**Umowa Powierzenia Przetwarzania Danych Osobowych**

zawarta w […], dnia […] r. pomiędzy:

**Toruńską Agencją Rozwoju Regionalnego S.A.** z siedzibą w Toruniu przy ul. Włocławska 167, wpisaną przez Sąd Rejonowy VII Wydział Gospodarczy w Toruniu do Krajowego Rejestru Sądowego pod numerem KRS 000006071, NIP: 956-00-15-177, REGON: 870300040, kapitał zakładowy: 33 290 000,00 zł, wpłacony w całości,

reprezentowaną przez:

……………………………………… - …………………………….

w dalszej części niniejszej Umowy zwaną „**Administratorem**”,

a

………………………………………………………

reprezentowanym przez: […]

w dalszej części niniejszej Umowy zwanym „**Przetwarzającym**”,

dalej łącznie zwanymi „**Stronami**”.

Mając na uwadze, że:

1. Strony, w związku z zakończonym postępowaniem o udzielenie zamówienia publicznego zawarły w dniu .. umowę na ***Wykonanie aplikacji internetowej generatora wniosków wraz z systemem obsługi Wnioskodawcy oraz zaprojektowanie i wdrożenie serwisu www w ramach projektu Fundusz Eksportowy dla Kujaw i Pomorza*** (dalej „Umowa Podstawowa”),
2. w związku, z wykonywaniem Umowy Podstawowej Administrator powierza Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą Umową (dalej „Umowa”);
3. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora;
4. Strony, zawierając Umowę, dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej **RODO**;
5. Na użytek niniejszej Umowy przyjmuje się definicje określone w art. 4 RODO,

Strony niniejszym postanawiają, co następuje:

**§ 1 Przedmiot Umowy**

1. Administrator oświadcza, że jest administratorem danych w rozumieniu art. 4 pkt 7 RODO w związku z realizacją Projektu pn. Fundusz Eksportowy dla Kujaw i Pomorza (dalej **Projekt**), którego celem jest zwiększenie zdolności eksportowej przedsiębiorstw z sektora MŚP z województwa kujawsko-pomorskiego, promocja gospodarcza regionu, poprzez promocję marek regionu oraz wzrost kompetencji MŚP w zakresie internacjonalizacji, i jest uprawniony do powierzenia przetwarzanych danych osobowych przetwarzanych w związku z realizacją Projektu innym podmiotom.
2. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętych Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
3. Na warunkach określonych niniejszą Umową oraz Umową Podstawową, które stanowią udokumentowane polecenie przetwarzania danych, w rozumieniu art. 28 ust. 3 lit. a) RODO, Administrator powierza Przetwarzającemu przetwarzanie dalej opisanych danych osobowych a Przetwarzający zobowiązuje się przetwarzać dane osobowe w sposób zapewniający spełnienie wymogów określonych w RODO, jak również w innych przepisach, mających zastosowanie do przetwarzania powierzonych danych i obowiązujących w trakcie realizacji Umowy.
4. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Podmiot przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
5. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
6. Charakter i cel przetwarzania, a także kategorie osób oraz zakres danych osobowych powierzonych do przetwarzania, wynikają z Umowy Podstawowej i zostały określone w ***Załączniku nr 1*** do niniejszej Umowy

**§ 2 Obowiązki Przetwarzającego**

1. Przetwarzający zobowiązany jest przetwarzać dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.
2. Przetwarzający oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej, czyli poza Europejski Obszar Gospodarczy („**EOG**”). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują dane poza EOG. W przypadku gdyby Przetwarzający miał zamiar lub obowiązek przekazywać dane poza EOG zobowiązany jest do uprzedniego poinformowania o tym zamiarze Administratora, w celu umożliwienia mu podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.
3. Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Przetwarzający zobowiązuje się do uprzedniego odebrania od osób, które zostaną upoważnione do przetwarzania danych w wykonaniu Umowy, udokumentowanych zobowiązań do zachowania tajemnicy, ewentualnie zobowiązany jest zapewnić, że osoby gwarantują zachowanie poufności z uwagi na podleganie ustawowemu obowiązkowi zachowania tajemnicy.
5. Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, stosownie do postanowień Umowy, zapewniając wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych spełniało wymogi RODO i chroniło dane przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem, w tym między innymi:
   1. Pseudonimizację i szyfrowanie danych,
   2. Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   3. Zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   4. Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych;
   5. Zdolność do zarządzania okresem retencji danych, z uwzględnieniem bezwzględnych wymogów prawnych okresu ich archiwizacji;
   6. Techniczną zdolność do identyfikacji i aktualizacji poszczególnego rekordu Danych przetwarzanego w ramach zbioru.
6. Minimalne wymogi dla zapewnienia bezpieczeństwa danych zawiera ***załącznik nr 2*** do niniejszej umowy, przy czym Przetwarzający, jako podmiot profesjonalnie zajmujący się przetwarzaniem danych, zapewnia stałe ocenianie wdrożonych środków organizacyjnych i technicznych oraz ich bieżące dostosowywanie do występujących zagrożeń.
7. Na żądanie Administratora, w całym okresie obowiązywania Umowy, Przetwarzający okaże Administratorowi stosowne dokumenty, certyfikaty, wykazy lub inne dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
8. Przetwarzającyprzestrzegawarunków korzystania z usług innego podmiotu przetwarzającego (Podwykonawcy) stosownie do postanowień § 6 Umowy.
9. Przetwarzający zobowiązuje się pomagać Administratorowi w odpowiadaniu na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („**Prawa jednostki”**).
10. Przetwarzający współpracuje z Administratorem przy wykonywaniu przez niego obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO, w  szczególności w zakresie ochrony danych, zgłaszania naruszeń organowi nadzorczemu, zawiadamiania osób dotkniętych naruszeniem ochrony danych, oceną skutków dla ochrony danych oraz uprzednimi konsultacjami z organem nadzorczym.
11. Jeżeli Przetwarzający poweźmie wątpliwości, co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości. Przekazanie informacji o stwierdzonej wątpliwości następuje drogą pisemną i wymaga uzasadnienia. Strony uzgadniają, że niedopełnienie obowiązków określonych w zakresie powyższego informowania, skutkować będzie utratą możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
12. Przetwarzający, po zakończeniu świadczenia usług związanych z przetwarzaniem, usuwa lub zwraca Administratorowi wszelkie dane osobowe, w zależności od decyzji Administratora oraz usuwa wszelkie ich istniejące kopie, chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
13. Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je bez zbędnej zwłoki Administratorowi. Strony ustalają maksymalny czas tego zgłoszenia na 24 godziny od stwierdzenia naruszenia. Zgłoszenie odbywa się na dane kontaktowe wskazane w par. 11 pkt. 4 Umowy. Przetwarzający umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o wszelkich ustaleniach, dotyczących naruszenia z chwilą ich dokonania. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją, dotyczącą naruszenia, pozwalającą Administratorowi spełnić obowiązki wynikające z RODO, w szczególności w zakresie wykonania analizy ryzyka naruszenia praw i wolności osób fizycznych, których naruszenie dotyczyło.
14. Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i  ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach, w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany, w opinii Administratora, grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.
15. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.
16. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru kategorii czynności przetwarzania (wymóg art. 30 ust. 2 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr kategorii czynności przetwarzania danych w imieniu Administratora.
17. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

**§ 3 Obowiązki Administratora**

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości, co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

**§ 4 Prawo kontroli**

* + - 1. Administrator kontroluje sposób przetwarzania powierzonych danych osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli z minimum czternastodniowym wyprzedzeniem. Administrator lub wyznaczone przez niego osoby są uprawnione do:

1. wstępu do pomieszczeń, w których przetwarzane są dane osobowe,
2. wglądu do dokumentacji związanej z przetwarzaniem danych osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania danych osobowych, ich bezpieczeństwa oraz udostępnienia rejestru kategorii czynności przetwarzania.
   * + 1. Przetwarzający współpracuje z Urzędem Ochrony Danych Osobowych w zakresie wykonywanych przez niego zadań.
       2. Przetwarzający:
   1. Udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,
   2. Umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.
      * 1. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 14 dni.
        2. Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

**§ 5 Bezpieczeństwo danych**

1. Przetwarzający przeprowadza własne analizy ryzyka przetwarzania powierzonych przez Administratora danych oraz współpracuje z Administratorem przy przeprowadzaniu takich analiz, a także stosuje się do wyników tych analiz, co do organizacyjnych i technicznych środków ochrony danych.
2. Przetwarzający przedstawi Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i  dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

**§ 6 Dalsze powierzenie danych do przetwarzania**

**oraz transfer danych do krajów trzecich**

1. Przetwarzający może powierzyć dane objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy, po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w § 6 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Przetwarzającego w niniejszej Umowie.
4. Przetwarzający nie ma prawa przekazać Podwykonawcy całości wykonania Umowy.
5. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
6. Listę zaakceptowanych przez Administratora podwykonawców na dzień podpisania niniejszej Umowy zawiera *załącznik nr 3* do niniejszej umowy.

**§ 7 Odpowiedzialność Przetwarzającego**

1. Przetwarzający jest odpowiedzialny za udostępnienie lub inne wykorzystanie danych niezgodnie z  treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania Danych osobom nieupoważnionym.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych:
   1. o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego tych danych,
   2. w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych.
3. Przetwarzający odpowiada za szkody spowodowane swoim działaniem lub zaniechaniem przy realizacji niniejszej umowy, w szczególności za niedopełnienie obowiązków, wynikających z niniejszej Umowy oraz obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.

**§ 8 Czas obowiązywania Umowy**

Umowa zostaje zawarta na czas obowiązywania Umowy Podstawowej.

**§ 9 Rozwiązanie umowy**

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Przetwarzający:
   1. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   2. przetwarza dane w sposób niezgodny z Umową;
   3. powierzył przetwarzanie danych innemu podmiotowi bez zgody Administratora.
2. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do:
   1. usunięcia danych,
   2. usunięcia wszelkich ich istniejących kopii lub zwrotu danych, chyba, ·że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie danych.
3. Strony uzgodnią sposób usunięcia danych odrębnym dokumentem w ciągu maksymalnie 7 dni   
   od zakończenia Umowy.
4. Po wykonaniu zobowiązania, o którym mowa w ust. 3 powyżej, Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

**§ 10 Zasady zachowania poufności**

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („**dane poufne**”).
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Przetwarzający zobowiązuje się poinformować o obowiązkach wynikających z niniejszej Umowy wszystkie osoby, w tym w szczególności pracowników, audytorów, doradców, podwykonawców, ekspertów, które z uwagi na udział w realizacji niniejszej Umowy, będą miały styczność z danymi poufnymi i zobowiązać te osoby, przed udostępnieniem im danych poufnych, na piśmie do przestrzegania zasad zachowania poufności informacji co najmniej w takim samym zakresie, jak określony w niniejszej Umowie.
4. Jakiekolwiek przekazywanie bądź ujawnianie osobom trzecim danych poufnych dopuszczalne jest tylko za uprzednim pisemnym zezwoleniem Administratora.
5. W przypadku nieuprawnionego wykorzystania, przekazania lub ujawnienia danych poufnych przez Przetwarzającego, Administrator uprawniony jest do żądania od Przetwarzającego zapłaty kary umownej w wysokości 10.000,00 zł (słownie: dziesięć tysięcy złotych 00/100) za każdy przypadek nieuprawnionego wykorzystania, przekazania lub ujawnienia danych poufnych. Zapłata kary umownej wskazanej powyżej nie ogranicza prawa Administratora do dochodzenia od Przetwarzającego odszkodowania na zasadach ogólnych, w przypadku gdy wysokość poniesionej szkody przewyższa zastrzeżoną w niniejszej Umowie wysokość kary umownej.

**§ 11 Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.
4. Ze strony Administratora osobami do kontaktów w sprawie realizacji Umowy są:

…………….... adres poczty elektronicznej: ……………………………………...

………………. adres poczty elektronicznej: ……………………………………

1. Ze strony Przetwarzającego osobami do kontaktów w sprawie realizacji Umowy są:

……………....adres poczty elektronicznej: ……………………………………...

………………..adres poczty elektronicznej: ……………………………………

1. Zmiana danych dotyczących osób do kontaktu, wskazanych w ust. 4 i 5 powyżej nie jest traktowana jako zmiana warunków Umowy.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Administrator | Przetwarzający |

Załącznik nr 1

**Charakter i cel przetwarzania, a także kategorie osób oraz zakres danych osobowych powierzonych do przetwarzania**

* + - 1. Przetwarzający będzie przetwarzał dane wyłącznie w celu realizacji Umowy Podstawowej, którym jest zaprojektowanie i wdrożenie aplikacji internetowej, składającej się z serwisu www wraz z systemem zarządzania, generatora wniosków aplikacyjnych, systemu obsługi bonów płatniczych.
      2. Przetwarzanie obejmować będzie w szczególności następujące czynności: utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, łączenie, pobieranie, przeglądanie, przesyłanie, kopiowanie, dopasowywanie lub łączenie, ograniczanie, usuwanie.
      3. Przetwarzający będzie przetwarzał:

1. dane pracowników i współpracowników Administratora oraz pracowników i współpracowników Partnerów Administratora, niezbędne do korzystania z wdrożonej aplikacji, w szczególności: imię, nazwisko, stanowisko, adres poczty elektronicznej, numer telefonu, numer PESEL, dane dotyczące realizowanych czynności w systemie.
2. dane potencjalnych uczestników oraz uczestników Projektu w zakresie: dane identyfikujące osoby fizyczne, takie jak imię i nazwisko, adres, adres poczty elektronicznej, firma i adres, login, numer telefonu, numer faksu, numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), numer identyfikacji podatkowej (NIP), numer w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON) lub inne identyfikatory funkcjonujące w danym państwie, forma prawna prowadzonej działalności, forma własności mienia tej osoby, płeć, wiek, wykształcenie, identyfikatory internetowe.

**Załącznik nr 2**

**Minimalne wymogi dla zapewnienia bezpieczeństwa danych**

System, którego dotyczy Umowa Podstawowa musi posiadać mechanizm autoryzacji wymagający podania loginu i hasła. System musi zostać zabezpieczony przed podatnościami aplikacji internetowych takimi jak: „Sql Injection”, „xss”, „Broken Authentication”. W celu zapewnienia bezpieczeństwa komunikacja pomiędzy przeglądarką internetową, a serwerem aplikacyjnym będzie odbywać się za pomocą szyfrowanego połączenia z wykorzystaniem zaufanych certyfikatów SSL. Zabezpieczenie kryptograficzne nie może być niższe niż TLS 1.2. W celu zabezpieczenia infrastruktury zostanie wykorzystany: firewall aplikacyjny, IPS/IDS, WAF, ochronę przed atakami DDoS, system antywirusowy i antymalware. W Generatorze będą przetwarzane dane osobowe. W związku z powyższym narzędzie musi być zgodne z aktualnie obowiązującymi przepisami o ochronie danych osobowych. Przetwarzający powinien zapewnić i udokumentować spełnienie wymogów Privacy by default, Privacy by design.

**1. System zarządzania bezpieczeństwem**

Przetwarzający powinien posiadać wdrożony system zarządzania bezpieczeństwem informacji (SZBI).

W zakresie usługi hostingowej powinien posiadać certyfikat ISO: 27001.

Przetwarzający powinien posiadać opracowaną Politykę Bezpieczeństwa Informacji wraz z procedurami i instrukcjami, opisującymi wprowadzone rozwiązania z zakresu bezpieczeństwa informacji , w tym danych osobowych. Polityka powinna być aktualizowana przynajmniej raz w roku oraz każdorazowo w przypadku pojawienia się istotnych zmian mających wpływ na jej zawartość.

Przetwarzający powinien posiadać odpowiednie zasoby kadrowe, gwarantujące efektywne wykonywanie działań zmierzających do zapewnienia ochrony danych, takie jak: Inspektor Ochrony Danych, Administrator Systemów Informatycznych , Risk Manager, koordynujący zarządzanie ryzykiem w zakresie bezpieczeństwa oraz powiązanymi planami działań, Security Measures Manager, który wdraża i wykorzystuje stosowne mechanizmy w związku ze zidentyfikowanymi zagrożeniami.

**2. Audyty**

Przetwarzający powinien zapewnić wykonywanie regularnych audytów SZBI oraz rozliczalność z ich wykonywania.

**3. Audyty realizowane przez Administratora**

W trakcie obowiązywania umowy (eksploatacji systemu), Przetwarzający powinien umożliwić Administratorowi przeprowadzanie audytów technicznych, w tym testów penetracyjnych w odniesieniu do poszczególnych elementów zarządzania usługą.

**4. Zarządzanie sytuacjami związanymi z ryzykiem**

Przetwarzający powinien dysponować opracowaną i wdrożoną formalną metodologią zarządzania sytuacjami związanymi z ryzykiem, która jest weryfikowana przynajmniej raz w roku lub w przypadku pojawienia się istotnych zmian. Metodologia ta powinna dotyczyć również danych osobowych, w tym danych szczególnej kategorii w rozumieniu RODO oraz spełniać wymogi RODO w tym zakresie. W szczególności Przetwarzający powinien umieć wykazać formalnie przeprowadzoną analizę, gdzie zostały zidentyfikowane zasoby, krytyczne procesy, zagrożenia i podatności przy przetwarzaniu powierzonych danych osobowych.

**5. Zarządzanie zmianami**

Przetwarzający powinien posiadać wdrożoną formalną procedurę zarządzania zmianami, w której w szczególności:

* Jasno zdefiniowano role i zakresy odpowiedzialności;
* Określone zostały kryteria klasyfikacji służące identyfikacji etapów, jakie należy realizować podczas wprowadzania zmiany;
* Stosowane są zasady zarządzania priorytetami; realizowana jest analiza ryzyka związanego ze zmianami;
* Przeprowadzane są testy penetracyjne (jeśli dotyczy); zmiana jest planowana i programowana z Administratorem (jeśli dotyczy powierzonych danych);
* Wdrożenie jest realizowane stopniowo (1/10/100/1000) a, w przypadku ryzyka, przewidziana jest procedura powrotu do poprzedniego stanu;
* Realizowany jest przegląd poszczególnych zasobów, których dotyczy zmiana.

**6. Polityka rozwoju systemów i aplikacji**

Przetwarzający zapewnia wprowadzenie stosownych, udokumentowanych procedur, opisujących zasady bezpiecznego rozwoju, środki „privacy by design” i „Privacy by default” oraz politykę przeglądu kodu (wykrywanie podatności, obsługa błędów, zarządzanie dostępem i rekordami, bezpieczeństwo przechowywania i komunikacji). Przetwarzający powinien zapewnić:

* Przeprowadzanie regularnych przeglądów kodu;
* Zatwierdzanie nowych funkcjonalności przed ich wdrożeniem, testy walidacyjne w środowisku oraz stopniowe wdrażanie (1/10/100/1000);
* Podział ról i odpowiedzialności programistów oraz osób odpowiedzialnych za produkcję.

**7. Monitoring usług i infrastruktury systemu IT**

Przetwarzający powinien zapewnić bieżące monitorowanie systemu IT ,w tym:

* Wykrywanie awarii związanych z działaniem usługi i bezpieczeństwem danych;
* Kontrolę funkcji krytycznych i wysyłanie komunikatów ostrzegawczych do osób nadzorujących funkcjonowanie systemu;
* Powiadomienie osób odpowiedzialnych i wszczęcie odpowiednich procedur;
* Zagwarantowanie ciągłości działania usługi w odniesieniu do działań zautomatyzowanych;
* Zapewnienie integralności monitorowanych zasobów.

**8. Zarządzanie incydentami**

Przetwarzający powinien posiadać wdrożony proces zarządzania awariami, pozwalający zapobiegać, wykrywać i radzić sobie z awariami mającymi miejsce w infrastrukturach zarządzania usługą, jak i w ramach samej usługi. Procesy te powinny podlegać procedurze stałego ulepszania w zakresie nadzoru, ewaluacji, jak również zarządzania incydentami oraz działaniami naprawczymi.

W zakresie incydentów dotyczących danych osobowych Przetwarzający powinien posiadać opracowaną procedurę niezwłocznego powiadamiania Administratora o incydentach oraz zapewnić wsparcie w wyjaśnianiu jego okoliczności, tak aby Administrator mógł się wywiązać z obowiązków wynikających z RODO w tym zakresie (analiza przyczyn oraz ryzyka dla praw i wolności osób fizycznych).

**9. Zarządzanie podatnościami**

Przetwarzający powinien zapewnić opiekę technologiczną w odniesieniu do nowych podatności, które powinny być identyfikowane na bieżąco dzięki:

* Informacyjnym stronom WWW;
* Ostrzeżeniom twórców i producentów wdrożonych rozwiązań;
* Incydentom oraz obserwacjom przekazywanym przez zespoły eksploatacyjne Przetwarzającego, osoby trzecie lub klientów;
* Regularnie przeprowadzanym wewnętrznym i zewnętrznym skanom podatności;
* Audytom technicznym, jak również przeglądom kodu i konfiguracji.

Przetwarzający powinien zapewnić, że jeśli nowa podatność zostanie wykryta, wyznaczone do tego celu osoby przeprowadzą analizę, mającą na celu określenie jej wpływu na system IT oraz potencjalne scenariusze działań.

W razie konieczności, Przetwarzający zapewni, że zastosowane zostaną środki podnoszące poziom bezpieczeństwa, a następnie opracowany zostanie plan działań naprawczych.

Przetwarzający powinien zapewnić, że każdy wdrożony środek bezpieczeństwa zostanie włączany do planów działań oraz będzie kontrolowany i formalnie monitorowany, a następnie regularnie weryfikowany w celu ponownego oszacowania skuteczności.

**10. Zarządzanie ciągłością działania**

Przetwarzający zapewni stosowanie różnorodnych mechanizmów, zapewniających ciągłość działania systemu IT w tym dostępność sprzętu (w części dotyczącej hostingu w ścisłej współpracy z hostingodawcą na podstawie zawartych umów) aplikacji i procesów eksploatacyjnych:

Przetwarzający, we współpracy z hostingodawcą (jeśli dotyczy), zapewni stosowanie innych mechanizmów, takich jak kopie bezpieczeństwa, konfigurację sieci i urządzeń, w celu zapewnienia przywrócenie usługi w przypadku incydentu.

Przetwarzający zapewni wykonywanie kopii w systemie 3/2/1.

**11. Zagrożenia naturalne i środowiskowe**

Przetwarzający zapewni wprowadzenie odpowiednich środków, mających na celu przeciwdziałanie zagrożeniom naturalnym i środowiskowym, takim jak pożary, powodzie, adekwatnie do zidentyfikowanych ryzyk w tym obszarze.

**12. Ogólne środki bezpieczeństwa w obiektach fizycznych**

Przetwarzający zapewni, że fizyczny dostęp do obiektów, w których przetwarzane będą dane osobowe, będzie możliwy tylko dla osób uprawnionych, w oparciu o rozwiązania takie, jak:

* Polityka dotycząca praw dostępu (karty dostępu, polityka kluczy)
* Mechanizmy wykrywania obecności (monitoring wizyjny, czujniki ruchu, ochrona fizyczna);
* Wejścia chronione, kontrolowane za pomocą czytników kart dostępu;
* Mechanizmy antywłamaniowe.

**13. Podnoszenie świadomości i szkolenie pracowników**

Przetwarzający zapewni regularne szkolenie personelu w zakresie bezpieczeństwa danych (szkolenia nowych pracowników, szkolenia okresowe, kampanie testowe w celu upewnienia się, że wszyscy pracownicy reagują w sposób adekwatny w sytuacji zagrożenia).

**14. Kontrola logicznego dostępu do systemów informacyjnych**

Przetwarzający zapewni, że wdrożona została rygorystyczna polityka zarządzania logicznymi dostępami pracowników do systemu IT:

* Uprawnienia przyznawane i monitorowane, zgodnie z zasadą najmniejszego uprzywilejowania oraz zasadą stopniowego zdobywania zaufania;
* Uprawnienia przypisywane do pełnionych ról, a nie indywidualnych osób;
* Zarządzanie prawami dostępu oraz uprawnieniami przypisanymi do użytkownika lub systemu realizowane w oparciu o procedurę rejestracji, modyfikacji i anulacji;
* Weryfikowanie tożsamości użytkowników przed każdą zmianą w metodach uwierzytelnienia;
* Ograniczenie możliwości resetowania haseł pracowników w przypadku utraty hasła,
* Wdrożona rygorystyczna polityka dotycząca haseł; generatory haseł, podwójne metody uwierzytelniania,
* Zdalny dostęp do systemu realizowany poprzez rozwiązanie typu VPN wymagające wprowadzenia hasła znanego tylko użytkownikowi oraz klucza współdzielonego skonfigurowanego w stacji roboczej.

**15. Kontrola dostępu do Panelu klienta (Administratora)**

Przetwarzający zapewni dostęp do Panelu klienta realizowany za pośrednictwem imiennego konta (identyfikator klienta) oraz hasła:

* Hasło wybrane przez klienta musi spełniać kryteria złożoności określone w interfejsie użytkownika;
* Na serwerach przechowywane będą jedynie skróty haseł (ang. hash);
* Weryfikacja dwuetapowa w Panelu klienta z wykorzystaniem systemu jednorazowych haseł (OTP) wysyłanych w wiadomościach SMS, aplikacji mobilnej lub kompatybilnego klucza U2F.
* Ograniczenie dostęp do Panelu klienta tylko do wcześniej określonych adresów IP;
* Wszystkie działania klientów w Panelu klienta lub API będą rejestrowane;

**16. Bezpieczeństwo stanowisk pracy i bezpieczeństwo sprzętu mobilnego**

Przetwarzający zapewni, że wdrożone zostały środki bezpieczeństwa dotyczące standardowych stanowisk roboczych pracowników i współpracowników Przetwarzającego:

* Automatyczne zarządzanie aktualizacjami;
* Instalacja i aktualizacja programu antywirusowego oraz regularne skanowanie; instalacja aplikacji pochodzących wyłącznie z zatwierdzonego katalogu;
* Systematyczne szyfrowanie dysków twardych;
* Brak uprawnień administracyjnych dla pracowników w odniesieniu do ich stanowisk roboczych;
* Procedura postępowania względem potencjalnie zagrożonego stanowiska roboczego;
* Standaryzacja sprzętu;
* Procedura usuwania sesji oraz resetowania stanowisk roboczych po odejściu pracownika z firmy.

**Zabezpieczanie urządzeń mobilnych**

Przetwarzający zapewni, że zostały wdrożone środki bezpieczeństwa mające na celu ochronę urządzeń mobilnych pracowników i współpracowników Przetwarzającego, takie jak:

* obowiązkowa rejestracja urządzeń w centralnym systemie zarządzania przed łączeniem się z zasobami wewnętrznymi Zleceniobiorcy (WiFi, poczta e-mail, kalendarze, książki adresowe, etc.);
* weryfikacja polityki bezpieczeństwa zastosowanej w urządzeniu (kod do odblokowywania, czas, po którym następuje blokada, szyfrowanie przechowywanych treści) ;
* procedura zdalnego czyszczenia urządzeń w przypadku kradzieży lub zgubienia.

**17. Bezpieczeństwo sieci**

Przetwarzający zapewni, że wszystkie wykorzystywane urządzenia są zabezpieczone przy użyciu następujących środków: firewall aplikacyjny, IPS/IDS, WAF, ochrona przed atakami DDoS, licencjonowane systemy antywirusowy i antymalware.

**18. Zarządzanie ciągłością działania**

Przetwarzający zapewni wdrożenie polityki prowadzenia rejestrów serwerów i urządzeń używanych do świadczenia usługi dla Administratora:

* Wszystkie systemy oraz dane niezbędne do zapewnienia ciągłości usług, do rekonstrukcji systemu informacyjnego lub do przeprowadzenia analizy po zaistniałej awarii będą zapisywane (pliki baz danych technicznych i administracyjnych, dzienniki aktywności, kody źródłowe aplikacji, ustawienia serwerów, aplikacji i sprzętu, itd.);
* Częstotliwość, czas oraz sposoby przechowywania kopii zapasowych zdefiniowane zgodnie z potrzebami każdego zapisanego zasobu; proces tworzenia kopii monitorowany i objęty systemem zarządzania ostrzeżeniami i błędami.

**19. Prowadzenie rejestrów**

Przetwarzający zapewni wdrożenie polityki prowadzenia rejestrów serwerów i urządzeń używanych do świadczenia usług dla Administratora:

* Kopie zapasowe i scentralizowane przechowywanie dzienników;
* Wgląd do logów oraz ich analiza przez ograniczoną liczbę upoważnionych osób zgodnie z polityką przyznawania uprawnień i zarządzania dostępami;
* Lista działań objętych obowiązkiem prowadzenia rejestrów:
* Logi serwerów kopii zapasowych, na których hostowane są dane;
* Logi maszyn zarządzających infrastrukturą Administratora;
* Logi maszyn do monitoringu infrastruktury;
* Logi programów antywirusowych;
* Kontrola integralności logów i systemów, jeśli dotyczy;
* Zadania i zdarzenia realizowane przez Administratora w jego infrastrukturze;
* Logi i alerty o wykryciu włamania do sieci,
* Logi urządzeń sieciowych;
* Logi maszyn administratora;
* Logi serwerów czasu;
* Logi czytników kart dostępu.

**Załącznik nr 3**

**Lista zaakceptowanych przez Administratora podmiotów przetwarzających**

|  |  |
| --- | --- |
| Dane Podmiotu (nazwa, forma działania, adres, nr NIP, dane kontaktowe) | Zakres usługi |
|  |  |
|  |  |
|  |  |