Znak postępowania: 9/INFO/60PLUS/POWER/2021

Załącznik nr 8 do SWZ

UMOWA O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

zawarta dnia ……..r. w Białymstoku, pomiędzy:

Białostocką Fundacją Kształcenia Kadr z siedzibą w Białymstoku przy ul. Spółdzielczej 8, 15-441 Białystok, wpisaną do rejestru przedsiębiorców oraz rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego pod numerem KRS: 0000037027, legitymującą się NIP: 5422098509, REGON: 050503972, reprezentowaną przez:

1. Bogusława Plawgo – Prezesa Zarządu,
2. Michała Skarzyńskiego – Członka Zarządu,

zwaną dalej w treści umowy **Zamawiającym**

a, ……

zwanym dalej **Wykonawcą**

Zamawiający i Wykonawca w dalszej części umowy łącznie mogą być zwani **Stronami.**

§ 1

1. Niniejsza Umowa zostaje zawarta na okres **od dnia …….. r. do dnia ……. r**. na czas realizacji: „**Usługi opracowania informatycznego w zakresie opracowania internetowych narzędzi do realizacji zadań merytorycznych w projekcie „Praca60plus: interdyscyplinarny model przedłużenia aktywności zawodowej pracowników w wieku emerytalnym realizowany w obszarze ergonomii, elastyczności i walidacji środowisk pracy”** .
2. **Zamawiający** oświadcza, że zgodnie z Rozporządzeniem 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 (zwanym dalej "RODO") administratorem danych osobowych jest Minister Właściwy do spraw rozwoju regionalnego pełniący funkcję Instytucji Zarządzającej dla Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, mający swoją siedzibę przy ul. Wspólnej 2/4 Warszawa, a Zamawiający jest podmiotem podprzetwarzającym dane osobowe, które są przetwarzane przy wykorzystaniu Usługi („Dane Osobowe”). Szczegółowy opis rodzaju Danych Osobowych oraz kategorie osób, których Dane Osobowe dotyczą znajduje się w Załączniku nr 1.
3. Strony zawały umowę nr **……..**, która stanowi integralną część niniejszej umowy.

§ 2

1. Wykonawca w związku z realizacją zadania, o jakim mowa powyżej, będzie uzyskiwał dostęp do danych osobowych beneficjentów w Projekcie.
2. Zamawiający oświadcza, iż Dane Osobowe zostały pozyskane i są przetwarzane przez niego zgodnie z obowiązującymi przepisami prawa, w tym zgodnie z RODO.
3. Zamawiający potwierdza w szczególności, że:
    a. zebrał i posiada wymagane przepisami zgody,

b. przekazał osobom, których dane dotyczą informacje o przetwarzaniu ich danych w zakresie i w sposób wymagany przez RODO,
c. jest uprawniony do przetwarzania Danych Osobowych i powierzenia ich do przetwarzania Wykonawcy w zakresie i celu określonym w Załączniku nr 1 do Umowy.

4. Jeśli Zamawiający nie jest administratorem Danych Osobowych, potwierdza, że uzyskał wymaganą przepisami RODO zgodę właściwego administratora na powierzenie ZAMAWIAJĄCEMU dalszego przetwarzania Danych Osobowych w takim celu i zakresie.
5. Zamawiający potwierdza, że techniczne i organizacyjne środki wdrożone przez WYKONAWCĘ, określone w Załączniku nr 2, są odpowiednie i wystarczające dla ochrony praw osób, których Dane Osobowe dotyczą, i uznaje, że WYKONAWCA zapewnia wystarczające gwarancje w tym zakresie.
6. Niezależnie od powyższego, WYKONAWCA zobowiązuje się, zgodnie z zasadami Umowy, do korzystania z Usługi w sposób bezpieczny i zgodny z prawem, w tym do odpowiedniego zabezpieczenia danych uwierzytelniających do Konta Zamawiającego zapewnienia bezpieczeństwa Danych Osobowych podczas przekazywania ich do Usługi, podejmowania odpowiednich działań mających na celu bezpieczne szyfrowanie lub tworzenie we własnym zakresie kopii zapasowych Danych Osobowych podpowierzonych Wykonawcy oraz ochrony Danych Osobowych przed nieuprawnionym dostępem osób trzecich.

§ 3

1. Wykonawca zobowiązuje się przetwarzać pozyskane dane osobowe wyłącznie w celu wykonania umowy, o jakiej mowa na wstępie.
2. Wykonawca zobowiązuje się zapoznać z treścią Załącznika nr 5 do umowy o dofinansowanie zawartej przez Instytucję Zarządzającą z Zamawiającym, w celu przyjęcia do wiadomości zakresu danych do przetwarzania.

§ 4

1. Wykonawca zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Wykonawca zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Wykonawca zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Wykonawca zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w danej firmie, jak i po ustaniu stosunku pracy.
5. Wykonawca po zakończeniu świadczenia usług związanych z przetwarzaniem, zobowiązany jest do przechowywania danych osobowych po zakończeniu umowy o

powierzenie danych osobowych do dnia wskazanego w paragrafie 6 załącznika nr 6 (wzór projektowane postanowienia umowy) w celu kontroli.

6. W miarę możliwości Wykonawca pomaga Zamawiającemu w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Wykonawca po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Zamawiającemu, niezwłocznie w ciągu 24 h.

§ 5

1. Zamawiający zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Wykonawcę przy przetwarzaniu i zabezpieczeniu podpowierzonych danych osobowych spełniają postanowienia umowy.
2. Zamawiający realizować będzie prawo kontroli w godzinach pracy Wykonawcy i z minimum 3 dniowym jego uprzedzeniem. W przypadku niezależnej od Wykonawcy niemożliwości przeprowadzenia Kontroli w planowanym terminie lub innych niespodziewanych przeszkód, Wykonawca powiadomi Zamawiającego o takich okolicznościach i zaproponuje nowy termin Audytu, nie później jednak niż w ciągu 7 dni od terminu wskazanego przez Zamawiającego.
3. Wykonawca zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Zamawiającego, nie dłuższym niż 5 dni.
4. Wykonawca udostępnia Zamawiającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Kontrola może odbyć się za pośrednictwem niezależnego audytora pod warunkiem zawarcia z Wykonawcą stosownej umowy zachowania poufności.
6. Zamawiający zobowiązuje się, że jako upoważniony audytor nie zostanie wyznaczony podmiot prowadzący pośrednio lub bezpośrednio działalność konkurencyjną w stosunku do działalności prowadzonej przez Wykonawcę. Przez działalność konkurencyjną rozumie się każdą działalność, odpłatną lub nieodpłatną, w kraju lub za granicą, niezależnie od formy prawnej, która jest prowadzona w tym samym lub takim samym zakresie przedmiotowym i skierowana do tego samego kręgu odbiorców, pokrywająca się – chociażby częściowo – z zakresem działalności podstawowej lub ubocznej Wykonawcy lub podmiotów z grupy Wykonawcy na świecie. Dla oceny czy dany podmiot jest konkurencyjny, brany pod uwagę będzie nie tylko przedmiot działalności takiego podmiotu wynikający z treści umowy lub innego dokumentu stanowiącego podstawę jego funkcjonowania, ale również przedmiot działalności faktycznie wykonywanej przez ten podmiot. W przypadku zlecenia przeprowadzenia Audytu podmiotom konkurencyjnym w stosunku do Wykonawcy, jest on uprawniony do odmowy przeprowadzenia Audytu do czasu wyznaczenia innego Wykonawcy Audyt w imieniu Zamawiającego lub do czasu ustalenia dalszego sposobu postępowania pomiędzy Wykonawcą a Zamawiającym.
7. Kontrola podlega następującym warunkom:
    a. może dotyczyć jedynie Danych Osobowych powierzonych do przetwarzania Wykonawcy na podstawie Umowy i będzie ograniczony do siedziby Wykonawcy i urządzeń służących do przetwarzania Danych Osobowych oraz personelu zaangażowanego w czynności przetwarzania objęte zakresem Umowy,

b. będzie prowadzona sprawnie i tak szybko jak to jest możliwe,
c. będzie odbywać się nie częściej niż raz w roku, chyba że Kontrola jest wymagana zgodnie z wymogami prawa lub przez właściwy organ nadzorczy, bądź też ma miejsce niezwłocznie po stwierdzeniu istotnego naruszenia Danych Osobowych przetwarzanych na podstawie Umowy,
d. może być wykonywana w zwykłych godzinach pracy Wykonawcy, w sposób nie zakłócający działalności gospodarczej Wykonawcy i zgodnie z politykami bezpieczeństwa Wykonawcy,
e. Zamawiający ponosi wszelkie koszty wynikające z lub poniesione w związku z Kontrolą, z wyjątkiem przypadków, w których ujawnione zostanie poważne naruszenie zasad bezpieczeństwa Danych Osobowych, dotyczące lub zagrażające Danym Osobowym Zamawiającego
f. Kontrola nie może zmierzać ani prowadzić do ujawnienia tajemnic prawnie chronionych (w tym tajemnicy przedsiębiorstwa Wykonawcy) Zamawiający jest zobowiązany do utworzenia raportu podsumowującego wraz ustaleniami z Kontroli. Raport zostanie przekazany Wykonawcy i będzie stanowić informacje poufne o Wykonawcy, które nie mogą być ujawniane stronom trzecim bez pisemnej zgody Wykonacy, chyba że wymaga tego obowiązujące prawo.

§ 6

1. Wykonawca jest zobowiązany do przetwarzania Danych Osobowych wyłącznie zgodnie z poleceniami przekazanymi przez Zamawiającego, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego stanowi inaczej. W tym drugim przypadku stosuje się §4 ust.6 Umowy.
2. Polecenia Zamawiającego znajdują się w Umowie oraz Umowie o Świadczenie Usługi lub są zlecane odrębnie. Zamawiający jest zobowiązany zapewnić, że wszelkie polecenia przekazywane Wykonawcy są zgodne z obowiązującymi przepisami o ochronie danych osobowych.
3. Wszelkie dalsze polecenia, które wykraczają poza polecenia określone w ust. 2 powyżej, muszą dotyczyć przedmiotu Umowy lub Umowy o Świadczenie Usługi. Jeżeli wdrożenie dalszych poleceń skutkuje kosztami dla Wykonawcy, poinformuje on Zamawiającego o takich kosztach wraz z wyjaśnieniem wysokości kosztów przed wykonaniem polecenia. Po potwierdzeniu przez Zamawiającego, że poniesie on koszty wykonania polecenia oraz po ich zapłacie, Wykonawca jest zobowiązana do realizacji dalszego polecenia pod warunkiem, że pozwalają na to możliwości techniczne i organizacyjne. Zamawiający udziela dalszych poleceń na piśmie, chyba że pilny charakter lub inne szczególne okoliczności uzasadniają udzielenie poleceń w formie elektronicznej. Polecenia w formie innej niż pisemna powinny być niezwłocznie odpowiednio udokumentowane.
4. Wykonawca niezwłocznie informuje Zamawiającego, jeżeli jego zdaniem polecenie narusza RODO lub inne przepisy prawa powszechnie obowiązującego Unii Europejskiej lub państwa członkowskiego i zwraca się do Zamawiającego o wycofanie, zmianę lub potwierdzenie kwestionowanego polecenia. W oczekiwaniu na decyzję Wykonawca jest uprawniony do zawieszenia wykonania kwestionowanego polecenia. W przypadku, w którym wykonanie polecenia Zamawiającego mimo złożenia wyjaśnień prowadziłoby do naruszenia powszechnie obowiązujących przepisów prawa Unii Europejskiej lub

państwa członkowskiego, Wykonawca jest uprawniony do wstrzymania się od realizacji tego polecenia.

5. Wykonawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Wykonawcę danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Wykonawcy, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez Wykonawcę tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO),. Niniejszy ustęp dotyczy wyłącznie danych osobowych podpowierzonych przez Zamawiającego.

§ 7

Wykonawca zobowiązuje się do podjęcia wszelkich kroków służących zachowaniu poufności przez pracowników mających dostęp do danych osobowych, danych osobowych w tajemnicy.

§ 8

1. Wykonawca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy, po uzyskaniu uprzedniej pisemnej zgody Zamawiającego. Zgoda Zamawiającego jest także wymagana przy przypadku umowy podpowierzania kolejnym podwykonawcom przez podwykonawcę. Lista podwykonawców stanowi Załącznik nr 3.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Zamawiającego danych chyba, że obowiązek taki nakłada na Wykonawcę prawo Unii lub prawo państwa członkowskiego, któremu podlega Wykonawca. W takim przypadku przed rozpoczęciem przetwarzania Wykonawca informuje Zamawiającego 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 ust. 1 powyżej, powinien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Wykonawcę w niniejszej Umowie.
4. Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 9

1. Umowa zostaje zawarta na czas obowiązywania Umowy głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy głównej skutkuje rozwiązaniem niniejszej Umowy.
2. Zamawiający jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Wykonawca nie podjął środków zabezpieczających, o których mowa w art. 32-36 RODO, a także w sytuacji, gdy Wykonawca nie stosował się do wymogów przewidzianych w Rozporządzeniu.
3. Każdej ze Stron przysługuje prawo rozwiązania niniejszej Umowy w trybie natychmiastowym, w przypadku naruszenia postanowień niniejszej Umowy przez drugą Stronę Umowy.

§ 10

Wszelkie spory wynikłe na gruncie niniejszej umowy Strony zobowiązują się rozstrzygać polubownie, a w przypadku braku osiągnięcia porozumienia poddają je rozstrzygnięciu właściwego sądu w Białymstoku.

§ 11

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. Integralną część Umowy stanowią:
   Załącznik nr 1: „Opis przetwarzania Danych Osobowych";
   Załącznik nr 2: Instrukcja Zarządzającego z Zamawiającym, w celu przyjęcia do wiadomości zakresu danych do przetwarzania
   Załącznik nr 3: Załącznik nr 3 – Lista podwykonawców Wykonawcy

Zamawiający **Wykonawca**

Załącznik 1 – Opis przetwarzania Danych Osobowych

1. Cel przetwarzania powierzonych Danych

Dane Osobowe będą przetwarzane przez Wykonawcę w celu realizacji usługi polegającej na realizacji **usługi opracowania informatycznego w zakresie opracowania internetowych narzędzi do realizacji zadań merytorycznych w projekcie „Praca60plus: interdyscyplinarny model przedłużenia aktywności zawodowej pracowników w wieku emerytalnym realizowany w obszarze ergonomii, elastyczności i walidacji środowisk pracy**„

2. Charakter i czynności przetwarzania

Przetwarzanie przez Wykonawcę będzie miało charakter niezautomatyzowany.

3. Kategorie osób, których dotyczą dane

Zamawiający podpowierza Wykonawcy przetwarzanie Danych Osobowych następujących kategorii osób:

- Uczestników projektu

Co do zasady, Usługa nie jest przeznaczona do przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, danych osobowych dotyczących wyroków skazujących i naruszeń prawa o których mowa w art. 10 RODO, ani też danych osobowych dzieci. Jednakże, decyzja co do zakresu danych, które Zamawiający przekazuje Wykonawcy w Usłudze należy do Zamawiającego. Decydując się umieścić w usłudze takie dane, Zamawiający potwierdza, że środki zabezpieczeń wdrożone przez Wykonawcę są w jego ocenie wystarczające do ochrony powierzonych Danych Osobowych.

4. Kategorie powierzonych Danych Osobowych

Zamawiający powierza Wykonawcy do przetwarzania następujące kategorie Danych Osobowych: imię, nazwisko, telefon, mail, rok urodzenia, nawa firmy, nazwa stanowiska i wyniki ankiet psychologicznych, ergonomicznych, kompetencyjnych.

Załącznik nr 2.

I. Bezpieczeństwo obszaru przetwarzania

1. Ustalono minimalny zakres stosowania technicznych środków bezpieczeństwa w celu zapewnienia bezpieczeństwa danych osobowych. Rodzaj i zakres stosowanych dodatkowych technicznych środków bezpieczeństwa ustalany jest indywidualnie w zależności od zidentyfikowanych zagrożeń, wymaganego stopnia ochrony i możliwości technicznych.
2. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych poprzez zastosowanie systemów kontroli dostępu, systemu sygnalizacji włamania i napadu, systemu dozoru realizowanego przez pracowników ochrony fizycznej, zamków mechanicznych lub szyfrowych.
3. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed pożarem poprzez zastosowanie drzwi o podwyższonej klasie odporności na ogień.
4. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed zniszczeniem na skutek pożaru lub zalania poprzez zastosowanie systemu alarmu pożarowego oraz systemu sygnalizacji włamania i napadu.
5. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się w celu monitorowania oraz identyfikowania zagrożeń i zdarzeń niepożądanych przez zastosowanie systemu telewizji przemysłowej.

II. Bezpieczeństwo transmisji danych

1. Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych (szyfrowanie danych w tranzycie).
2. Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności poprzez zastosowanie segmentacji sieci teleinformatycznych (segmentacja sieci).
3. Klucze szyfrujące służące do zabezpieczenia teletransmisji danych przechowywane są w bezpiecznym miejscu z zarządzaniem dostępem do nich oraz z wykazaną możliwością odtwarzania klucza.

III. Bezpieczeństwo nośników danych

1. Dane osobowe przechowywane na nośnikach danych w stanie spoczynku zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych. (szyfrowanie danych w spoczynku)
2. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności poprzez zastosowanie fizycznej lub logicznej separacji danych. (separacja danych)
3. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie danych w czasie rzeczywistym. (replikacja danych)
4. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących przyrostowe lub całościowe kopie bezpieczeństwa danych w ustalonym interwale czasowym. (backup danych)

5. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności poprzez zastosowanie mechanizmów i procedur przywracania danych, przełączania źródeł danych oraz odtwarzania kopii bezpieczeństwa danych.
6. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych, przed zainstalowaniem w urządzeniu, zabezpiecza się przed dostępem osób nieuprawnionych poprzez ograniczenie i kontrolę dostępu realizowaną za pomocą szaf pancernych i sejfów.
7. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą poufności danych przez zastosowanie wbudowanych procedur kryptograficznej ochrony danych. (kryptograficzna ochrona nośników danych)
8. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie systemów automatycznego monitoringu działania, wykorzystania pojemności i czasu dostępności.
9. Nośniki danych służące do przetwarzania danych osobowych zabezpiecza się przed niedozwolonym wykorzystaniem poprzez zastosowanie procedur użycia i konfiguracji elementów infrastruktury informatycznej (zarządzanie konfiguracją).
10. Nośniki danych służące do przetwarzania danych osobowych przeznaczone do ponownego wykorzystania zabezpiecza się przed ujawnieniem danych osobie nieuprawnionej lub systemowi informatycznemu poprzez zastosowanie bezpiecznych metod usuwania danych.
11. Nośniki danych służące do przetwarzania danych osobowych przeznaczone do likwidacji zabezpiecza się przed ponownym wykorzystaniem poprzez trwałe i celowe mechaniczne uszkodzenie.

IV. Bezpieczeństwo baz danych

1. Dane osobowe przechowywane w bazach danych zabezpiecza się przed utratą integralności poprzez zastosowanie reguł spójności w zakresie semantycznym (definicja typu danych), zakresie encji (definicja kluczy podstawowych) oraz w zakresie referencyjnym (definicja kluczy obcych).
2. Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu.

V. Bezpieczeństwo infrastruktury informatycznej

1. Dane osobowe zabezpiecza się przed utratą poufności za pomocą bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.
2. Dane osobowe zabezpiecza się przed utratą poufności i dostępności za pomocą monitorowania poprawności działania oraz sposobu użycia bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.
3. Dane osobowe zabezpiecza się przed utratą dostępności poprzez zastosowanie dodatkowych, zapasowych i awaryjnych źródeł zasilania infrastruktury informatycznej służącej do przetwarzania danych osobowych.
4. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych (komputery, serwery, urządzenia sieciowe) zabezpiecza się przed dostępem osób nieuprawnionych oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu.
5. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania.
6. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez zastosowanie oprogramowania typu Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anty DDOS.

7. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie zwielokrotnienia, wirtualizacji i automatycznych procedur skalowania.
8. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie automatycznych procesów monitorowania dostępności, obciążenia i wydajności.
9. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania.

Załącznik nr 3 – Lista podwykonawców Wykonawcy

Podczas świadczenia Usługi, Wykonawca korzysta ze wsparcia spółek z grupy przedsiębiorstw PP oraz zewnętrznych podwykonawców. Podwykonawcy wskazani poniżej świadczą usługi obejmujące niektóre funkcjonalności Usługi (webinary), usługi hostingu i kolokacji, wsparcia w obsłudze Zamawiającego, a także usługi związane ze śledzeniem incydentów bezpieczeństwa, reagowaniem na nie, diagnozowaniem i rozwiązywaniem problemów w Usłudze.

Podwykonawcy	Siedziba