Załącznik nr 3
do zapytania ofertowego DSI-I.1333.18.2022

UMOWA NR ……
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zwana dalej „Umową powierzenia”
zawarta w dniu ..... r. w Białymstoku pomiędzy:
Województwem Podlaskim, zwanym w treści umowy powierzenia **Administratorem**, w imieniu którego działa Zarząd Województwa Podlaskiego z siedzibą w Białymstoku przy ul. Kardynała Stefana Wyszyńskiego 1, 15-888 Białystok, reprezentowany przez:

1. ……
2. ……

a

……
zwanym/zwaną dalej „**Podmiotem przetwarzającym**”, reprezentowanym/reprezentowaną przez:

1. ……
2. ……

zwanymi następnie łącznie „Stronami”, o następującej treści:

§ 1
Podstawa prawna

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 osobowych), zwane dalej RODO.

§ 2
Powierzenie do przetwarzania danych osobowych

1. Na podstawie art. 28 RODO Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wyłącznie w celu wykonania zobowiązań w zakresie realizacji zadań wynikających z umowy …….
2. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w ramach procesu/ów z Rejestru Czynności Przetwarzania:

a) 110 Administrowanie systemami i aplikacjami dziedzinowymi SI UMWP

3. Przetwarzanie danych osobowych w procesie/ach, o których mowa w ust. 2 jest zgodne z prawem i spełnia warunki art. 6 ust. 1 lit. c) RODO.

4. Niniejsza umowa stanowi udokumentowane polecenie administratora, zgodnie z art. 29 RODO.

§ 3

Oświadczenia stron

1. Administrator oświadcza, iż jest w rozumieniu art. 4 pkt. 7 RODO Administratorem Danych Osobowych powierzanych do przetwarzania w ramach niniejszej umowy i przetwarza je na podstawie:

   a) procesu 110 Administrowanie systemami i aplikacjami dziedzinowymi SI UMWP - na podstawie prawnej zawartej w art.. 6 ust 1 RODO lit. c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   b) dla kategorii wyszczególnionych w załączniku nr 3.1 punkt 2 Administrator oświadcza, iż jest Podmiotem przetwarzającym.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, rozporządzeniem RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa i wolność osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza też, iż dysponuje odpowiednimi środkami technicznymi i organizacyjnymi, doświadczeniem, wiedzą i wykwalifikowanym personelem, umożliwiającymi mu prawidłowe wykonanie niniejszej Umowy powierzenia,
4. Podmiot przetwarzający na potwierdzenie gwarancji ochrony praw osób, których dane dotyczą, zgodnie z wymogiem art. 28 ust. 1 RODO, przekazał Administratorowi opis wdrożonych mechanizmów zapewniających bezpieczeństwo przetwarzania danych osobowych, stanowiący *załącznik nr 2* do niniejszej Umowy powierzenia.
5. Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora o których mowa w art. 30 ust. 2 RODO.

§ 4

Cel przetwarzania, kategorie danych osobowych oraz kategorie osób, których dane dotyczą

1. Kategorie danych osobowych, w zakresie niezbędnym do realizacji Umowy, o której mowa w § 2 ust. 1, oraz kategorie osób, których dane dotyczą powierzone Podmiotowi przetwarzającemu do przetwarzania zostały określone w *załączniku nr 1* do niniejszej umowy powierzenia.

2. Przetwarzanie danych osobowych odbywa się przy wykorzystaniu systemu informatycznego.

3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu aktualizacji i wsparcia na posiadany przez Zamawiającego System Barracuda Email Security Gateway model V 400 (400VX).

§ 5

Zasady przetwarzania danych przez Podmiot przetwarzający

1. Podmiot przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w niniejszej Umowie powierzenia.
2. Przekazanie powierzonych danych do państwa trzeciego (poza EOG) może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakładają na Podmiot przetwarzający przepisy prawa, któremu podlega Podmiot przetwarzający. 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. Podmiot przetwarzający oświadcza, iż przetwarzanie powierzonych mu danych będzie zgodne z wymaganiami określonymi w RODO, wdrożył odpowiednie środki techniczne i organizacyjne odpowiadające wymogom RODO, w tym wszelkie środki, o których mowa w art. 32 RODO, a przede wszystkim zabezpieczył dane przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
4. Podmiot przetwarzający, ponadto:
   a) w zakresie charakteru przetwarzania, współpracuje z Administratorem poprzez stosowanie odpowiednich środków technicznych i organizacyjnych w zakresie wywiązywania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w części wykonywania jej praw określonych w rozdziale III RODO;
   b) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
5. Podmiot przetwarzający zobowiązuje się odpowiedzieć niezwłocznie na każde pytanie Administratora dotyczące powierzonych mu do przetwarzania, na podstawie niniejszej Umowy powierzenia, danych osobowych oraz udostępnia wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.
6. Dostęp do powierzonych Podmiotowi przetwarzającemu danych osobowych mogą posiadać tylko osoby upoważnione przez Podmiot przetwarzający, zgodnie z jego wewnętrznymi procedurami. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania tajemnicy, o której mowa w art. 28 ust. 3 pkt b RODO, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
7. Podmiot przetwarzający zobowiązuje się niezwłocznie, jednak nie później niż w ciągu 7 dni od powzięcia informacji, zawiadomić Administratora o:
   a) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa;
   b) każdym żądaniu otrzymanym od osoby, której dane zostały powierzone mu do przetwarzania, powstrzymując się jednocześnie od odpowiedzi na żądanie;
   c) każdym postępowaniu, decyzji lub orzeczeniu dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych, które zostały mu powierzone do przetwarzania na podstawie niniejszej Umowy powierzenia;

d) każdej planowanej inspekcji, kontroli lub audytowi dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych, które zostały mu powierzone do przetwarzania na podstawie niniejszej Umowy powierzenia.

8. Planując dokonanie zmian w sposobie przetwarzania danych osobowych, Podmiot przetwarzający ma obowiązek zastosować się do wymogów, o których mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminie, który zapewni Administratorowi realną możliwość reagowania, jeżeli planowane przez Podmiot przetwarzający zmiany w opinii Administratora zagrażają uzgodnionemu poziomowi bezpieczeństwa powierzonych do przetwarzania danych osobowych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek ich przetwarzania przez Podmiot przetwarzający.

9. Podmiot przetwarzający w przypadku podejrzenia incydentu lub zaistnienia naruszenia ochrony danych osobowych:
   a) informuje Administratora bez zbędnej zwłoki, o podejrzeniu i/lub stwierdzeniu naruszenia ochrony danych osobowych, nie później niż w ciągu 24 godzin od powzięcia takiej informacji, w formie zgodnej z załącznikiem nr 3 do niniejszej Umowy powierzenia;

   b) współpracuje przy ocenie naruszenia i ewentualnym zawiadomieniu o tym organu nadzorczego i osób, których dane dotyczą;
   c) przekazuje informacje niezbędne Administratorowi do przeprowadzenia oceny skutków dla ochrony danych oraz przeprowadzania uprzednich konsultacji z organem nadzorczym i wdrożenia zaleceń organu;
   d) umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających;
   e) przekazując informację o stwierdzeniu naruszenia, przesyła również wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.
10. W przypadku, gdy Podmiot przetwarzający będzie pozyskiwał dane w imieniu Administratora, jego obowiązkiem jest również realizacja obowiązku informacyjnego, o którym mowa w art. 13 i art. 14 RODO.
11. Podmiot przetwarzający, z chwilą wygaśnięcia niniejszej umowy, zobowiązuje się zwrócić wszelkie dane osobowe, których przetwarzanie zostało mu powierzone oraz skutecznie usunąć wszelkie ich istniejące kopie, również z nośników elektronicznych pozostających w jego dyspozycji, chyba że przepisy prawa nakazują mu przechowywanie danych osobowych. Podmiot przetwarzający zrealizuje niniejsze czynności o których mowa oraz przedstawi Administratorowi oświadczenie potwierdzające ich realizację, w terminie nie dłuższym niż 5 dni od wygaśnięcia lub rozwiązania niniejszej umowy.
12. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z umową powierzenia, a w szczególności za udostępnienie osobom nieupoważnionym.
13. W przypadku naruszenia przepisów niniejszej Umowy powierzenia lub RODO z przyczyn leżących po stronie Podmiotu przetwarzającego, w następstwie czego Administrator zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany,

Podmiot przetwarzający zobowiązuje się pokryć Administratorowi poniesione z tego tytułu straty.

§ 6

Korzystanie z usług innego podmiotu przetwarzającego przez podmiot przetwarzający

1. Podmiot przetwarzający, do wykonania w imieniu Administratora konkretnych czynności przetwarzania związanych z realizacją umowy, o której mowa w § 2 ust. 1, może korzystać z usług innego podmiotu przetwarzającego, pod warunkiem, że:
   a) inny podmiot przetwarzający zapewnienia, podobnie jak Podmiot przetwarzający, wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO;
   b) Podmiot przetwarzający dokona tego w drodze pisemnej umowy przy zachowaniu co najmniej tych samych obowiązków ochrony danych, jak w niniejszej Umowie powierzenia oraz na czas nie dłuższy niż czas obowiązywania niniejszej Umowy powierzenia;
   c) Podmiot przetwarzający poinformuje Administratora o zamiarze korzystania z usług innego podmiotu przetwarzającego, wraz z informacją o tym podmiocie i zastosowanych w tym podmiocie zabezpieczeniach zapewniających odpowiedni stopień bezpieczeństwa, który odpowiadał będzie ryzyku związanemu z powierzeniem danych osobowych, z którego usług zamierza korzystać dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec korzystania z usług tego innego podmiotu przetwarzającego.
2. Administrator może w terminie 14 dni, licząc od dnia przekazania informacji, wyrazić sprzeciw wobec korzystania z usług wskazanego podmiotu.
3. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków innego podmiotu przetwarzającego spoczywa na Podmiocie przetwarzającym.

§ 7

Kontrole

1. Administrator, zgodnie z art. 28 ust. 3 lit. h) RODO, ma prawo do kontroli sposobu wykonywania niniejszej Umowy powierzenia poprzez przeprowadzenie, zapowiedzianych na 7 dni kalendarzowych wcześniej, kontroli dotyczących przetwarzania powierzonych danych osobowych przez Podmiot przetwarzający bądź podmiot, z którego usług korzysta Podmiot przetwarzający oraz żądania składania przez podmioty kontrolowane pisemnych wyjaśnień.
2. Osoby wykonujące czynności kontrolne złożą oświadczenie o zachowaniu poufności w zakresie stosowanych przez Podmiot przetwarzający technicznych i organizacyjnych środków ochrony danych osobowych, w myśl którego odbiorcami informacji w tym zakresie pozostanie Administrator oraz podmioty mające dostęp do tych informacji z mocy odrębnych przepisów prawa. Kontrolerem/audytorem nie może być podmiot prowadzący działalność konkurencyjną wobec Podmiotu przetwarzającego, lub osoby

pozostające w stosunku pracy z Podmiotem przetwarzającym lub w inny sposób z nim współpracujące.

3. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego bądź innego podmiotu, z którego usług korzysta Podmiot przetwarzający.
4. Na zakończenie kontroli, przedstawiciel Administratora sporządza protokół w 2 jednobrzmiących egzemplarzach, z których jeden doręcza Podmiotowi kontrolowanemu. Podmiot kontrolowany może wnieść pisemne zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego otrzymania.
5. Administrator/przedstawiciel Administratora ma obowiązek rozpatrzyć zgłoszone zastrzeżenia i poinformować Podmiot kontrolowany o uwzględnieniu zastrzeżeń w całości lub części, bądź ich nieuwzględnieniu w terminie 5 dni roboczych.
6. Podmiot kontrolowany zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie stwierdzonych uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych w terminie wskazanym przez Administratora nie dłuższym niż 5 dni roboczych, z zastrzeżeniem uwzględnienia całości lub części zastrzeżeń zgodnie z ust. 4.

§ 8 Osoby kontaktowe

1. Inspektor Ochrony Danych (IOD) pełni funkcję osoby kontaktowej dla potrzeb m.in. komunikacji dotyczącej podejrzenia naruszenia / naruszeń ochrony danych osobowych i dla osób, których dane osobowe dotyczą.
2. Z Inspektorem Ochrony Danych Administratora p. Robertem Kursą należy kontaktować pod numerem telefonu: (85) 66 54 169, pod adresem poczty elektronicznej: iod@wrotapodlasia.pl.
3. Z Inspektorem Ochrony Danych Podmiotu przetwarzającego …… należy kontaktować pod numerem telefonu: ……, pod adresem poczty elektronicznej: ……

§ 9
Czas obowiązywania umowy

1. Niniejsza umowa powierzenia przetwarzania danych osobowych zostaje zawarta na czas określony do dnia obowiązywania umowy, o której mowa § 2 ust. 1.
2. Wygaśnięcie niniejszej umowy jest równoważne z wygaśnięciem umowy, o której mowa w § 2 ust. 1.

§ 10
Rozwiązanie umowy

1. Administrator ma prawo rozwiązać niniejszą umowę powierzenia bez zachowania terminu wypowiedzenia, gdy Podmiot przetwarzający:
   a) przetwarza powierzone dane osobowe w sposób niezgodny z niniejszą Umową powierzenia;

b) korzysta z usług innego podmiotu przetwarzającego bez poinformowania Administratora o takim zamiarze;
c) nie usunął w wyznaczonym terminie uchybień stwierdzonych w toku kontroli, o której mowa w § 6.

2. Rozwiązanie umowy jest równoznaczne z rozwiązaniem umowy, o której mowa w § 2 ust. 1.

§ 11
Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powierzenia wymagają formy pisemnej pod rygorem nieważności.
2. Spory wynikłe z tytułu niniejszej Umowy powierzenia będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora.
3. W sprawach nieuregulowanych w niniejszej Umowie powierzenia mają zastosowanie przepisy Kodeksu cywilnego oraz RODO.
4. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy powierzania a umową, o której mowa w § 2 ust. 1 w zakresie danych osobowych, pierwszeństwo mają postanowienia niniejszej Umowy powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Podmiotem przetwarzającym należy regulować poprzez zmiany niniejszej Umowy.
5. Umowę powierzenia sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

…… ……
Administrator **Podmiot przetwarzający**

Załącznik nr 3.1 do umowy powierzenia przetwarzania danych osobowych – Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

Lp.	**Kategorie danych osobowych powierzanych do przetwarzania**	**Kategorie osób, których dane dotyczą**
1.	Wszystkie dane zawarte w wiadomościach e-mail.	Pracownicy UMWP, radni sejmiku Województwa Podlaskiego, klienci UMWP oraz jednostek sektora publicznego, korzystający z poczty.
2.	Wszystkie dane zawarte w wiadomościach e-mail.	Pracownicy jednostek samorządu terytorialnego, ich jednostek podległych, wojewódzkich samorządowych jednostek organizacyjnych z którymi Administrator zawarł porozumienie o współpracy oraz klienci korzystający z poczty.
Operacje podmiotu przetwarzającego na powierzanych danych osobowych		
□ zbieranie, □ organizowanie, □ porządkowanie, □ przechowywanie, □ utrwalanie, x odzyskiwanie, □ rejestracja, □ adaptowanie, □ modyfikowanie, x pobieranie, x przeglądanie, □ wykorzystywanie, □ ujawnianie poprzez przesłanie, □ ujawnianie poprzez transmisję, □ rozpowszechnianie, □ dopasowywanie, x blokowanie, □ łączenie, x ograniczanie, □ usuwanie, □ niszczenie, □ archiwizowanie, □ nagrywanie, □ fotografowanie, □ inne …….		

…… ……

Administrator **Podmiot przetwarzający**

Załącznik nr 3.2 do umowy powierzenia przetwarzania danych osobowych – Wdrożone mechanizmy zapewniające bezpieczeństwo przetwarzania danych osobowych.

	Lp.	Warunek powierzenia danych osobowych	Spełnienie warunku powierzenia przetwarzania danych osobowych	
			TAK/NIE*	**Uzasadnienie**
1.		Podmiot przetwarzający- posiada wdrożoną Politykę ochrony danych osobowych lub inne akty wewnętrzne określające zasady ochrony danych osobowych,	TAK/NIE*	Nazwa i data sporządzenia dokumentu, w tym data ostatniej aktualizacji dokumentu/ów (jeśli dotyczy):
2.		Podmiot przetwarzający posiada wdrożone normy ISO / certyfikowany kodeks postępowania.	TAK/NIE*	Nr wdrożonej normy ISO lub nazwa certyfikowanego kodeksu postępowania.
3.		Podmiot przetwarzający dla powierzonych przez Administratora danych zapewnia środki techniczne i organizacyjne odpowiednie do rodzaju przetwarzanych danych, w szczególności zapewnia:		
		pseudonimizacje i szyfrowanie danych osobowych.	TAK/NIE*	Jeśli TAK opisać sposób realizacji – jeśli NIE podać uzasadnienie:
		poufność, integralność, dostępność i odporność systemów i usług przetwarzania.	TAK/NIE*	Jeśli TAK opisać sposób realizacji – jeśli NIE podać uzasadnienie:
		zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	TAK/NIE*	Jeśli TAK opisać sposób realizacji – jeśli NIE podać uzasadnienie:
		regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.	TAK/NIE*	Jeśli TAK opisać sposób realizacji – jeśli NIE podać uzasadnienie:
8.		Podmiot przetwarzający stosuje następujące środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do charakteru, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych o różnym	TAK/NIE*	Stosowane środki techniczne i organizacyjne mające zapewnić bezpieczeństwo danych osobowych przed niżej opisanymi zagrożeniami – opisać sposób realizacji zabezpieczeń stosowany dla każdego z rodzajów zagrożeń:
				zniszczeniem
				utratą
				modyfikacją

Lp.	Warunek powierzenia danych osobowych	Spełnienie warunku powierzenia przetwarzania danych osobowych		
		TAK/NIE*	Uzasadnienie	
	prawdopodobieństwie i wadze zagrożenia.		nieuprawnionym ujawnieniem	
			nieuprawnionym dostępem	
			Inne zabezpieczenia (jeśli funkcjonują)	
15.	Podmiot przetwarzający wyznaczył Inspektora Ochrony Danych.	TAK/NIE*	Jeśli TAK to proszę podać imię i nazwisko Inspektora, nr tel. i adres mailowy: Jeśli Nie to podstawa prawna danego stanu rzeczy	
16.	Podmiot przetwarzający dopuścił do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie do ww. czynności.	TAK/NIE*	Określić sposób realizacji:	
17.	Podmiot przetwarzający zapewnia odpowiedni poziom przeszkolenia z zakresu przepisów o ochronie danych osobowych osobom, które posiadają upoważnienie do ww. czynności.	TAK/NIE*	Jeśli TAK to podać zakres przeszkolenia osób upoważnionych.	
18.	Podmiot przetwarzający zobowiązał osoby upoważnione do przetwarzania danych osobowych do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych lub osoby te podlegają ustawowemu obowiązkowi zachowania tajemnicy.	TAK/NIE*	Określić sposób realizacji:	
19.	Podmiot przetwarzający prowadzi Rejestr naruszeń danych osobowych powierzonych przez Administratora danych.	TAK/NIE*	Jeśli TAK podać sposób prowadzenia rejestru:	

Lp.	Warunek powierzenia danych osobowych	Spełnienie warunku powierzenia przetwarzania danych osobowych	
		TAK/NIE*	**Uzasadnienie**
20.	Podmiot przetwarzający dokonał dalszego powierzenia danych osobowych powierzonych przez Administratora danych.	TAK/NIE*	Jeśli TAK to proszę podać: 1) Nazwę podmiotu: 2) Datę zawarcia umowy 3) Zakres przedmiotowy umowy 4) Termin obowiązywania umowy
21.	Czy w przeciągu 6 ostatnich miesięcy doszło do naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia organowi nadzorczemu?	TAK/NIE*	
22.	Podmiot przetwarzający posiada aktualne oprogramowania, zarówno użytkowe jak i systemowe, z wysokim poziomem odporności na cyberataki.	TAK/NIE*	Nie dotyczy *jeżeli przetwarzanie danych osobowych nie będzie odbywać się z wykorzystaniem Internetu i komputerów*
23.	Podmiot przetwarzający zapewnia nadzór nad osobami niebędącymi pracownikami podmiotu przetwarzającego, a przebywającymi w jego siedzibie, wykluczający ich dostęp do danych osobowych.	TAK/NIE*	

*niepotrzebne skreślić

……

Podmiot przetwarzający

Załącznik nr 3.3 do umowy powierzenia przetwarzania danych osobowych – Wdrożone mechanizmy zapewniające bezpieczeństwo przetwarzania danych osobowych.

Zgłoszenie podejrzenia incydentu/zaistnienia naruszenia ochrony danych osobowych

- o Zgłoszenie wstępne *Proszę usunąć „○” i wstawić „X” przy właściwej treści*
- o Zgłoszenie uzupełniające/zmieniające
- o Trwające podejrzenie incydentu/zaistnienia naruszenie

Data rozpoczęcia podejrzenia incydentu/zaistnienia naruszenia
Dokładny termin lub czas przybliżony
D/M/R …….. (godzina, adres, nr pokoju)

Sposób stwierdzenia podejrzenia incydentu/zaistnienia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa
……
……..

Data i czas zakończenia podejrzenia incydentu/zaistnienia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. Nie należy wypełniać jeżeli naruszenie trwa nadal
D/M/R ……..
Komentarz do czasu podejrzenia incydentu/zaistnienia naruszenia *(opcjonalnie)*
Proszę podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia zdarzenia
……
……..

Charakter możliwości naruszenia: *Wstaw X przy właściwej treści*

- o Naruszenie poufności danych *Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych*
- o Naruszenie integralności danych *Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania*
- o Naruszenie dostępności danych *Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną*

Na czym polegało zdarzenie? *Wstaw X przy właściwej treści. Można usunąć nieprzydatne przykłady*

- o Zgubienie lub kradzież nośnika/urządzenia
- o Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
- o Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem do nadawcy
- o Nieuprawnione uzyskanie dostępu do informacji
- o Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
- o Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
- o Uzyskanie poufnych informacji poprzez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

- o Nieprawidłowa anonimizacja danych osobowych w dokumencie
- o Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
- o Niezamierzona publikacja
- o Dane osobowe wysłane do niewłaściwego odbiorcy
- o Ujawnienie danych niewłaściwej osobie
- o Ustne ujawnienie danych osobowych
- o Zdarzenie dotyczy dziecka/dzieci - w związku ze świadczeniem usług społeczeństwa informacyjnego skierowanego do dziecka/dzieci
- o Inne……

Przyczyna zdarzenia:

- o Wewnętrzne działanie w podmiocie/organizacji/urzędzie
- o Zewnętrzne działanie w podmiocie/organizacji/urzędzie
- o Inne przyczyny: ……

Szczegółowy opis danych, które zostały lub mogły zostać ujawnione:

- o Dane identyfikacyjne *np. imię i nazwisko, login, hasło (zapisane otwartym tekstem lub hashowane), nr dowodu osobistego/paszportu, adres IP, nr tel. stacjonarnego/komórkowego,*
- o Krajowy nr identyfikacyjny *(PESEL)*
- o Dane kontaktowe *np. e-mail, nr tel. stacjonarnego/komórkowego, adres korespondencyjny*
- o Dane ekonomiczne i finansowe *np. historie transakcji, faktury, dane o rachunkach bankowych*
- o Oficjalne dokumenty *np. akty notarialne, legitymacje*
- o Dane lokalizacyjne *np. GPS, miejsce zamieszkania.*
- o Inne *Opisz kategorie danych.……..*

Proszę wymienić/opisać te dane

……..……
……..……

Dane szczególnej kategorii:

- o Dane o pochodzeniu rasowym lub etnicznym
- o Dane o poglądach politycznych
- o Dane o przekonaniach religijnych lub światopoglądowych
- o Dane o przynależności do związków zawodowych
- o Dane dotyczące seksualności lub orientacji seksualnej
- o Dane dotyczące zdrowia
- o Dane genetyczne
- o Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

Dane, o których mowa w art. 10 RODO:

- o Dane dotyczące wyroków skazujących
- o Dane dotyczące czynów zabronionych
- o Inne *Opisz* ……

Przybliżona liczba wpisów danych osobowych, których dotyczy zdarzenie ……

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów/operacji

Kategorie osób:

- Pracownicy
- Użytkownicy
- Subskrybenci
- Studenci
- Uczniowie
- Klienci
- Pacjenci
- Dzieci
- Osoby o szczególnych potrzebach np. osoby starsze, niepełnosprawne itp.
- Inne ……..

Przybliżona liczba osób, których mogło dotyczyć zdarzenia ……..

ŚRODKI BEZPIECZEŃSTWA ZASTOSOWANE PRZED PODEJRZENIEM INCYDENTU / ZAISTNIENIEM NARUSZENIEM DOTYCZĄCYM TEGO ZDARZENIA

……
……..……
……..
……

MOŻLIWE KONSEKWENCJE DLA OSOBY, KTÓREJ DANE DOTYCZĄ

- Utrata kontroli nad własnymi danymi osobowymi
- Ograniczenie możliwości realizowania praw z art. 15 – 22 RODO
- Dyskryminacja
- Kradzież lub sfałszowanie tożsamości
- Strata finansowa
- Naruszenie dobrego imienia
- Utrata poufności danych osobowych chronionych tajemnicą zawodową
- Nieuprawnione odwrócenie pseudonimizacji
- Inne ……..

Ryzyko naruszenia praw i wolności osób fizycznych

- Niskie
- Średnie
- Wysokie

ŚRODKI ZARADCZE

Komunikacja z osobami, których dane dotyczą

Czy osoby, których dane dotyczą, zostaną powiadomione o zdarzeniu?

- Tak

Proszę opisać czy każda osoba, której dotyczy podejrzenie naruszenia zostanie powiadomiona, w jaki sposób (na e-maila, pisemnie itp.) ……..……..
……

Proszę wskazać datę, kiedy osoby, których dane dotyczą, zostaną powiadomione o zdarzeniu ……..
lub proszę wpisać „nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą/nie dotyczy”

Liczba osób, które zostaną powiadomione …….

Środki komunikacji, jakie zostaną wykorzystane do zawiadomienia osoby, której dane dotyczą

……
……..
Proszę przedstawić/załączyć proponowaną do wysłania treść zawiadomienia osób, których dane dotyczą zdarzenia

- Nie, ponieważ:
  - Przed zdarzeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacji uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych

Proszę opisać te środki ……..……..
……

- Nie oceniłem

Środki w celu zaradzenia podejrzenia incydentu/zaistnienia naruszenia ochrony danych osobowych

Proszę opisać dodatkowe środki zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków podejrzenia incydentu/zaistnienia naruszenia

……
……..

Transgraniczne przetwarzania

Czy w przypadku oceny Administratora, iż doszło do naruszenie danych osobowych/naruszenia ochrony danych osobowych zostanie wystosowane zgłoszenie innemu organowi nadzorczemu UE / spoza UE *(opcjonalnie) Proszę podać kraj/e* ……..…

Czy w przypadku oceny Administratora, iż doszło do naruszenie danych osobowych/naruszenia ochrony danych osobowych zostanie wystosowane zgłoszenie innemu organowi UE/ spoza UE z powodu innych zobowiązań prawnych *(opcjonalnie) Wymień inne organy, którym naruszenie zostanie zgłoszone z powodu innych zobowiązań prawnych* ……..

…….
Podpis osoby dokonującej zgłoszenia