POLITYKA BEZPIECZEŃSTWA W RELACJACH Z PODMIOTAMI ZEWNĘTRZNYMI

Numer referencyjny dokumentu: 1.2

SPIS TREŚCI

§ 1

WSTĘP

1. Zgodnie z § 17 *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, wprowadza się do stosowania *Politykę bezpieczeństwa w relacjach z podmiotami zewnętrznymi*, **stanowiącą dokument I poziomu SZBIiCD**.
2. Relacje UMWP z podmiotami zewnętrznymi mają charakter sformalizowany, a współpraca odbywa się w oparciu o obowiązujące przepisy prawa, *Politykę Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, niniejszą *Politykę* oraz indywidualne umowy i porozumienia.
3. Rejestry zawartych umów i porozumień prowadzone są w poszczególnych komórkach organizacyjnych UMWP przez ich kierowników lub osoby przez nich wyznaczone.
4. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów Urzędu oraz utrzymania ciągłości realizacji usług świadczonych przez ww. podmioty, wprowadza się niniejsze zasady i wymogi bezpieczeństwa i ciągłości działania.
5. Przedmiotowe zasady i wymogi dot. w szczególności:
   1) udostępniania aktywów informacyjnych oraz monitorowania i kontroli dostępu,
   2) przestrzegania określonych zasad i wymogów przez podmioty zewnętrzne,
   3) obowiązków podmiotów zewnętrznych w zakresie zapewnienia ochrony aktywów informacyjnych UMWP i ciągłości świadczonych usług,
   4) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji i/lub ciągłości działania,
   5) uświadamiania pracowników podmiotów zewnętrznych w zakresie bezpieczeństwa informacji i ciągłości działania,
   6) postępowania z poufnymi informacjami, w tym powierzonymi podmiotom zewnętrznym danymi osobowymi,
   7) dodatkowych wymogów w zakresie utrzymania ciągłości realizacji procesów krytycznych.
6. Jednocześnie zapisy niniejszej *Polityki* stanowią punkt wyjścia do indywidualnych ustaleń i zapisów uzupełniających w umowach lub porozumieniach z podmiotami zewnętrznymi, których zakres zależy od charakteru i specyfiki współpracy.
7. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w UMWP dokumentacji bezpieczeństwa i ciągłości działania, dopuszcza się stosowanie dodatkowych wymogów określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi *„zewnętrzne”* nie obniżają poziomu bezpieczeństwa pozostałych

informacji przetwarzanych w UMWP i nie generują ryzyka utraty ciągłości działania Urzędu.

8. Zapisy niniejszego dokumentu mają charakter uzupełniający do treści *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego - dokument główny oraz* dokumentów II i III poziomu SZBIiCD, tworząc wspólnie kompleksową dokumentację bezpieczeństwa i ciągłości działania.
9. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa i ciągłości działania określonymi w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania*.

§ 2

WYKAZ SKRÓTÓW I DEFINICJI

1. Stosowany w treści niniejszej *Polityki* termin „podmiot zewnętrzny" (m.in. wykonawcy i kontrahenci, dostawcy produktów, materiałów i usług) oznacza wszystkich pracowników tego podmiotu, wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów Urzędu w związku z realizacją zawartej umowy lub porozumienia.
2. Pozostałe stosowane w niniejszej *Polityce* definicje i skróty należy rozumieć zgodnie z *Wykazem skrótów i definicji*, stanowiącym załącznik nr 1 do *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny.*

§ 3

ZAKRES STOSOWANIA

1. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* określa podstawowe zasady i wymogi w zakresie współpracy z podmiotami zewnętrznymi, w tym współpracy w obszarze dostaw technologii informacyjnych i telekomunikacyjnych.
2. Podmiot zewnętrzny będący stroną zawartej umowy lub porozumienia zobowiązany jest do zapoznania podległych mu pracowników realizujących przedmiot ww. umowy lub porozumienia z zasadami ochrony aktywów informacyjnych Urzędu Marszałkowskiego Województwa Pomorskiego (UMWP), określonymi w szczególności w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz niniejszej *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi.*
3. Pracownicy podmiotów zewnętrznych, o których mowa w ust. 2 zobowiązani są do przestrzegania wymogów określonych w ww. *Politykach*.

§ 4

PRZYZNAWANIE DOSTĘPU DO AKTYWÓW INFORMACYJNYCH URZĘDU

1. Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych Urzędu, w tym do:
   1) informacji sklasyfikowanych w poszczególnych grupach:
      a) dane osobowe,
      b) tajemnice prawnie chronione,
      c) tajemnice Urzędu,
      d) informacje jawne,
   2) aktywów wspierających przetwarzanie ww. informacji:
      a) sprzęt (w tym komputery, nośniki informacji),
      b) oprogramowanie,
      c) sieć,
      d) personel (w tym pracownicy UMWP),
      e) lokalizacja/siedziba (w tym pomieszczenia biurowe Urzędu),
      f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Urzędu),

w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

2. Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie i/lub realizację umowy lub porozumienia, na zasadach i w trybie określonym w *Polityce kontroli dostępu* i treści *dedykowanych Polityk dla poszczególnych grup informacji*.
3. Przyznawanie rozszerzonych uprawnień lub dodatkowych przywilejów możliwe jest po przedłożeniu stosownego uzasadnienia przez ww. kierownika i po formalnym odnotowaniu przedmiotowej zmiany.
4. Dostęp zdalny podmiotów zewnętrznych do aktywów informacyjnych Urzędu, np. w związku z wykonywaniem prac serwisowych i aktualizacji, przyznawany jest w zakresie niezbędnym do realizacji zadań i tylko pod nadzorem uprawnionych pracowników Urzędu.
5. Zasady dostępu fizycznego do budynków i pomieszczeń UMWP dla pracowników podmiotów zewnętrznych:
   1) Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków UMWP, hole, korytarze oraz wybrane pomieszczenia niestanowiące pomieszczeń ograniczonego dostępu i/lub podwyższonego poziomu bezpieczeństwa, w tym pomieszczenia użyteczności publicznej takie jak punkty obsługi klienta, poczta etc.

2) Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy administracyjnej (ograniczonego dostępu), w tym pomieszczeń biurowych, w zakresie wynikającym z realizacji zadań określonych w treści zawartych umów lub porozumień i na formalny wniosek właściwego kierownika.

3) W strefie o podwyższonym poziomie bezpieczeństwa obejmującej m.in. serwerownie, pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem wybranych pracowników Departamentu Cyfryzacji (DC) tj. Generalnego Administratora Systemu Informatycznego (GASI) lub Administratora Systemu Informatycznego (ASI). Dostęp do strefy o podwyższonym poziomie bezpieczeństwa jest na bieżąco rejestrowany.

§ 5

PODSTAWOWE ZASADY BEZPIECZEŃSTWA I CIĄGŁOŚCI DZIAŁANIA W ZAKRESIE WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI

1. W uzupełnieniu do zasad i wymogów określonych w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, pracownicy podmiotów zewnętrznych zobowiązani są przestrzegać poniższych zasad.
2. W przypadku korzystania z budynków i pomieszczeń UMWP, pracownicy podmiotów zewnętrznych zobowiązani są do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.
3. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla pracowników podmiotów zewnętrznych z zakresu bezpieczeństwa informacji i ciągłości działania.
4. Ww. pracownicy zobowiązani są stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń.
5. Celem zabezpieczenia aktywów, o których mowa w ust. 4, pracownicy podmiotów zewnętrznych zobowiązani są do przesyłania plików zawierających informacje chronione (m.in. dane osobowe) z wykorzystaniem sieci Internet, w tym za pośrednictwem poczty elektronicznej, w formie zaszyfrowanej. Zaszyfrowane pliki musza być przesyłane w sposób umożliwiający ich ponowne odszyfrowanie po stronie odbiorcy np. po podaniu unikalnego hasła do pliku.

   Hasło do zabezpieczonych plików należy przekazać odbiorcy innym kanałem komunikacji od użytego do przesłania danych. Za powyższe czynności odpowiedzialna jest osoba przekazująca dane.
6. Pracownikom podmiotów zewnętrznych nie wolno podejmować prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych, w tym:

   1) samowolnie modyfikować ustawień związanych z bezpieczeństwem,

   2) świadomie wprowadzać błędnych danych,

3) podejmować prób przywłaszczenia lub rozszyfrowania informacji uwierzytelniających innych użytkowników.

7. W ramach zapewnienia poufności przetwarzanych informacji, pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas nieokreślony (w trakcie jak i po zakończeniu trwania umowy lub porozumienia) informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnieniem osobom nieuprawnionym.
8. Wymóg zachowania poufności, o którym mowa w ust. 7 obejmuje wszelkie informacje chronione, których ujawnienie mogłoby narazić UMWP na szkodę. Przedmiotowy wymóg nie dotyczy informacji, które:
   1) są jawne i ogólnodostępne,
   2) przekazane zostały podmiotowi zewnętrznemu z możliwością dalszego ujawnienia.
9. W trakcie trwania umowy lub porozumienia, podmiot zewnętrzny zobowiązuje się ponadto:
   1) do wykonania przedmiotu umowy lub porozumienia:
      a) zgodnie z wymogami prawa powszechnie obowiązującego i treścią zawartej umowy lub porozumienia,
      b) z zachowaniem najwyższej profesjonalnej staranności i przy wykorzystaniu całej posiadanej wiedzy i doświadczenia,
      c) przy wsparciu personelu posiadającego niezbędną wiedzę i umiejętności,
      d) w sposób niepowodujący przerwania lub zakłócenia ciągłości pracy Urzędu,
   2) nie zapoznawać się z dokumentami, analizami, zawartością systemu i aplikacji, dysków twardych etc., które nie są związane z przedmiotem umowy lub porozumienia,
   3) nie powielać powierzonych informacji w zakresie szerszym, niż jest to niezbędne dla realizacji przedmiotu umowy lub porozumienia, w tym nie kopiować informacji celem udostępnienia ich osobom nieuprawnionym.
10. Podmiot zewnętrzny zobowiązany jest do zapewnienia pełnej rozliczalności działań pracowników i innych osób, którym powierzył realizację zadań wynikających z zawartej umowy/porozumienia, w tym do ich niezwłocznego wskazania na żądanie Urzędu.
11. Po zakończeniu przedmiotowej współpracy, podmiot zewnętrzny zobowiązany jest niezwłocznie, w zależności od decyzji Urzędu, zwrócić lub zniszczyć udostępnione aktywa, w tym sprzęt lub informacje przekazane mu na dowolnych nośnikach, włączając wszelkie ich kopie.

    Na pisemne polecenie Urzędu, fakt zwrotu aktywów, w tym informacji potwierdza się w formie pisemnego protokołu przekazania.

    W przypadku zniszczenia aktywów, podmiot zewnętrzny zobowiązany jest (na polecenie Urzędu) złożyć pisemne oświadczenie potwierdzające przeprowadzenie zniszczenia.

12. Dodatkowe zapisy dot. obowiązków podmiotów zewnętrznych wykonujących usługę ochrony i sprzątania w budynkach i pomieszczeniach UMWP określa dedykowana procedura Departamentu Zamówień Publicznych i Administracji (DAZ), stanowiąca dokument III poziomu SZBIiCD.

§ 6

TREŚĆ UMÓW I POROZUMIEŃ Z PODMIOTAMI ZEWNĘTRZNYMI

1. Celem ograniczenia ryzyka związanego z dostępem podmiotów zewnętrznych do aktywów UMWP lub utratą ciągłości działania Urzędu, w treści zawieranych umów lub porozumień wprowadza się niezbędne wymogi dot. bezpieczeństwa aktywów informacyjnych i/lub utrzymania ciągłości świadczonych usług, do których przestrzegania w trakcie i po zakończeniu umowy lub porozumienia zobowiązany jest ww. podmiot zewnętrzny.
2. Jeżeli zawarcie danej umowy/porozumienia wymaga uprzednich konsultacji przed jej/jego podpisaniem (w ramach których udostępniane są podmiotowi zewnętrznemu informacje poufne UMWP i/lub aktywa wspierające ich przetwarzanie), dodatkowe zapisy/wymogi bezpieczeństwa (poza tymi znajdującymi się w zawieranej umowie/porozumieniu) należy przedłożyć podmiotowi zewnętrznemu.

   Podmiot zewnętrzny, przed rozpoczęciem przedmiotowych konsulatacji, zobowiązuje się do zapoznania się i przestrzegania przedłożonych wymogów np. w formie umowy o zachowaniu poufności (NDA – non-disclosure agreement).
3. Właściwy kierownik komórki organizacyjnej, odpowiedzialny za przygotowanie i/lub realizację umowy lub porozumienia, przygotowuję adekwatne zapisy dot. bezpieczeństwa informacji i/lub ciągłości działania.
4. Podstawowy zakres wymogów, o których mowa w ust. 1 i 2 wynika wprost z obowiązujących przepisów prawa oraz dokumentacji bezpieczeństwa i ciągłości działania, w szczególności *Polityki bezpieczeństwa informacji i ciągłości działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz niniejszej *Polityki*.
5. Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania, o których mowa powyżej określa załącznik nr 1 do niniejszej *Polityki*.
6. Poza ww. podstawowymi wymogami, szczegółowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach/porozumieniach z podmiotami zewnętrznymi powinny uwzględniać m.in..:
   1) kompletny opis dostarczanego produktu lub usługi,
   2) zakres i poziom świadczonych usług,
   3) cel i zakres przetwarzanych informacji/ udostępnionych aktywów wspierających,
   4) zakres odpowiedzialności podmiotu zewnętrznego z tytułu prawa i zapisów umowy/porozumienia,
   5) zasady dot. okresowego/bieżącego raportowania z tytułu postępów w realizacji umowy/porozumienia,
   6) zasady zarządzania zmianami przy realizacji umowy/porozumienia,

7) listę osób realizujących przedmiot umowy/porozumienia (co najmniej poprzez wskazanie osób koordynujących realizację zadań po obu stronach),

8) wykaz osób upoważnionych do wymiany informacji i listę zatwierdzonych narzędzi do komunikacji,

9) zasady i tryb postępowania w przypadku awarii lub katastrofy (maksymalny czas reakcji, maksymalny czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,

10) akceptowalny poziom dostępności świadczonych usług (np. zapisy dotyczące gwarantowanego poziomu oraz warunków świadczonych usług z zakresu IT - SLA),

11) zasady ochrony własności intelektualnej i praw autorskich, oraz ich ewentualnego przeniesienia,

12) warunki renegocjacji lub zakończenia umowy/porozumienia.

7. Zakres oraz stopień szczegółowości ww. zapisów dot. bezpieczeństwa informacji i/lub ciągłości działania w treści umowy lub porozumienia zależy od przedmiotu i specyfiki podejmowanej współpracy oraz zidentyfikowanych zagrożeń.

8. Przy zawieraniu umów lub porozumień z kluczowymi dostawcami usług lub produktów, niezbędnych do realizacji procesów krytycznych, tam gdzie to uzasadnione należy uwzględnić dodatkowe zapisy w zakresie utrzymania ciągłości działania i świadczenia usług na rzecz UMWP dot.:

   1) ustanowienia po stronie dostawców Planów ciągłości działania (PCD) z czasami nie dłuższymi niż czasy docelowego wznowienia działania (RTO) zidentyfikowane dla danego procesu krytycznego,

   2) wykonywania przynajmniej raz do roku testów PCD przez dostawcę,

   3) ich ewentualnego uczestnictwa w testach ciągłości działania realizowanych przez Urząd,

   4) umożliwienia przeprowadzenia audytów PCD u dostawcy.

   W przypadku korzystania przez dostawcę z usług podwykonawców wymogi określone w pkt 1-4 dotyczą również podwykonawców.

9. W przypadku powierzenia podmiotom zewnętrznym przetwarzania danych osobowych, podmiot przetwarzający zobowiązany jest zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przedmiotowe przetwarzanie spełniało wymogi RODO.

   Ww. gwarancje i wdrożenie ww. środków podlegają weryfikacji Administratora Danych (AD)/właściwego AZ kierownika właściwej komórki organizacyjnej UMWP na zasadach określonych w *Polityce bezpieczeństwa danych osobowych.,* np. w oparciu o udostępnioną i uzupełnioną przez podmiot przetwarzający *Listę kontrolną (weryfikacyjną) podmiotu przetwarzającego*, której wzór stanowi załącznik nr 2 do niniejszej *Polityki*.

10. Przy okazji doskonalenia dostarczanych produktów i usług, zmiany wynikające m.in. z wprowadzenia nowych wersji dokumentacji bezpieczeństwa i ciągłości działania,

wprowadzenia nowych zabezpieczeń, zmiany lokalizacji, należy - tam gdzie to niezbędne - uwzględnić w formie aneksów do już istniejących umów lub porozumień.

§ 7

MONITOROWANIE I PRZEGLĄD USŁUG ŚWIADCZONYCH PRZEZ PODMIOTY ZEWNĘTRZNE

1. Dostęp podmiotów zewnętrznych i korzystanie z aktywów informacyjnych Urzędu przez ich pracowników są nadzorowane i monitorowane, m.in. za pośrednictwem systemu monitoringu wizyjnego (CCTV).
2. Bieżący nadzór nad udostępnianiem i korzystaniem przez podmioty zewnętrzne z aktywów informacyjnych UMWP prowadzi właściwy kierownik komórki organizacyjnej lub osoba/osoby przez niego wyznaczone.
3. Ww. osoby zobowiązane są również do monitorowania czy współpracujące podmioty zewnętrzne realizują swoje zadania zgodnie z prawem i treścią zawartych umów lub porozumień, a dostarczane przez nich produkty i usługi są zgodne z przedmiotem umowy lub porozumienia oraz spełniają oczekiwania odbiorców.
4. Na wniosek UMWP, podmiot zewnętrzny zobowiązany jest przekazać informacje dotyczące postępów prac, przyczyn opóźnień lub nienależytego wykonywania zawartej umowy lub porozumienia. Informacje przekazywane są niezwłocznie w formie pisemnej.
5. W uzasadnionych przypadkach, podmiot zewnętrzny zobowiązany jest umożliwić weryfikację postępów prac bezpośrednio w swojej siedzibie w trybie postępowania sprawdzającego (audytu bezpieczeństwa).
6. Przedmiotowe zapisy dot. monitorowania i przeglądu usług świadczonych przez podmioty zewnętrzne mogą zostać doszczegółowione w treści zawartych umów lub porozumień (ewentualnie w aneksach do już istniejących umów lub porozumień).

§ 8

ZGŁASZANIE PRZYPADKÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI PRZEZ PODMIOTY ZEWNĘTRZNE

1. Osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w UMWP i/lub utraty ciągłości realizacji usług świadczonych na rzecz UMWP, zobowiązani są niezwłocznie poinformować o szczegółach i charakterze zdarzenia kierownika Referatu Bezpieczeństwa Informacji w Departamencie Organizacji (kierownika DO-B) lub pracownik DO-B przez niego wskazanego.
2. Zgłoszenie, o którym mowa w ust. 1, należy przesłać drogą mailową na adres incydent@pomorskie.eu, podając dane kontaktowe, okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia (można skorzystać z *Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania*, którego wzór stanowi załącznik nr 3 do niniejszej *Polityki*)

3. W uzasadnionych przypadkach dopuszcza się dokonanie przedmiotowego zgłoszenia w innym trybie np. telefonicznie na numer 58 326 85 18, 58 326 87 52 lub 58 326 89 71.
4. Po powzięciu informacji o okolicznościach mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji i/lub utracie ciągłości realizacji usług świadczonych na rzecz UMWP, dalsze postępowanie, w tym obsługa i wyjaśnienie przyczyn incydentu związanego z bezpieczeństwem informacji, odbywa się zgodnie z *Procedurą obsługi i postepowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłością działania*, stanowiącą załącznik do *Polityki zarządzania incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania*.
5. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązującej dokumentacji bezpieczeństwa i ciągłości działania przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.
6. Z tytułu działań podmiotów zewnętrznych i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dot. niewłaściwego przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
    1) kodeksie pracy,
    2) kodeksie cywilnym,
    3) kodeksie karnym,
    4) RODO oraz ustawie o ochronie danych osobowych.

§ 9

ZASADY WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Poza współpracą z tytułu zawartych umów i porozumień, z uwagi na wymogi prawa powszechnie obowiązującego, celem zapewnienia kompleksowej ochrony przetwarzanych informacji i utrzymania ciągłości działania Urzędu, w tym ochrony przed cyberzagrożeniami, wymiany wiedzy i doświadczeń oraz wsparcia procesu zarządzania zdarzeniami, w tym incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania, pracownicy UMWP współpracują z wybranymi instytucjami, organizacjami oraz podmiotami sektora publicznego i prywatnego.
2. W ramach przedmiotowej współpracy, w uzasadnionych przypadkach, w szczególności:
    1) w przypadku wybranych incydentów o priorytecie wysokim,
    2) w przypadku incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,
    3) w przypadku incydentów noszących znamiona przestępstwa,

informacja o incydencie przekazywana jest do właściwych podmiotów zewnętrznych, w tym:

a) organów ścigania w przypadku incydentów wyczerpujących znamiona przestępstwa (np. przestępstwa przeciwko ochronie informacji wskazane w Kodeksie Karnym),

b) Agencji Bezpieczeństwa Wewnętrznego,

c) właściwych zespołów reagowania na incydenty bezpieczeństwa komputerowego – w tym CSIRT NASK.

3. Współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych prowadzona jest w obszarze ochrony danych osobowych, w tym wymiany doświadczeń i stałego podnoszenia wiedzy pracowników UMWP.

4. Przypadki naruszenia ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych są niezwłocznie zgłaszane organowi nadzorczemu (Prezesowi UODO), na zasadach i w trybie szczegółowo określonym w obowiązującej w UMWP *Procedurze obsługi i postępowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania.*

Załącznik nr 1 Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznymi

§ …

BEZPIECZEŃSTWO INFORMACJI i UTRZYMANIE CIĄGŁOŚĆ DZIAŁANIA

1. Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* będący stroną zawartej Umowy/Porozumienia* zobowiązany jest do zapewnienia bezpieczeństwa informacji przetwarzanych w związku jej/jego* realizacją, ochrony pozostałych udostępnionych mu aktywów Urzędu Marszałkowskiego Województwa Pomorskiego (UMWP)/Zamawiającego*, wspierających przetwarzanie tych informacji, w szczególności do zapewnienia ich poufności, integralności i dostępności oraz do zapewnienia ciągłości realizacji usług świadczonych na rzecz Urzędu/Województwa Pomorskiego/na jego rzecz*.
2. Ww. Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* zobowiązuje się do wykonania przedmiotu Umowy/Porozumienia* zgodnie z przepisami prawa powszechnie obowiązującego oraz do zapoznania się przed jej/jego* podpisaniem i przestrzegania wymogów w zakresie bezpieczeństwa informacji i ciągłości działania określonych w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz dedykowanej *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi*, dostępnych w Biuletynie Informacji Publicznej Urzędu Marszałkowskiego Województwa Pomorskiego (*bip.pomorskie.eu*), w zakładce *Bezpieczeństwo Informacji*.
3. Podmiot, o którym mowa w ust. 1 i 2, w ramach niniejszej Umowy/Porozumienia* zobowiązuje się w szczególności:
   1) stale troszczyć o powierzone mu informacje i aktywa wspierające ich przetwarzanie oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w tym zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnionym udostępnieniem, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi,
   2) korzystać z powierzonych mu informacji i aktywów wspierających ich przetwarzanie, zgodnie z oraz wyłącznie do celów wynikających z zapisów zawartej Umowy/Porozumienia*,
   3) przesyłać informacje chronione z wykorzystaniem sieci Internet w formie zaszyfrowanej,
   4) nie powielać, w tym nie kopiować informacji chronionych, udostępnionych i opracowanych w trakcie Umowy/Porozumienia* w zakresie szerszym, niż jest to potrzebne do jej/jego* realizacji,
   5) informować Urząd Marszałkowski Województwa Pomorskiego (UMWP)/Zamawiającego* o każdym podejrzeniu naruszeniu bezpieczeństwa informacji i/ lub utraty ciągłości realizacji usług świadczonych na jego rzecz,
   6) niezwłocznie po zakończeniu niniejszej Umowy/Porozumienia*, trwale usunąć i/lub zniszczyć informacje chronione przetwarzane w ramach jej/jego* realizacji,

chyba że obowiązek ich dalszego przetwarzania wynika wprost z przepisów prawa powszechnie obowiązującego.

4. Jednocześnie Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* potwierdza, że pracownicy bezpośrednio realizujący przedmiot niniejszej Umowy/Porozumienia* zostali zapoznani i zobowiązani do przestrzegania przedmiotowych wymogów w zakresie bezpieczeństwa informacji i ciągłości działania.

** niepotrzebne skreślić*

LISTA KONTROLNA (WERYFIKACYJNA) PODMIOTU PRZETWARZAJĄCEGO

Lista kontrola - narzędzie do wstępnej weryfikacji, czy Podmiot Przetwarzający (PP) zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie, które będzie dokonywała w imieniu Zamawiającego – Województwo Pomorskie reprezentowane przez Zarząd WP, jako administratora danych, spełniało wymogi RODO.

Lista kontrolna ma charakter dwupoziomowy. Pytania poziomu I (1,2,3…) mają charakter podstawowy a udzielenie odpowiedzi na nie ze strony PP jest niezbędne do przeprowadzenie ww. weryfikacji. Dodatkowo lista zawiera szereg pytań uzupełniających (pytania poziomu II – 3.1, 3.2., 3.3 …), które w zależności od specyfiki i charakteru przetwarzania mogą zostać wykorzystane do pogłębionej weryfikacji wstępnej i/lub jako narzędzie pomocnicze przy przeprowadzania audytów i inspekcji przez administratora, w ramach wykonywania swoich uprawień określonych w art. 28 ust. 3 lit. h) RODO[1].

Poniższe pytania nie dotyczą zabezpieczeń stosowanych wobec wszystkich danych, będących w posiadaniu Wykonawcy/Podmiotu, ale jedynie wobec danych powierzonych.

Nazwa i siedziba Podmiotu Przetwarzającego (PP)	
Adres świadczenia usług dla administratora (jeżeli inny niż powyżej)	
Dane kontaktowe	

PYTANIA WSTĘPNE				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			
1.		Czy PP stosuje zatwierdzony przez organ nadzorczy **kodeks postępowania**, o którym mowa w art. 40 RODO?	☐ TAK ☐ NIE	
2.		Czy PP posiada **certyfikat** zgodny z art. 42 RODO?	☐ TAK ☐ NIE	
Proszę wypełnić dalej, jeżeli na oba powyższe pytania udzielono odpowiedzi NIE				
WIEDZA FACHOWA I WIARYGODNOŚĆ				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			
3.		Czy PP posiada **doświadczenie** w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeżeli TAK, to jak długie?	☐ TAK ☐ NIE	

[1] **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

4.		Czy PP wdrożył **środki dotyczące certyfikacji / zapewnienia jakości procesów**, usług/produktów, w tym zasady zarządzania bezpieczeństwem informacji (ZBI)? Jeżeli TAK, proszę zaznaczyć jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐TAK ☐ NIE	☐ ZBI na podstawie normy ISO 27001 ☐ ZBI na podstawie normy ISO 27001 – (certyfikowany SZBI) ☐ ZBI z elementami wykorzystania normy ISO 27001? ☐ [dla podmiotów publicznych] ZBI zgodnie z KRI[2]? ☐ inne – jakie? (SKU)[3]? ……..
5.		Czy PP wyznaczył **inspektora ochrony danych** lub gdy nie wymagają tego przepisy prawa inną osobę / zespół odpowiedzialny za nadzór nad ochroną danych osobowych (art. 37 RODO)? Jeżeli TAK, proszę o podanie danych kontaktowych.	☐ TAK ☐ NIE	
	5.1.	*Czy IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
	5.2.	*Czy dane IOD zostały opublikowane na stronie podmiotu przetwarzającego?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
	5.3.	*Czy IOD posiada zastępcę? Jeżeli NIE – proszę przejść do pytania 6.*	☐ TAK ☐ NIE	
	5.4.	*Czy zastępca IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
	5.5.	*Czy dane zastępcy IOD zostały opublikowane na stronie podmiotu przetwarzającego?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
6.		Czy PP zapewnia, aby osoby wyznaczone do wykonywania zadań z zakresu PP posiadały odpowiednią wiedze i przygotowanie praktyczne	☐ TAK ☐ NIE	

[2] **Krajowe Ramy Interoperacyjności** – r*ozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (D.U. 2016 Poz. 113)

[3] **SKU** – Standardowe Klauzule Umowne – Zał. III Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych Decyzji Wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 RODO oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725.

		do wykonywania swoich obowiązków z zakresu przetwarzania powierzonych danych? Jeżeli TAK, czy jest to udokumentowane np. odbytymi szkoleniami w zakresie ochrony danych osobowych, bezpieczeństwa informacji?		
7.		Czy PP posiada referencje od innych podmiotów, które obsługiwał/obsługuje w zakresie powierzania przetwarzania danych osobowych na ich zlecenie? Jeżeli TAK, prosimy o przedstawienie takich referencji.	☐ TAK ☐ NIE	
8.		Czy w ciągu ostatnich 3 lat, stwierdzono prawomocną decyzją Prezesa Urzędu Ochrony Danych Osobowych lub prawomocny wyrokiem sądu naruszenie ochrony danych osobowych przez PP? Jeżeli TAK, czy zostały wdrożone zabezpieczenia eliminujące ryzyko naruszeń w przyszłości?	☐ TAK ☐ NIE	
	8.1.	*Czy poza ww. wystąpiły incydenty/naruszenia ochrony danych osobowych przy przetwarzaniu danych powierzonych przez Administratora?*	☐ TAK ☐ NIE	
PODPOWIERZENIE				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			
9.		Czy w procesie przetwarzania powierzonych danych wykorzystywane są/będą usługi innych **podwykonawców** (tzw. podpowierzenie przetwarzania danych)? (art. 28 ust. 4 RODO; SKU) Jeżeli TAK, proszę wymienić podprocesorów (WYKAZ PODPROCESORÓW) Jeżeli NIE, proszę przejść do pytania nr 12	☐ TAK ☐ NIE	
10.		Czy z podmiotami, o których mowa w pytaniu 9 zostały podpisane umowy/porozumienia/inny instrument prawny regulujący podpowierzenie, zgodne z art. 28 ust. 3 RODO?	☐ TAK ☐ NIE	
11.		Czy PP przy wyborze swojego podwykonawcy przeprowadza działania weryfikujące lub preaudytowe, czy podwykonawca spełnia wystarczające gwarancje wdrożenia odpowiednich środków	☐ TAK ☐ NIE	

		zabezpieczających, by przetwarzanie spełniało wymogi RODO i chroniło podmioty danych? (art.28 RODO)		
	11.1.	*Czy PP przed podpisaniem umowy z podwykonawcami, którym zostanie powierzone przetwarzanie danych osobowych, uzyskano zgodę Administratora?*	☐ TAK ☐ NIE	
	11.2.	*Czy PP weryfikuje / przeprowadza doraźne lub bieżące kontrole/audyty swoich podwykonawców? (art. 28 ust. 3 lit. h) RODO; art. 32 ust. 1 lit. d) RODO*	☐ TAK ☐ NIE	
	11.3.	*Czy wnioski z ww. kontroli/audytów zostały udokumentowane np. w raporcie audytowym?*	☐ TAK ☐ NIE	
ZASOBY – ŚRODKI ORGANIZACYJNE				
Dokumentacja wewnętrzna				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			
12.		Czy PP dokonuje okresowej **analizy ryzyka** (art. 24, 25, **32**, 35 RODO) i dokumentuje jej przeprowadzenie, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z: a) przypadkowego lub niezgodnego z prawem zniszczenia, b) utraty, modyfikacji, nieuprawnionego ujawnienia, c) lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
	12.1.	*Czy PP przeprowadzał okresową **analizę ryzyka w zakresie zagrożeń dla praw i wolności** podmiotów danych w związku z powierzanymi czynnościami?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
13.		Czy opracowano i wdrożono **dokumentację** ochrony danych opisującą zasady przetwarzania i zabezpieczania danych osobowych (np. polityka ochrony danych – art. 24 RODO), lub inną dokumentację określającą procedury standardy, dobre praktyki itp., która będzie miała zastosowanie do przetwarzania powierzonych danych osobowych)? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	

	13.1.	*Czy w ciągu ostatnich 12 miesięcy w PP dokonano **przeglądu** pod kątem aktualności i adekwatności ww. dokumentacji ochrony danych osobowych?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
14.		Czy PP prowadzi **rejestr kategorii** czynności przetwarzania (RKCP) zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
	14.1.	*Czy PP zarejestrował w **rejestrze kategorii** czynności przetwarzania (RKCP) proces związany z powierzonymi czynnościami?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
15.		Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych posiadają **upoważnienia** do przetwarzania danych osobowych? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
	15.1.	*Czy osoby, które przetwarzają powierzone dane osobowe zostały upoważnione do przetwarzania danych osobowych?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
	15.2.	*Czy ww. osoby zostały zobowiązane do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
	15.3.	*Czy PP prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
16.		Czy PP wdrożył **procedurę gwarantującą realizację praw** osób, których dane dotyczą? (w tym art. 5, 6, 7,12-22 RODO) Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
17.		Czy PP postępuje zgodnie z zasadą „**privacy by design" i „privacy by default**"? (art. 25 RODO)? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	

18.		Czy poza dokumentacja ochrony danych osobowych PP wdrożył środki organizacyjne zapewniające zdolność do ciągłego zapewnienia **poufności, integralności, dostępności** i odporności systemów i usług przetwarzania? (art. 5, 32 RODO; SKZ) Jeżeli TAK, proszę zaznaczyć, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	☐ dokumentacja bezpieczeństwa informacji, obejmująca w szczególności bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo osobowe i bezpieczeństwo teleinformatyczne ☐ dokumentacja ciągłości działania, w tym PCD i procedury odtworzeniowe ☐ dokumentacja dot. zarządzania usługami ☐ dokumentacja dot. zarządzania jakością ☐ przydzielone role i odpowiedzialność wewnątrz organizacji w zakresie zapewnienia bezpieczeństwa informacji, w tym zarzadzania incydentami ☐ przydzielone role i odpowiedzialność wewnątrz organizacji w zakresie utrzymania ciągłości świadczonych usług ☐ dedykowane kanały i ścieżki komunikacji/współpracy wewnętrznej i zewnętrznej w obszarze bezpieczeństwa informacji ☐ dedykowane kanały i ścieżki komunikacji/współpracy wewnętrznej i zewnętrznej w obszarze ciągłości działania ☐ regularne monitorowanie (przeglądy) i doskonalenie wdrożonych środków/zabezpieczeń ☐ podstawowe zasady bezpieczeństwa, w tym zasada czystego biurka/zasada czystego ekranu ☐ okresowe szkolenia dla pracowników z zakresu bezpieczeństwa informacji ☐ okresowe szkolenia dla pracowników z zakresu utrzymania ciągłości działania ☐ inne (jakie?) ……
19.		Czy PP wdrożył środki zapewniające zdolność do szybkiego **przywrócenia dostępności danych** osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? (art. 32, 33 RODO; SKZ) Jeżeli TAK, proszę zaznaczyć, jakie?	☐ TAK ☐ NIE	☐ dokumentacja ciągłości działania, w tym PCD i procedury odtworzeniowe

		Jeżeli NIE, proszę wyjaśnić dlaczego?		☐ procedury/instrukcje zarządzania incydentami/ postępowania w sytuacji naruszenia ochrony danych osobowych ☐ ewidencja/rejestr incydentów zw. z bezpieczeństwem informacji ☐ ewidencja/rejestr naruszeń ochrony danych osobowych ☐ inne (jakie?) ……
20.		Czy PP wdrożył procesy umożliwiające **regularne testowanie**, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetrwania? (art. 32 RODO; SKZ) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
21.		Czy PP wdrożył środki zapewniające ochronę danych w czasie ich **przekazywania**? (art. 5 RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
22.		Czy PP wdrożył środki zapewniające **minimalizacje danych** (art. 5 RODO; SKU)? Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
23.		Czy PP wdrożył środki zapewniające **odpowiednią jakość danych** (art. 5 RODO; SKU)? Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
24.		Czy PP wdrożył środki zapewniające **ograniczone przechowywanie danych**? (art. 5 RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	

25.		Czy PP wdrożył środki zapewniające **rozliczalność**? (art. 5 RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
26.		Czy PP wdrożył środki umożliwiające **przenoszenie danych i zapewnienie ich usuwalności**? (art. 17; 20; RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
27.		Czy PP jest przygotowany do **poddania się audytowi** prowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych? (art. 28 ust. 3 lit. h RODO) Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
28.		Czy w ostatnich 12 miesiącach PP realizował umowę powierzenia ? Jeżeli NIE, proszę przejść do pytania nr 29	☐ TAK ☐ NIE	
	28.1.	*Czy w ostatnich 3/6/12 miesiącach, do PP, w ramach funkcjonującej umowy powierzenia, trafiły jakieś żądania osób fizycznych z art. 12-22 RODO?* *Jeżeli TAK, to czy Administrator został o tym poinformowany i w jaki sposób?*	☐ TAK ☐ NIE	
	28.2.	*Czy PP pomagał Administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw wynikających z RODO?* *Jeżeli TAK, proszę opisać w jaki sposób.*	☐ TAK ☐ NIE	
	28.3.	*Czy PP spełnił obowiązek informacyjny z art. 13 lub art. 14 RODO wobec osób, których dane są przetwarzane w związku z powierzeniem danych?* *Jeżeli TAK, proszę dołączyć stosowna klauzulę informacyjną oraz przekazać dokumentację potwierdzającą spełnienie tego obowiązku.*	☐ TAK ☐ NIE	
ZASOBY – Zabezpieczenia fizyczne obszaru przetwarzania danych				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			

29.		Czy PP wdrożył środki służące zapewnieniu **bezpieczeństwa fizycznego** miejsc, w których przetwarzane są dane osobowe? (art.32 RODO; SKU) Jeżeli TAK, proszę zaznaczyć, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	☐ procedury bezp. fizycznego/kontroli dostępu, w tym polityka/procedura zarządzania kluczami ☐ ogrodzone budynki i teren przyległy, zapory, szlabany ☐ fizyczne zabezpieczenia wejść i okien do budynków/pomieszczeń ☐ wydzielone strefy bezpieczeństwa ☐ dokumentacja zawierająca dane osobowe przechowywana w zamykanych pomieszczeniach/meblach biurowych; ☐ podstawowa kontrola dostępu do budynku (ochrona, portiernia itp.); ☐ dodatkowa kontrola dostępu do pomieszczeń (czytnik kart magnetycznych, kod do drzwi, „kołowrotki" itp.); ☐ monitoring wizyjny budynku; ☐ monitoring wizyjny piętra, na którym przechowywane są powierzone dane; ☐ system sygnalizacji włamania i napadu; ☐ system sygnalizacji pożaru; ☐ dźwiękowy system alarmowy/ostrzegawczy ☐ system klimatyzacji ☐ czujniki pomiaru wilgotności/temperatury etc. ☐ zapasowa lokalizacja na wypadek sytuacji kryzysowej ☐ inne (jakie?) ……...
30.		Czy PP korzysta z **usług zewnętrznych firm sprzątających/ochroniarskich** lub innych, które dla realizacji swoich obowiązków muszą mieć zapewniony dostęp do obszaru przetwarzania danych osobowych? Jeżeli TAK, czy dostęp tych osób do obszaru przetwarzania danych osobowych został uregulowany w sposób gwarantujący poufność przetwarzanych danych?	☐ TAK ☐ NIE	

	30.1.	*Czy obszar objęty monitoringiem został oznaczony za pomocą odpowiedniej ikonografiki, a osobom wchodzącym na teren objęty monitoringiem są przekazywane informacje o przetwarzaniu ich danych osobowych?*	☐ TAK ☐ NIE	
31.		Czy pracownicy zostali zobowiązani do **niszczenia dokumentów/innych nośników** zawierających dane osobowe przy użyciu niszczarek lub w inny sposób nie pozwalają na odtworzenie dokumentu w łatwy sposób?	☐ TAK ☐ NIE	
32.		Czy PP korzysta z usług wyspecjalizowanych podmiotów zajmujących się niszczeniem nośników papierowych zawierających dane osobowy ?	☐ TAK ☐ NIE	
ZASOBY – ŚRODKI TECHNICZNE (OPROGRAMOWANIE I SPRZĘT)				
LP.		**PYTANIE**	**ODPOWIEDZ**	**UZASADNIENIE/DODATKOWE WYJAŚNIENIA**
p. I	**p. II**			
33.		Czy PP wdrożył środki umożliwiające **identyfikację i autoryzację użytkowników**, w tym poprzez proces nadawania, przeglądu i odbierania uprawnień? (art. 5, 32 RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
34.		Czy PP wdrożył środki dotyczące **zarządzania wewnętrznym systemem IT i bezpieczeństwem IT**? (art. 32 RODO; SKU) Jeżeli TAK, proszę zaznaczyć, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	☐ oprogramowanie posiadające aktualne licencje ☐ regularnie aktualizowany system operacyjny ☐ regularnie aktualizowane oprogramowanie AV ☐ oprogramowanie antyspamowe ☐ oprogramowanie anti-malware ☐ Firewall ☐ DLP ☐ IDS ☐ IPS ☐ EDR ☐ XDR

				☐ SIEM/zarządzanie podatnościami ☐ SPF/DMARC ☐ DMZ ☐ zabezpieczenia anti-ransomware ☐ segmentacja sieci LAN ☐ logiczne odseparowanie sieci gościnnej od sieci korporacyjnej ☐ zabezpieczona sieć wewnętrza (hashowanie, identyfikacja adresu MAC, inne – jakie?) ☐ hardening systemów/aplikacji ☐ zabezpieczone sieci bezprzewodowe (Wi-Fi); ☐ regularny backup danych ☐ oprogramowanie pozwalające na bezpieczne przechowywanie kluczy logowania do różnych systemów przez użytkowników (menadżery haseł etc.); ☐ wieloskładnikowe uwierzytelnienie (MFA) ☐ urządzenia mobilne (np. telefony), na których przetwarzane są dane powierzone posiadają skonfigurowaną kontrolę dostępu? ☐ klucze U2F ☐ zespół CERT/CSIRT (całodobowy/w określonych godzinach?) ☐ Operacyjne Centrum Bezpieczeństwa - SOC (całodobowy/w określonych godzinach?) ☐ UPS/agregaty prądotwórcze ☐ VPN ☐ synchronizacja czasu w systemach i urządzeniach

				☐ szyfrowanie danych w spoczynku (np. na dyskach/nośnikach wymiennych) ☐ szyfrowanie danych w tranzycie ☐ przetwarzanie w chmurze ☐ dedykowane osoby/zespół do nadzoru nad bezpieczeństwem IT – bieżący monitoring systemów i aplikacji, ruchu sieciowego ☐ formalny proces zarządzania uprawnieniami IT ☐ regularne przeglądy uprawnień do systemów IT ☐ regularne testowanie systemów i aplikacji pod kątem podatności ☐ analiza logów ☐ rozwiązania ograniczające komunikację ze znanymi złośliwymi adresami IP (czarna lista) ☐ rozwiązania ograniczające dostęp do zaufanych stron (biała lista) ☐ wdrożone zasady wykonywania, przechowywania, weryfikacji i niszczenia kopii bezpieczeństwa danych ☐ wdrożone zasady konserwacji i napraw sprzętu; ☐ wdrożone zasady korzystania ze sprzętu służbowego udostępnianego pracownikom; ☐ wdrożone zasady zabezpieczenia sprzętu służbowego i/lub urządzeń przydzielanych pracownikom wynoszonych poza obszar przetwarzania danych osobowych ☐ wdrożone zasady bezpieczeństwa informacji podczas transportu; ☐ zabezpieczone data center/serwerownie (wzmożona kontrola dostępu, AC, czujniki ruchu, pomiar temperatury/wilgotności, system pożarowy etc.)

				☐ wdrożona polityka zmiany haseł; ☐ wdrożone środki zabezpieczające (organizacyjno-techniczne) umożliwiające prowadzenie bezpiecznej pracy zdalnej, jeśli zadania są realizowane w formie pracy zdalnej; ☐ wdrożone zasady korzystania z poczty elektronicznej przez pracowników; ☐ zakaz wykorzystywania zasobów służbowych do celów prywatnych; ☐ BYOD ☐ inne (jakie?) ……
	34.1.	*Czy PP powołał lub wyznaczył Administratora Systemów Informatycznych (ASI) lub inną osobę, która opiekuje się infrastrukturą i siecią u PP z technicznego punktu widzenia?* *Jeżeli NIE, proszę wyjaśnić dlaczego?*	☐ TAK ☐ NIE	
35.		Czy PP wdrożył środki umożliwiające **pseudonimizację i szyfrowanie** danych osobowych? (art. 32 RODO; SKZ) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
36.		Czy PP wdrożył środki umożliwiające **rejestrowanie zdarzeń**? (art. 5; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
37.		Czy PP wdrożył środki służące do **konfiguracji systemu**, w tym konfiguracji domyślnej? (art. 32 RODO; SKU) Jeżeli TAK, proszę wymienić, jakie? Jeżeli NIE, proszę wyjaśnić dlaczego?	☐ TAK ☐ NIE	
38.		Czy pracownicy zostali zobowiązani do **szyfrowania** powierzonych danych osobowych przesyłanych drogą elektroniczną (np. raportowanie)? (art. 32 RODO)	☐ TAK ☐ NIE	

		Jeżeli NIE, proszę wyjaśnić dlaczego?		

……..

Data i podpis osoby sporządzającej listę kontrolną

FORMULARZ ZGŁOSZENIA NARUSZENIA BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA nr ……./rok[4]

1. Data i godzina zgłoszenia			
2. Źródło zgłoszenia			
2.1 Imię i nazwisko Zgłaszającego			
2.2 Stanowisko		2.3 Numer telefonu/adres email (służbowy)	
2.5 Nazwa podmiotu[5]			
3. Opis potencjalnego naruszenia bezpieczeństwa informacji/ utraty ciągłości działania			
Proszę pokrótce opisać okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia bezpieczeństwa informacji / utratę ciągłości realizacji usług świadczonych na rzecz UMWP			

[4] Uzupełnia kierownik DO-B lub osoba przez niego wskazana

[5] W przypadku zgłoszeń od zleceniobiorców oraz innych i podmiotów zewnętrznych wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów informacyjnych Urzędu