Kwestionariusz Oceny Podwykonawcy

W związku z przetwarzaniem danych osobowych.

Mając na uwadze prawidłowe spełnienie przez Administratora Danych wymogów 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, zwane dalej RODO), w szczególności art. 28 dotyczącego Podmiotów Przetwarzających przedstawiamy Państwu niniejszy kwestionariusz samooceny w celu weryfikacji stopnia spełnienia przez Państwa, jako podmiotu przetwarzającego stopień spełnia wymogów RODO oraz prawidłowego zabezpieczenia przetwarzanych na rzecz nas danych osobowych.

0. Instrukcja wypełnienia kwestionariusza oceny

Szanowni Państwo,

Prosimy o sumienne wypełnienie niniejszego arkusza. Po jego uzupełnieniu prosimy o przesłanie do wskazanej osoby wypełniony arkusz w formie elektronicznej, oraz wydrukowany i podpisany zgodnie z Państwa reprezentacją.

Przedstawiony kwestionariusz sanowi potwierdzenie realizacji przez Państwa stopnia spełnienia wymagań RODO oraz zabezpieczenia systemów informatycznych służących do przetwarzania dnaych osobowych.

Mając na uwadze ewentualne Państwa pytania dotyczące sposobu wypełniania ankiety prosimy o zapoznanie się z niniejszymi uwagami.

1. Za Administratora Danych uważa się Zleceniodawcę, podmiot przekazujący kwestionariusz do oceny.
2. Niniejszy kwestionariusz oceny jest przeznaczony dla podmiotów którym Administrator Danych powierza lub ma zamiar powierzyć przetwarzanie danych osobowych. Mając na uwadze uniwersalność kwestionariusza mogą występować obszary możliwe do wyłączenia.
3. Odpowiadając na pytania niniejszego kwestionariusza należny brać pod uwagę kontekst działalności oaz zakres współpracy z Administratorem Danych.
4. Odpowiadając na poniższe pytania należy brać pod uwagę wyłącznie te procesy, działania czy systemy które służą lub mają wpływ na realizację umowy lub inne współpracy na rzecz Administratora Danych. W stosunku do systemów informatycznych należy ocenić również inne systemy wspomagające które mogą wpływać na proces przetwarzania danych Zleceniodawcy lub zabezpieczenia powierzonych przez niego danych.
5. Zakąłdamy, że dla prawidłowego wypełnienia arkusza (np. w obszarze teleinformatycznym) może być niezbędne zaczerpnięcie wiedzy osób zajmujących się nadzorowaniem badanych obszarów.
6. W przypadku udzielenia odpowiedzi “NIE DOTCZY” prosimy o dokonanie uzasadnienia (opis lub wybór z listy).
7. W sytuacji, jeżeli chcieli by Państwo (była by potrzeba) odniesienia sie do któregoś z punktów kwestionariusza, prosimy o skorzystanie z arkusza UWAGI. Dopisując informacje w polu Uwagi prosimy o odniesienie się do konkretnego punktu kwestionariusza.

Zapoznałem się z instrukcją wypełnienia kwestionariusza ☐ Tak ☐ Nie

Autor kwestionariusza: N-Serwis.pl Sp. z o.o. [www.n-serwis.pl]
wersja kwestionariusza: 1.0

Kwestionariusz Oceny Podwykonawcy

W związku z przetwarzaniem danych osobowych.

1.	Dane podmiotu przetwarzającego				
1.1	Nazwa Firmy				
1.2	Adres				
1.3	Kod pocztowy, Miasto				
1.4	Strona internetowa				
1.5	Liczba pracowników	Samozatrudnienie			
1.6	Liczba podwykonawców	Brak			
1.7	Zakres powierzenia danych we współpracy z Administratorem Danych	1.Księgowość/ kadry ☐ Dotyczy	2.IT/ aplikacje/ serwis systemów ☐ Dotyczy	3. Usługi prawne/ Inne specjalistyczne ☐ Dotyczy	4. Inne Proszę opisać
1.8	Osoba wypełniająca				
1.9	Telefon i email osoby wypełniającej				

2.	Profil działalności podmiotu przetwarzającego I współpracy
2.1	Zakres działalności i zakres współpracy z Administratorem Danych
2.2	Data i numer umowy z Administratorem Danych
2.3	Okres współpracy z Administratorem Danych (całościowo w latach)

3.	Systemy informatyczne służace do przetwarzania danych osobowych Administratora Danych			
3.1	Podsumowanie ilość:	Upoważnionych użytkowników systemu informatycznego Brak	Ilosć wykorzystywanych systemów Brak	Ilość systemów poza zasobami procesora Brak

3.2 Proszę wymienić systemy oraz wskazać ich parametry

	Nazwa systemu	Lokalizacja (w siedzibie/hostowany)	Technologia bazy danych
3.2.1		Instalacja w siedzibie firmy	Relacyjna Baza SQL
3.2.2		Instalacja w siedzibie firmy	Relacyjna Baza SQL

3.2.3			

4.	Stosowane zabezpieczenia	
4.1	**Polityka Bezpieczeństwa i zarządzanie bezpieczeństwem**	
4.1.1	Polityka Bezpieczeństwa jest w firmie sformalizowanym, zatwierdzonym przez jej władze zespołem norm i zasad bezpieczeństwa, stworzonym i zakomunikowanym wszystkim pracownikom.	☐ Tak ☐ Nie
4.1.2	Firma przeprowadza regularne szkolenia z zakresu Polityk Bezpieczeństwa dla osób upoważnionych obejmujące aktualne zagrożenia dla systemów informatycznych.	☐ Tak ☐ Nie
4.1.3	Firma identyfikuje zagrożenia dla systemów informatycznych i wdraża adekwatne rozwiązania mające na celu zmniejszenie szkodliwości zagrożeń.	☐ Tak ☐ Nie
4.1.4	Firma regularnie przeprowadza weryfikację Polityk Bezpieczeństwa i je aktualizuje.	☐ Tak ☐ Nie
4.1.5	Firma rozpoznaje i klasyfikuje zasoby informacyjne i systemy informatyczne, zgodnie z ich wrażliwością i wymaganiami dotyczącymi przetwarzanych przez nie danych.	☐ Tak ☐ Nie
4.1.6	Pracownicy mający dostęp do danych osobowych są przeszkoleni w zakresie wymagań ochrony danych osobowych i ich przetwarzania.	☐ Tak ☐ Nie
4.1.7	Został wyznaczony administrator bezpieczeństwa informacji, inspektor ochorny danych (ABI/ IOD) i realizuje swoje zadania.	☐ Tak ☐ Nie
4.1.8	Pracownicy podpisują umowę o poufności lub klauzlę poufności przed rozpoczęciem pracy na danych osobowych.	☐ Tak ☐ Nie
4.1.9	W ciągu dwóch ostatnich lat polityka ochrony danych osobowych podlegała kontroli przez zewnętrznego audytora.	☐ Tak ☐ Nie
4.1.10	Firma posiada kontrole nad systemami informatycznymi (w szczególności w przypadku outsourcingu usług IT) i jest w stanie utrzymać ciągłość działania systemów na podstawie posiadanych haseł i konfiguracji.	☐ Tak ☐ Nie

4.2	**Ochrona systemu informatycznego**	TAK
4.2.1	Dostęp do systemów informatycznych mają tylko zarejestrowani użytkownicy posiadający swój login i hasło, które trzeba okresowo zmieniać.	☐ Tak ☐ Nie
4.2.2	Udzielenie dostępu do systemów informatycznych jest oparte na regułach najmniejszego uprzywilejowania i jest zatwierdzane przez kierownictwo.	☐ Tak ☐ Nie
4.2.3	Zostały wdrożone zabezpieczenia stanowisk komputerowych, laptopów, komputerów i urządzeń mobilnych przed nieuprawnionym dostępem do danych.	☐ Tak ☐ Nie
4.2.4	W firmie stosuje się system centralnego zarządzania i monitorowania systemów informatycznych.	☐ Tak ☐ Nie
4.2.5	Wszystkie stanowiska komputerowe są chronione zaporą sieciową (firewall).	☐ Tak ☐ Nie
4.2.6	Wszystkie stanowiska komputerowe są chronione oprogramowaniem antywirusowym. Aktualizacje oprogramowania antywirusowego są odbywają się w sposób automatyczny.	☐ Tak ☐ Nie
4.2.7	Oprogramowanie (inne stosowane) związane z bezpieczeństwem teleinformatycznym jest regularnie aktualizowane.	☐ Tak ☐ Nie
4.2.8	Jest wdrożony i regularnie aktualizowany plan odzyskiwania danych w razie awarii. Kopie zapasowe są wykonywane w określonych odstępach czasu i przechowywane w sposób gwarantujący ich bezpieczeństwo.	☐ Tak ☐ Nie
4.2.9	Sprzęt komputerowy jest okresowo konserwowany w celu zapewnienia ciągłości pracy.	☐ Tak ☐ Nie

4.2.10	W ostatnich dwóch latach zaistniała konieczność odzyskiwania danych z kopii zapasowych.	☐ Tak ☐ Nie
4.2.11	Wszystkie domyślne hasła i konfiguracje do systemów, usług i urządzeń są zmieniane przed ich wdrożeniem.	☐ Tak ☐ Nie

4.3	**Kontrola ochrony danych osobowych**	TAK
4.3.1	Dostęp do danych osobowych jest zastrzeżony tylko dla tych pracowników, którzy potrzebują dostępu do wykonywania swoich zadań, ponadto przydzielanie dostępu podlega regularnej kontroli.	☐ Tak ☐ Nie
4.3.2	Dane osobowe w formie elektronicznej, są szyfrowane podczas ich przetwarzania poza systemami informatycznymi oraz szyfruje się przetwarzane kopie zapasowe.	☐ Tak ☐ Nie
4.3.3	Dane osobowe są szyfrowane w trakcie przesyłania przez sieć publiczną (internet).	☐ Tak ☐ Nie
4.3.4	Telefony komórkowe, tablety (urządzenia mobilne) i twarde dyski laptopów, służące do przetwarzania danych osobowych są szyfrowane.	☐ Tak ☐ Nie
4.3.5	Technicznie ograniczone jest kopiowanie danych osobowych na dyski przenośne i wysyłanie ich przez niezaszyfrowane maile.	☐ Tak ☐ Nie
4.3.6	Użytkownicy nie posiadają uprawnień umożliwiających im instalację oprogramowania.	☐ Tak ☐ Nie
4.3.7	Stosuje się monitorowanie dostępu do danych, sposoby pracy (użycia) danych osobowych i systemów (tzw. aktywne monitorowanie pracowników).	☐ Tak ☐ Nie
4.3.8	Stosuje sie narzędzia klasy DLP w celu ochrony danych osobowych.	☐ Tak ☐ Nie

4.4	**Bezpieczeństwo sieciowe i operacyjne**	TAK
4.4.1	Istnieje system blokowania treści w sieci wewnętrznej i Internecie, system jest regularnie aktualizowany i monitorowany.	☐ Tak ☐ Nie
4.4.2	System wykrywania/zapobiegania wirusom oraz włamaniom (IPS/IDS) jest wdrożony oraz regularnie aktualizowany i monitorowany.	☐ Tak ☐ Nie
4.4.3	Użytkownicy systemów mają dostęp do Internetu za pomocą urządzeń sieciowych (proxy), wyposażonych w oprogramowanie antywirusowe i system filtrowania stron internetowych. Filtrowaniu podlega również ruch szyfrowany protokołem SSL.	☐ Tak ☐ Nie
4.4.4	System informatyczny jest podzielony (np. VLAN) na obszary szczególnie wrażliwe (serwery, usługi publiczne), zwykłe obszary (zakres działalności użytkownika) oraz dostęp zdalny (VPN).	☐ Tak ☐ Nie
4.4.5	Zagrożenia bezpieczeństwa (zarażenie wirusem, próby uzyskania dostępu) są regularnie rejestrowane i aktywnie monitorowane.	☐ Tak ☐ Nie
4.4.6	Stosuje się dodatkowe zaawansowane zabezpieczenia sieci takie jak np. Aplication Web Filtering, Sand Box i inne.	☐ Tak ☐ Nie
4.4.7	Sieci WiFi są zabezpieczone silnym hasłem z wykorzystaniem co najmniej protokołu WPA2.	☐ Tak ☐ Nie
4.4.8	Sieci dla gości są wyizolowane i dają pełną gwarancję zachowania poufności danych przetwarzanych w sieci firmowej.	☐ Tak ☐ Nie
4.4.9	Stosuje sie serwery syslog korelujące dzienniki zdarzeń z różnych elementów infrastruktury (minimum: routery, sprzęt sieciowy, logi systemów operacyjnych, serwerów).	☐ Tak ☐ Nie

4.5	**Fizyczne bezpieczeństwo serwerownii i infrastruktury krytycznej**	TAK
4.5.1	Krytyczne systemy są umieszczone w co najmniej jednym przeznaczonym do tego pomieszczeniu z ograniczonym dostępem, wyposażonym w alarm i monitoring (tzw. serwerownia).	☐ Tak ☐ Nie

4.5.2	Systemy informatyczne (serwery) mają sprawny system bezpieczeństwa (awaryjne zasilanie, klimatyzacja, połączenie sieciowe).	☐ Tak ☐ Nie
4.5.3	Stosuje się klaster w celu zabezpieczenia infrastruktury sprzętowej. Ewentualnie całościowa kopia zapasowa przechowywana jest w oddzielnej lokalizacji.	☐ Tak ☐ Nie
4.5.4	W lokalizacjach o krytycznym znaczeniu zainstalowane są systemy wykrywania ognia i gaszenia pożaru.	☐ Tak ☐ Nie
4.5.5	System awaryjnego zasilania jest zabezpieczony akumulatorami, które są regularnie konserwowane.	☐ Tak ☐ Nie
4.5.6	Stosuje się aktywne systemy monitorowania parametrów środowiskowych i ich wpływu na infrastrukturę krytyczną.	☐ Tak ☐ Nie

4.6	**Fizyczne bezpieczeństwo danych osobowych**	TAK
4.6.1	Dostęp do danych osobowych (lub ich nośników) ograniczony jest wyłącznie dla upoważnionych pracowników i wyłącznie w granicach posiadanego upoważnienia.	☐ Tak ☐ Nie
4.6.2	Dane osobowe w formie papierowej znajdują się w zamykanych pomieszczeniach bez dostępu osób nieupoważnionych.	☐ Tak ☐ Nie
4.6.3	Dane osobowe w formie papierowej po godzinach pracy znajdują się w zamykanych szafach bez dostępu osób nieupoważnionych.	☐ Tak ☐ Nie
4.6.4	Stosuje się politykę „czystego biurka”.	☐ Tak ☐ Nie
4.6.5	Dostęp do pomieszczeń po godzinach pracy nie jest możliwy dla osób postronnych (sprzątanie, ochrona), lub jest szczegółowo nadzorowany.	☐ Tak ☐ Nie
4.6.6	Błędne lub zbędne wydruki niszczone są w sposób mechaniczny (np. przy użyciu niszczarek).	☐ Tak ☐ Nie
4.6.7	Wycofywane, uszkodzone nośniki danych (np. dyski, pen-drive) niszczone są w sposób gwarantujący trwałe uszkodzenie zapisanych na nich informacji.	☐ Tak ☐ Nie
4.6.8	Fizyczny dostęp do systemów informatycznych (np. komputerów, drukarek, laptopów, urządzeń mobilnych) jest ograniczony wyłącznie dla osób upoważnionych.	☐ Tak ☐ Nie
4.6.9	Systemy informatyczne dają gwarancję integralności zasobów (ochronę przed nieuprawnionym otwarciem, klonowaniem dysków).	☐ Tak ☐ Nie
4.6.10	Systemy informatyczne są zabezpieczone przed kradzieżą.	☐ Tak ☐ Nie
4.6.11	Systemy informatyczne rozlokowane są w taki sposób aby organicznych dostęp oraz wgląd do danych przez osoby nieupoważnione.	☐ Tak ☐ Nie
4.6.12	Stosuje się zabezpieczenia sprzętu poza siedzibą firmy.	☐ Tak ☐ Nie

5.	**Podpowierzenie wykonania usług na rzecz Administratora Dancyh podmiotom zewnętrznym**	
	[Proszę wypełnić, jeżeli przetwarzanie danych osobowych jest zlecane podmiotom zewnętrznym]	TAK
5.1	Umowa outsourcingowa zawiera wymogi bezpieczeństwa wymagane dla umów zawieranych z usługodawcą (zapisy umowne).	☐ Tak ☐ Nie
5.2	Istnieje lista podmiotów którym powierza się dane osobowe Administratora Danych.	☐ Tak ☐ Nie
5.4	Dostęp pod-procesora do danych osobowych Administratora jest ograniczony i nadzorowany.	☐ Tak ☐ Nie
5.5	Pod-procesor nie może wykonać kopii danych osobowych Administratora (poprzez zastosowanie zabezpieczeń technicznych).	☐ Tak ☐ Nie

5.6	**Wykonywanie których zadań zostało zlecone podmiotom zewnętrznym?**		**Wykonawca usług**
5.6.1	Zarządzanie serwerami, siecią, komputerami, bezpieczeństwem.	☐ Tak ☐ Nie	
5.6.2	Zarządzanie danymi (w tym serwis) w systemach i aplikacjach.	☐ Tak ☐ Nie	
5.6.3	Korzystanie z chmury obliczeniowej.	☐ Tak ☐ Nie	
5.6.4	Serwis księgowy/kadrowy.	☐ Tak ☐ Nie	
5.6.5	Serwis prawny.	☐ Tak ☐ Nie	
5.6.6	Kolokacja danych osobowych (serwery, archiwa).	☐ Tak ☐ Nie	
5.6.7	Inne (jakie?).	☐ Tak ☐ Nie	

6.	**Incydenty dotyczące bezpieczeństwa danych**	
6.1	Zagrożenia bezpieczeństwa danych osobowych (niezależnie od jej formy) są regularnie rejestrowane i aktywnie monitorowane.	☐ Tak ☐ Nie
6.2	Jest opracowany plan działania w razie wystąpienia incydentu, naruszenia bezpieczeństwa danych osobowych.	☐ Tak ☐ Nie
6.3	Informacje dotyczące naruszeń są brane pod uwagę w ocenie ryzyka prowadzonego przez Administratora Danych.	☐ Tak ☐ Nie
6.4	W stosunku do przetwarzanych danych osobowych, stosuje się (i regularnie testuje) plany ciągłości działania.	☐ Tak ☐ Nie
6.5	Czy zgłoszone zostały jakiekolwiek roszczenia wynikające z naruszenia prywatności, utraty lub kradzieży informacji osobistych lub handlowych lub nieuprawnionego dostępu do sieci komputerowej ?	☐ Tak ☐ Nie
6.6	Czy organ nadzorczy lub autoryzowany organ branżowy) przeprowadzili kiedykolwiek dochodzenie w zakresie danych osobowych lub żądali podania informacji w tym zakresie?	☐ Tak ☐ Nie
6.7	Czy firma była celem ukierunkowanego ataku na system komputerowy?	☐ Tak ☐ Nie
6.8	Czy kiedykolwiek otrzymano skargę od klienta, pracownika lub dostawcy usługi odnośnie ich danych osobowych (lub firmy)?	☐ Tak ☐ Nie
[Jeśli na któreś z powyższych pytań 6.5-6.8 została udzielona odpowiedź „TAK", prosimy o podanie szczegółów]		

6.9	Czy w ostatnim roku zaistniała konieczność odzyskiwania danych z kopii ?	☐ Tak ☐ Nie
6.10	Czy w ostatnim roku wystąpił incydent związany z ochroną danych lub bezpieczeństwem systemów (np. ramsomware) ?	☐ Tak ☐ Nie

7. Deklaracja

Niniejszym oświadczam(y), że wszystkie informacje podane we wniosku są prawdziwe i że żadne fakty nie zostały pominięte bądź zmienione. Zgadzam(y) się, że niniejszy formularz wraz z innymi dostarczonymi informacjami powinien stanowić podstawę kontroli podmiotu przetwarzającego przez Administratora Danych oraz że w wyniku udzielonych odpowiedzi Administrator Danych może dochodzić dodatkowych wyjaśnień lub dodatkowego sprawdzenia.

Nazwa firmy	Stanowisko
Data	Podpis osoby upoważnionej

Dodatkowe uwagi / wyjaśnienia (proszę podać numer punktu wyjaśnianego)