprzez szyfrowanie dysków komputerów, a administrator ma możliwość blokowania Pracowników z urządzeniami, które nie są szyfrowane, - opracowanie polityki dotyczącej korzystania, ochrony i okresów ważności kluczy kryptograficznych, które muszą być zmieniane raz na trzy miesiące (konieczność zmiany hasła w sejfie haseł), - dane są zaszyfrowane w ramach stosowanych przez Podmiot przetwarzający rozwiązań chmurowych, - wszędzie, gdzie jest to możliwe a w szczególności na kontach e-mail są wymuszone systemowo procedury dwuskładnikowego uwierzytelniania.
Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania	- zabezpieczenia kryptograficzne, - dwuskładnikowe uwierzytelnianie, - rozliczalność i kontrola dostępu do systemów, - zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników, - dostęp do danych jest możliwy poprzez wpisanie hasła do sejfu haseł, które dodatkowo chronione jest weryfikacją dwuetapową, - w razie awarii sprzętu pracownik w ciągu 10 minut jest w stanie rozpocząć pracę na nowym sprzęcie bez ryzyka utraty danych, - okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne, chroni się przed przechwyceniem, zakłóceniem lub uszkodzeniem ograniczając dostęp do pomieszczeń, - cykliczność wymiany sprzętu ze szczególnym uwzględnieniem potrzeb działu IT, - testy penetracyjne systemów, - nielimitowana przestrzeń na chronione w chmurze dane, - umowy z dostawcami zabezpieczające dostępność danych osobowych i związanych z tym usług, - system VPN do szyfrowania połączenia Internetowego.
Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego	- regularnie wykonywane zapasowe kopie informacji, oprogramowania i obrazów systemów zgodnie z ustaloną polityką kopii zapasowych w zakresie własnego systemu informatycznego, - zakresie pozostałych systemów, które działają w chmurze kopie zapasowe są wykonywane przez dostawców usług,

lub technicznego	- wdrożenie i udokumentowanie procesów, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.
Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania	- opracowano zasady prac nad rozwojem oprogramowania i systemów oraz stosuje się je w pracach rozwojowych prowadzonych wewnątrz organizacji, - funkcje bezpieczeństwa są testowane i dokumentowane w czasie prac rozwojowych oraz corocznych audytach prowadzonych przez firmy zewnętrzne, - podmiot przetwarzający ustanowił, dokumentuje i realizuje zasady projektowania bezpiecznych systemów oraz stosuje je do wszystkich prac implementacyjnych nad systemami informacyjnymi, - dane testowe są starannie wybierane, chronione i nadzorowane.
Środki umożliwiające identyfikację i autoryzację użytkowników	- wdrożono formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników, gdzie kluczowym system jest sejf haseł, - odwołanie upoważnienia powoduje utratę uprawnień m. in. do sejfu haseł, a administrator może zdalnie zablokować pocztę firmową i usunąć ją z urządzenia,użytkownika bez jego zgody, - opracowano polityki kontroli dostępu, która poddawana jest przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji, - użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia nadane przez Administratora, - wdrożono formalny proces rejestrowania i wyrejestrowywania użytkowników, - przydzielenie i wykorzystanie praw uprzywilejowanego dostępu ograniczono i nadzoruję się proces oraz powstała ścieżka dla odstępstw, na którą należy zdobyć zgodę, - w biurze do wejścia i wyjścia potrzebna jest karta dostępu a dostęp można odwołać w każdym momencie w sposób zdalny.
Środki zapewniające ochronę danych w czasie ich przekazywania	- wdrożono formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności, - standard API uwzględnia bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi, - informacje przekazywane w formie wiadomości elektronicznych są odpowiednio chronione poprzez weryfikację dwuetapową.
Środki zapewniające ochronę danych w czasie ich przechowywania	rozdzielenie struktury sieci na sieć firmową (tylko uprawnieni pracownicy pod kontrolą systemu antywirusowego) oraz sieć Gość (dla tych, którzy nie spełniają wymagań), -oddzielenie środowisk: rozwojowego, testowego i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami.
Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe	- budynek posiada odpowiednie zabezpieczenia wymagane przepisami (poprzednio siedziba banku), - monitoring wizyjny przy wejściu głównym oraz w ciągach komunikacyjnych, - karty dostępu dla pracowników i współpracowników rejestrujące wejścia i wyjścia do budynku, - właściciel biurowca, w którym biura ma Open Nexus zaprojektowała i stosuje fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami, - sprzęt komputerowy umieszczono i chroni się w zamkniętych strefach do których dostęp mają poprzez karty tylko uprawnione osoby, - dokumentacja wrażliwa jak np. dane osobowe pracowników przechowywana jest w zamkniętych szafach pancernych, - polityka czystego biurka oraz polityka czystego ekranu dla środków przetwarzania informacji poprzez regularne sprzątanie biura.
Środki umożliwiające rejestrowanie zdarzeń	- Podmiot przetwarzający, przechowuje i systematyzuje dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji i ochroną danych osobowych, - informacje w dziennikach chroni się przed manipulacją i nieuprawnionym dostępem (pełna historia zmian nadzorowana przez Google w zakresie zgłoszeń incydentów), - działania administratorów i operatorów systemów są rejestrowane, a dzienniki chronione i przeglądane minimum raz w roku podczasu audytu.
Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej	- system antywirusowy dla systemów Windows, który wymusza szyfrowanie urządzenia zaraz po instalacji antywirusa, - VPN dla wszystkich systemów, - wszystkie hasła przekazywane za pomocą sejfu haseł, - reszta systemów jest chmurowych (dostępnych przez przeglądarkę).

Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT	- procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych, - pozyskiwanie i ocena informacji o podatnościach technicznych wykorzystywanych, - systemów informacyjnych w celu przeciwdziałania związanemu z nimi ryzyku, - zasady instalowania oprogramowania przez użytkowników.
Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów	Podmiot przetwarzający posiada certyfikat systemu zarządzania bezpieczeństwem informacji ISO 27001:2017
Środki zapewniające minimalizację danych	- możliwość niezakładania konta profilu tam, gdzie nie jest to konieczne, co ogranicza możliwość gromadzenia jego danych, - zakładanie kont w oparciu o podstawowe dane,
Środki zapewniające odpowiednią jakość danych	-weryfikacja danych, - cykliczne usuwanie danych nieaktualnych przy każdorazowym zakładaniu lub odbieraniu uprawnień oraz coroczny przegląd zarządzania przed audytem bezpieczeństwa informacji.
Środki zapewniające ograniczone zatrzymywanie danych	- ustalenie okresów przechowywania danych w umowach powierzenia przetwarzania danych, - gwarancja możliwości usunięcia danych wykonawcy o ile przepisy na to pozwalają.
Środki zapewniające rozliczalność	- upoważnienia do przetwarzania danych osobowych dla pracowników, - wdrożono formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.
Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania	- podmiot przetwarzający zapewnia prawo do przenoszenia danych zgodnie z wytycznymi Europejskiej Rady Ochrony Danych, - usunięcia danych (nadmiarowych lub na pisemne żądanie Administratora) dokonuje dział IT.
Postępowanie dotyczące naruszeń ochrony danych	- rejestrowanie naruszeń ochrony danych i incydentów bezpieczeństwa informacji, - wdrożono procedury informowania Administratora o incydentach.

2. Podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Przetwarzający zobowiązuje się, do przetwarzania danych przekazanych przez Administratora wyłącznie na terenie Unii Europejskiej lub państw członkowskich i nie przekaże danych do państwa trzeciego lub organizacji międzynarodowej. Dotyczy to również podwykonawców wymienionych w §5 ust. 2 niniejszej umowy.
3. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
4. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które w jego imieniu będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
5. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
6. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania.
7. Podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.
8. Po zakończeniu świadczenia usług określonych umową główną, **zależnie od decyzji Administratora i postanowień umowy głównej**, Podmiot przetwarzający może:
    a. przechowywać archiwum na życzenie Zamawiającego - wówczas zastosowanie nadal znajdzie niniejszy załącznik, lub
    b. usunąć je lub
    c. zwrócić wszelkie dane osobowe Administratorowi.

W przypadku usunięcia lub zwrotu danych Podmiot przetwarzający ma obowiązek usunięcia wszelkich istniejących kopii nie później niż w ciągu 30 dni od pisemnego wezwania, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

9. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. Zgłoszenia będą dokonywane elektronicznie na podany przez Administratora adres mailowy podany w umowie głównej.
10. Podmiot Przetwarzający informuje Administratora o żądaniach osób fizycznych oraz konsultuje z nim treść i formę odpowiedzi na te żądania.
11. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych lub incydentu bezpieczeństwa informacji bez zbędnej zwłoki zgłasza je Administratorowi, nie później jednakże niż w okresie 24h od momentu stwierdzenia naruszenia ochrony danych osobowych lub incydentu bezpieczeństwa informacji.
12. Zgłoszenie, o którym mowa w ust. 11 zawiera:
    a. datę i co najmniej przybliżoną godzinę zdarzenia,
    b. datę i co najmniej przybliżoną godzinę powzięcia przez podmiot przetwarzający informacji o zdarzeniu,
    c. opis charakteru i okoliczności naruszenia,
    d. opis środków podjętych w celu usunięcia naruszenia i zapobieżenia jego skutkom.
    e. kategorie i przybliżoną liczbę wpisów (rekordów), których dotyczyło naruszenie,
    f. kategorie i przybliżoną liczbę osób, których dotyczyło naruszenie,
    g. opis potencjalnych konsekwencji i niekorzystnych skutków naruszenia dla osób, których dane dotyczą,
    h. opis środków technicznych i organizacyjnych, które zostały lub mają być zastosowane w celu złagodzenia potencjalnych niekorzystnych skutków naruszenia,
    i. imię, nazwisko i dane kontaktowe inspektora ochrony danych lub osoby, od której można uzyskać więcej informacji na temat zgłoszonego naruszenia.

§4 Prawo kontroli lub audytu

1. Administrator danych realizować będzie prawo kontroli lub audytu w godzinach pracy Podmiotu przetwarzającego. Prawo kontroli administrator realizuje samodzielnie lub korzystając z usług zewnętrznego podmiotu, o którym informuje Podmiot przetwarzający. Prawo kontroli przysługuje Administratorowi z 7-dniowym uprzedzeniem zaś tzw. kontrole ad hoc w sytuacji naruszeń wymagających zgłoszenia organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) lub powiadomienia osób fizycznych o naruszeniu ich danych jednakże przed jej przeprowadzeniem Administrator uprzedzi o niej telefoniczne lub mailowo Podmiot Przetwarzający.
2. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w rozsądnym terminie wskazanym przez Administratora danych, jeżeli uchybienia nie budzą wątpliwości Podmiotu przetwarzającego i nie przekraczają możliwości techniczno-organizacyjnych Podmiotu przetwarzającego. Wszelkie wątpliwości co do stanu faktycznego dotyczącego stwierdzonych uchybień oraz interpretacji przepisów Administrator oraz Podmiot przetwarzający wyjaśniają pisemnie lub drogą mailową aż do osiągnięcia porozumienia zakończonego pisemnym lub elektronicznym protokołem.
3. Jeżeli są niezgodności w zakresie interpretacji przepisów dotyczących wskazanych uchybień zgodnie z treścią niniejszego paragrafu i nie da się ich usunąć w drodze wyjaśnień, o których mowa w ust. 2 zdanie 2 niniejszego paragrafu Administrator danych ma prawo wypowiedzieć umowę . Wypowiedzenie wskazane w niniejszym ustępie niniejszej umowy jest tożsame z wypowiedzeniem umowy głównej i następuje w trybie natychmiastowym.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia, oraz umożliwia Administratorowi, jego imiennie upoważnionym pracownikom lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów (w tym audytów pomieszczeń), w tym inspekcji.

§5 Dalsze powierzenie danych do przetwarzania

1. Z uwagi na charakter świadczonych usług (SaaS[2]) niniejszym Administrator udziela Podmiotowi przetwarzającemu **ogólnej zgody na korzystanie z usług innych podmiotów przetwarzających** zarówno obecnych jak i przyszłych podwykonawców, np. wybór serwerowni w której składowane są dane.
2. Wykaz podwykonawców upoważnionych przez Open Nexus do dalszego przetwarzania danych osobowych w ramach realizacji niniejszej umowy:

Nazwa	**Zakres współpracy (cel powierzenia przetwarzania danych osobowych podwykonawcy)**
EXEA Sp. z o.o. ul. Włocławska 167 87-100 Toruń NIP: Sekretariat +48 56 699 54 00 biuro@exea.pl Inspektor ochrony danych iod@exea.pl	Podwykonawca EXEA udostępnia Open Nexus serwery oraz zapewnia wsparcie administracyjne na potrzeby rozwijanych przez Open Nexus usług. Spółka należąca do Toruńskiej Agencji Rozwoju Regionalnego. Exea Data Center to centrum przetwarzania danych w Polsce z certyfikacją TIER III of Constructed Facility, przyznaną po serii rygorystycznych testów infrastruktury obiektu, przeprowadzonych przez niezależną amerykańską agencję Uptime Institute. **Zgodnie z umową wszystkie dane są przechowywane w Polsce.**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany Telefon +49 (0)9831 505 0 E-Mail: info@hetzner.com Inspektor Ochrony Danych Margit Müller data-protection@hetzner.com	Współpraca z Podwykonawcą Hetzner obejmuje udostępnienie Open Nexus serwerów. Szybko rozwijająca się serwerownia dorównuje poziomem spółce OVH. **Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej.**
OVH Sp. z o.o. ul. Swobodna 1 50-088 Wrocław Telefon +48 71 750 02 00	Podwykonawca OVH udostępnia Open Nexus serwery. Jedna z największych serwerowni w Europie. Sieć pozwala na zapewnienie naszym klientom usług o najwyższej jakości. Trasa routingu jest zoptymalizowana a czas odpowiedzi jak najniższy. Sieć, której głównymi zaletami są bezpieczeństwo i gwarantowana przepustowość, jest unikalną wartością na rynku usług hostingowych w Europie. **Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej.** Pod linkiem umowa powierzenia przetwarzania danych osobowych. Pozostałe informacje nt bezpieczeństwa danych osobowych pod linkiem.
Google™ Emilii Plater 53 00-113 Warszawa Telefon: +48 22 207 19 00	Jedna z największych na świecie firm technologicznych oraz jeden ze strategicznych dostawców chmury publicznej chmurakrajowa.pl. Świadczy dla Open Nexus kilka zaawansowanych usług jak serwery, infrastruktura technologiczna, poczta firmowa, dokumenty oraz wideokonferencje oraz integrację systemOS.pl z dokumentami Google oraz backup danych (np. logi systemowe) w celu zapewnienia większego bezpieczeństwa systemu. **Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej.**
Microsoft Al. Jerozolimskie 195A 02-222 Warszawa Telefon: +48 22 594 10 00	Najbardziej znany jako producent systemów operacyjnych MS-DOS, Microsoft Windows i oprogramowania biurowego Microsoft Office. Open Nexus wykorzystuje oprogramowanie biurowe, a w przyszłości rozważa zastosowanie infrastruktury serwerowej, gdyż Spółka jest jednym z głównych strategicznych dostawców chmury publicznej w Polsce chmurakrajowa.pl. **Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej.** **Pod linkiem temat bezpieczeństwa danych i oraz prywatności Microsoft.**
VERCOM S.A. Roosevelta 22, 60-829 Poznań www.vercom.pl tel: +48 61 622 24 00 biuro@vercom.pl	Podwykonawca VERCOM SA świadczy usługi na rzecz Open Nexus w zakresie obsługi maili na potrzeby funkcjonowania systemów. Spółka technologiczna, tworząca innowacyjne rozwiązania w modelu SaaS. Laureat prestiżowego rankingu najdynamiczniej rozwijających się spółek technologicznych w Europie Deloitte Fast 50.

[2] Ma tu zastosowanie Art. 28 ust 2 (RODO) i Administrator może wyrazić sprzeciw w przypadku zmiany firmy przetwarzającej, co jest równoznaczne z możliwością rozwiązania umowy ze skutkiem natychmiastowym. Takie procedury spowodowane są tym że trudno byłoby zarządzać usługą w której obecnie ponad 3600 Klientów musi wyrazić zgodę na każdą zmianę podwykonawcy Open Nexus Sp. z o.o.. Gdyby jeden Zamawiający nie wyraził zgody to Open Nexus doszedłby do paraliżu i braku możliwości rozwijania usługi (SaaS) dla pozostałych Zamawiających.

iod@vercom.pl	**Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej** (link).
Operator Chmury Krajowej sp. z o.o., ul. Grzybowska 62, 00-844 Warszawa www.chmurakrajowa.pl Inspektor Ochrony Danych iod@ochk.pl	Chmura Krajowa jest dziś najbardziej wyspecjalizowanym dostawcą rozwiązań chmury obliczeniowej dla polskich przedsiębiorstw oraz instytucji publicznych. Jest to zaufany partner zarówno w sferze cyfrowych zabezpieczeń, procedur działania, jak i fizycznego bezpieczeństwa w centrach przetwarzania danych. Mechanizmy bezpieczeństwa są oparte na uznanych normach i najwyższych standardach: ISO 27001, ISO 22301, ISO 27017, ISO 27018 oraz CSA STAR. Chmura Krajowa powstała z inicjatywy PKO Banku Polskiego i Polskiego Funduszu Rozwoju. Partner świadczy dla Open Nexus kilka zaawansowanych usług jak przede wszystkim dostęp do zaawansowanego środowiska Google Cloud Platform i dedykowanych prywatnych zasobów chmurowych (IaaC, IaaS, SaaC) którego zasoby zabezpieczone zgodnie z najwyższymi standardami security przez Google. **Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej.**
Tenesys Sp. z o.o. u;. Wroniecka 18/5 61-763 Poznań, tel.: +48 61 6661140 email: contracts@tenesys.pl	Podwykonawca Tenesys Sp. z o.o. wspiera nasz zespół w utrzymaniu usług administracyjnych (DevOps) i jest wsparciem dla naszego zespołu IT, aby dbać o bezpieczeństwo rozwijanych przez nas systemów. Tenesys cieszy się nienaganną reputacją jako solidny i godny zaufania partner, wspierający przedsiębiorstwa w kraju i za granicą i poprzez swoje kompetencje pomaga openNexus w przyspieszaniu innowacji i poprawie wydajności naszych systemów.
Umbrella Limited Sp. z o.o. Ul. Tęczowa 19A 60-275 Poznań E-mail: contact@umbrella.limited Telefon: +48 789 249 446	Umbrella Limited to doświadczony software house świadczący usługi programistyczne. Współpraca z Umbrella Limited obejmuje usługi IT w zakresie tworzenia narzędzia AsystentOS, sprofilowanego w całości pod wymagania Open Nexus. AsystentOS w całości postawiony jest na serwerach Google. Zgodnie z umową wszystkie dane są przechowywane na terenie Unii Europejskiej. Podwykonawca dba o każdy detal realizowanych zleceń, a nad AsystentOS ze strony Umbrella Limited pracują kluczowi w firmie eksperci.
SFDC Ireland Limited 3rd and 4th FL, No 1 Central Park (Block G) Central Park, Leopardstown Dublin 18 Ireland	Światowy lider wśród rozwiązań CRM (customer relationship management). Salesforce to platforma oferująca rozwiązania dla zarządzania relacjami z klientem oraz wielokanałową obsługą zgłoszeń i reklamacji.
Web To Learn sp. z o.o. ul. Przemysława 3 83-400 KOŚCIERZYNA https://webtolearn.pl/kontakt/ Inspektor ochrony danych: pomoc@webtolearn.pl	Podwykonawca zapewniający prowadzenie webinarów, spotkań i lekcje online. Pozwala na zapewnienie naszym klientom usług edukacyjnych o najwyższej jakości.
UiPath SRL, 4 Vasile Alecsandri Street, 11 Daniel Constantin Street, 5th floor, building A, district 1, Bucharest, Romania	UiPath to globalna firma zajmująca się oprogramowaniem do automatyzacji procesów zrobotyzowanych, założona w Bukareszcie w Rumunii, działająca m.in na terenie Unii Europejskiej. Zgodnie z polityką prywatności wszystkie dane są przechowywane na terenie Unii Europejskiej (link)

3. Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym możliwość wyrażenia sprzeciwu wobec takich zmian w ciągu 7 dni od daty otrzymania informacji.
4. W przypadku wyrażenia sprzeciwu przez Administratora i braku zmiany decyzji Podmiotu przetwarzającego umowa niniejsza oraz Umowa główna może zostać rozwiązana przez Administratora lub Podmiot przetwarzający **w terminach określonych w przypadku wypowiedzenia umowy głównej**. Brak sprzeciwu w terminie, o którym mowa w ust. 3 oznacza akceptację zmian przez Zamawiającego.
5. Podmiot przetwarzający będzie przestrzegał warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 1, 2 i 4 RODO. Podmiot przetwarzający jest zobowiązany do przekazania Administratorowi, na każde jego żądanie, listy osób i podmiotów

zewnętrznych upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy.
6. Podmiot przetwarzający gwarantuje, że osoby upoważnione do przetwarzania danych osobowych będą zobowiązane do zachowania ciągłej tajemnicy na podstawie umowy lub będą podlegały podobnemu obowiązkowi wynikającemu z mocy prawa.
7. 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 danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych 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 Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
3. Podmiot przetwarzający ponosi odpowiedzialność odszkodowawczą wobec osób fizycznych na zasadach określonych w art. 82 RODO.
4. Pozostałe zakresy odpowiedzialności reguluje umowa główna oraz przepisy prawa powszechnie obowiązującego.

§7 Czas obowiązywania umowy

1. Niniejsza umowa zostaje zawarta na czas obowiązywania umowy głównej na usługi Open Nexus.
2. Strony są uprawnione do rozwiązania niniejszej umowy w trybie natychmiastowym w przypadku gdy:
    a) podmiot przetwarzający nie stosuje się do wiążących (ostatecznych, prawomocnych) decyzji i orzeczeń właściwych organów lub sądów,
    b) podmiot przetwarzający poinformował Administratora, że jego polecenie narusza przepisy prawa a Administrator mimo to nalega na wykonanie tego polecenia, lub w dalszym ciągu narusza wskazane przez podmiot przetwarzający przepisy prawa.
3. Rozwiązanie niniejszej umowy jest jednoznaczne z rozwiązaniem Umowy głównej.
4. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
5. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.