|  |  |
| --- | --- |
| **Umowa powierzenia przetwarzania danych osobowych**  (zwana dalej „Umową”)  zawarta w Warszawie pomiędzy:  **Fundacją Rozwoju Systemu Edukacji** z siedzibą w Warszawie, przy Al. Jerozolimskich 142A, 02‑305 Warszawa, wpisaną do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej – Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy KRS pod nr KRS: 0000024777, posiadającą NIP 5261000645, zwaną dalej „FRSE”, reprezentowaną zgodnie ze swoją reprezentacją przez osobę wskazaną przy podpisie,  a  [Przetwarzający], zwaną/ym w dalszej części Umowy „**Przetwarzającym**”, reprezentowaną/ym przez osobę wskazaną przy podpisie  zwanymi dalej Stronami, a każda z osobna Stroną  o następującej treści:  **§ 1**  **Postanowienia ogólne**   1. Ilekroć Umowa dotyczy podejmowania czynności przetwarzania danych w ramach zadań związanych z wdrożeniem, wykonaniem i rozliczeniem programu: 2. **Erasmus+, SALTO, Europejski Korpus Solidarności** - Administratorem danych osobowych podlegających powierzeniu w ramach Umowy jest Komisja Europejska;   W takiej sytuacji podejmowane procesy przetwarzania danych regulują przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE („**Rozporządzenie 1725**”).  W przypadku określonym powyżej, na podstawie zawartych umów, FRSE uprawniona jest zarówno do przetwarzania danych osobowych jako podmiot przetwarzający jak i do ich dalszego powierzenia na rzecz Przetwarzającego.  b) **POWER: PMU, VET, HE, SE, AE** - Administratorem danych osobowych podlegających powierzeniu w ramach Umowy jest Ministerstwo Funduszy i Polityki Regionalnej;  W takiej sytuacji, przetwarzanie następuje w trybie określonym przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych  i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („**Rozporządzenie**”).  c) **Edukacja-EOG, Polsko-Litewski Fundusz Wymiany Młodzieży (PLFWM), Polsko-Ukraińska Rada Wymiany Młodzieży (PURWM), Krajowy Plan Odbudowy (KPO), Fundusze Europejskie dla Rozwoju Społecznego (FERS)** - Administratorem danych osobowych podlegających powierzeniu w ramach Umowy jest FRSE a przetwarzanie danych następuje zgodnie z przepisami Rozporządzenia.   1. W pozostałych przypadkach FRSE występuje jako administrator danych osobowych uprawniony do określenia celów i sposobu przetwarzania danych a przetwarzanie danych następuje zgodnie z przepisami Rozporządzenia. 2. Realizacja Umowy następuje w związku z wdrożeniem, wykonaniem i rozliczeniem programów Erasmus+ i Europejski Korpus Solidarności zatem w takiej sytuacji Administratorem Danych Osobowych jest Komisja Europejska.   **§ 2**  **Oświadczenia Stron**   1. FRSE oświadcza, że jest Administratorem danych osobowych lub podmiotem przetwarzającym dane osobowe, uprawnionym do podpowierzenia ich przetwarzania w zakresie objętym niniejszą Umową na podstawie upoważnienia udzielonego przez administratora tych danych. 2. Przetwarzający oświadcza, że znane mu są przepisy Rozporządzenia oraz Rozporządzenia 1725 a wszelkie podejmowane przez niego działania są zgodne z obowiązkami wynikającymi z ww. regulacji oraz innych powszechnie obowiązujących przepisów prawa. 3. Przetwarzający oświadcza, że dokonał analizy ryzyka w ramach jego przedsiębiorstwa w związku z realizacją niniejszej Umowy i stosuje adekwatne do występujących zagrożeń naruszenia danych, środki bezpieczeństwa pozwalające na bezpieczne przetwarzanie. W szczególności Przetwarzający oświadcza, że stosowane przez niego środki bezpieczeństwa minimalizują występujące ryzyka naruszenia danych oraz umożliwiają sprawowanie kontroli nad zachodzącymi procesami przetwarzania i ich bezpieczeństwem.   **§ 3**  **Powierzenie przetwarzania danych osobowych**   1. FRSE powierza Przetwarzającemu, dane osobowe do przetwarzania, na zasadach  i w celu określonym w niniejszej Umowie. 2. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową oraz powszechnie obowiązującymi przepisami prawa, w szczególności Rozporządzeniem albo Rozporządzeniem 1725, które chronią prawa osób fizycznych, których dane dotyczą. 3. Dane powierzane w ramach Umowy obejmują następujące kategorie:   1) kategorie osób:   * 1. osoby kontaktowe wskazane we wnioskach o Znak Jakości EKS albo wnioskach do programu coachingowego złożonych do Centrum SALTO EECA w polskiej NA przez organizacje z regionu EECA i Norwegii lub przekazanych przez przedstawiciela SALTO EECA odpowiedzialnego za ten obszar działań,   2. przedstawiciele prawni wskazani we wnioskach o Znak Jakości EKS albo wnioskach do programu coachingowego złożonych do Centrum SALTO EECA w polskiej NA przez organizacje z regionu EECA i Norwegii lub przekazanych przez przedstawiciela SALTO EECA odpowiedzialnego za ten obszar działań   2) kategorie danych:   * 1. imię,   2. nazwisko,   3. nazwa organizacji składającej wniosek,   4. adres e-mail,   5. numer telefonu.   **§ 4**  **Zakres i cel przetwarzania danych**   1. Powierzone przez FRSE dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji umowy  nr **………………….z dnia……………… w przedmiocie:** świadczenie usług polegających naprzeprowadzaniu akredytacji organizacji z krajów Partnerstwa Wschodniego, Federacji Rosyjskiej oraz Norwegii lub innych wskazanych przez KE, ubiegających się o Znak Jakości w ramach EKS; monitoringu organizacji już akredytowanych; realizacji programu coachingowego (wspieranie nowych organizacji z krajów Partnerstwa Wschodniego zainteresowanych uzyskaniem Znaku Jakości EKS) składającego się z serii seminariów i spotkań, przygotowującego do akredytacji Znak Jakości Europejskiego Korpusu Solidarności organizacje w krajach Partnerstwa Wschodniego (**„Umowa Główna”**). 2. Przetwarzający przetwarza powierzone dane wyłącznie w imieniu i na udokumentowane polecenie (w szczególności w odniesieniu do rodzaju, zakresu, miejsca i procedury przetwarzania oraz wysyłania danych do państw trzecich i organizacji międzynarodowych) FRSE i zgodnie z tymi poleceniami oraz postanowieniami zawartymi w niniejszej Umowie, która stanowi polecenie FRSE. Wyjątkiem od powyższego jest jedynie sytuacja w której obowiązek przetwarzania nakłada na Przetwarzającego obowiązujące go prawo Unii lub państwa członkowskiego; w takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje FRSE o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny. 3. Na podstawie niniejszej Umowy, Przetwarzający będzie przetwarzał, dane osobowe wyszczególnione w §3 ust. 3. 4. Przetwarzający uprawniony jest do podejmowania czynności przetwarzania w zakresie: zbierania, wprowadzania, przechowywania, wglądu, organizowania danych, ich usunięcia lub niszczenia. utrwalania, organizowania, porządkowania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania, dopasowywania lub łączenia, ograniczania 5. W przypadku przetwarzania danych w ramach systemów informatycznych udostępnionych Przetwarzającemu przez FRSE, Przetwarzający zobowiązany jest do dokonywania czynności przetwarzania wyłącznie w ramach udostępnionego systemu informatycznego. Przetwarzający nie jest uprawniony do zapisywania danych poza systemem informatycznym FRSE ani ich przesyłania do innych systemów, z wyjątkiem sytuacji gdy przesłanie danych do innego systemu informatycznego związane jest nierozerwalnie z istotą podejmowanej czynności przetwarzania i jest niezbędne do wykonania zobowiązań wynikających z Umowy Głównej. 6. Przetwarzający zobowiązany jest do usunięcia danych otrzymanych od FRSE, o których mowa w § 3 ust. 3,Umowy, niezwłocznie po zakończeniu świadczenia usługi, o której mowa w § 4 ust. 1 Umowy.   **§ 5**  **Obowiązki Przetwarzającego**   1. Przetwarzający zobowiązuje się do prawidłowego zabezpieczenia powierzonych danych osobowych poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzykom związanym  z przetwarzaniem danych osobowych. 2. Stosując środki techniczne zmierzające do zabezpieczenia danych Przetwarzający kieruje się przede wszystkim zasadą minimalizacji czynności przetwarzania danych wymagających realizacji określonego celu oraz dąży do podejmowania czynności przetwarzania w zakresie zapewniającym: 3. pseudonimizacja oraz szyfrowanie danych osobowych; 4. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; 5. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich  w razie incydentu fizycznego lub technicznego; 6. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych  i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. 7. Przetwarzający gwarantuje, że przed rozpoczęciem przetwarzania powierzonych danych, wdrożył techniczne i organizacyjne środki określone w **Załączniku nr 1** do niniejszej Umowy. W przypadku gdy Administratorem danych osobowych powierzanych w ramach Umowy jest Komisja Europejska, Przetwarzający zobowiązuje się dodatkowo do wypełnienia **Załącznika nr 3** do Umowy. Przy wypełnianiu **Załącznika nr 1** oraz **Załącznika nr 3** (jeśli dotyczy) Przetwarzający musi zastosować się do wymagań FRSE. 8. Przetwarzający gwarantuje, że będzie utrzymywał środki wskazane w **Załączniku nr 1** oraz **Załączniku nr 3** (jeśli dotyczy) przez okres obowiązywania Umowy i że będzie monitorował adekwatność tych środków w toku przetwarzania powierzonych danych, zmieniając te środki w przypadku w którym okazałyby się niewystarczające, zgodnie z ust. 4. Zmiana **Załącznika nr 1** oraz **Załącznika nr 3** (jeśli dotyczy) nie wymaga zmiany Umowy, a jedynie zawiadomienia FRSE. 9. Jako że środki techniczne i organizacyjne podlegają postępowi technicznemu, zezwala  się Przetwarzającemu na wdrożenie alternatywnych adekwatnych środków, pod warunkiem, że poziom ochrony przez nie zapewniany nie będzie niższy niż poziom ochrony środków określonych w **Załączniku nr 1** i **Załączniku nr 3** (jeśli dotyczy). Na żądanie FRSE, Przetwarzający wdroży skuteczne środki techniczne i organizacyjne wykraczające poza środki określone, jeżeli środki techniczne i organizacyjne wymienione w **Załączniku nr 1** i **Załączniku nr 3** (jeśli dotyczy) do niniejszej Umowy okażą się niewystarczające lub jeżeli wymagać tego będą postęp techniczny lub zmiany legislacyjne. Jeżeli Przetwarzający ustali, że wdrożone środki są niewystarczające lub że postęp techniczny lub zmiany legislacyjne wymagają szerzej zakrojonej ochrony, poinformuje o tym niezwłocznie – nie później niż w terminie 10 dni roboczych – FRSE. 10. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych, wymaganej od profesjonalisty. 11. Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy. 12. Przetwarzający zobowiązany jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Ponadto Przetwarzający oświadcza, że każda osoba  (np. pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych, inne osoby pracujące na rzecz Podmiotu przetwarzającego), która zostanie dopuszczona  do przetwarzania powierzonych przez Podmiot przetwarzający danych osobowych zostanie zobowiązana do zachowania tych danych w tajemnicy. Zobowiązanie do zachowania tajemnicy określone powyżej obejmuje podmioty, wymienione w niniejszym ustępie 8 po zakończeniu obowiązywania niniejszej Umowy. Postanowienia dotyczące zachowania tajemnicy, o której mowa w niniejszym ustępie, Przetwarzający ma obowiązek stosować odpowiednio także wobec swoich Podwykonawców i osób dopuszczonych przez Podwykonawców  do przetwarzania danych osobowych. 13. W przypadku stwierdzenia naruszenia ochrony danych osobowych lub zaistnienia podejrzenia jego wystąpienia, Przetwarzający zawiadamia FRSE o stwierdzonym lub możliwym naruszeniu bez zbędnej zwłoki, lecz nie później niż w ciągu 24 godzin od stwierdzenia naruszenia  lub wystąpienia podejrzenia jego wystąpienia. Zgłoszenie, o którym mowa w zdaniu poprzedzającym, musi co najmniej zawierać: 14. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii  i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie; 15. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych; 16. opis możliwych konsekwencji naruszenia ochrony danych osobowych; 17. opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków mających na celu zminimalizowania jego ewentualnych negatywnych skutków.   W przypadku nieposiadania wszystkich wskazanych informacji w momencie zgłoszenia, Przetwarzający może wysłać zgłoszenie bez brakujących informacji i następnie – po ich uzyskaniu – wysłać uzupełnienie zgłoszenia niezwłocznie, nie później niż 24 godziny od uzyskania brakujących informacji.  10. Uwzględniając charakter przetwarzania oraz dostępne mu informacje, Przetwarzający pomaga FRSE wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia oraz art. 33-41 Rozporządzenia 1725.  11. W celu uniknięcia wątpliwości poza wynagrodzeniem określonym w Umowie Głównej, Przetwarzającemu nie przysługuje żadne dodatkowe wynagrodzenie z tytułu powierzenia mu przez FRSE przetwarzania danych i wypełniania niniejszej Umowy.  **§ 6**  **Prawo kontroli**   1. FRSE oraz upoważnieni przez FRSE audytorzy mają prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy oraz powszechnie obowiązujących przepisów prawa,  w szczególności Rozporządzenia albo Rozporządzenia 1725. 2. FRSE realizować będzie prawo kontroli w godzinach pracy Przetwarzającego i za minimum 3 dniowym uprzedzeniem. 3. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli  w terminie wskazanym przez FRSE nie dłuższym niż 7 dni, chyba że stwierdzone uchybienia wymagają podjęcia natychmiastowych działań. W takiej sytuacji Przetwarzający niezwłocznie dokona czynności zabezpieczających dane do czasu przywrócenia stanu przetwarzania zgodnego z Umową. 4. Przetwarzający będzie dokumentował spełnianie obowiązków wynikających z niniejszej Umowy. Przetwarzający zobowiązany jest udostępnić FRSE wszelkie informacje oraz dokumenty umożliwiające weryfikację zakresu stosowanych środków zabezpieczających, podejmowane czynności przetwarzania oraz wykazanie spełnienia obowiązków obciążających Przetwarzającego na podstawie powszechnie obowiązujących przepisów prawa,  w szczególności Rozporządzenia albo Rozporządzenia 1725 oraz Umowy niezwłocznie, najpóźniej 3 dni po otrzymaniu żądania od FRSE.   **§ 7**  **Dalsze powierzenie danych do przetwarzania**   1. Przetwarzający będzie powierzał dane osobowe objęte niniejszą Umową do dalszego przetwarzania wyłącznie dalszym podmiotom przetwarzającym „Dalszy podmiot przetwarzający” uprzednio zaakceptowanym przez FRSE w formie pisemnej pod rygorem nieważności i wpisanym na listę zaakceptowanych Dalszych podmiotów przetwarzających stanowiącą Załącznik nr 2 do Umowy. Dotyczy to zarówno podmiotów, którym Przetwarzający powierzył dane na podstawie umowy, jak i dalszych pomiotów, którym dane zostały przekazane przez podmioty, którym Przetwarzający powierzył dane. W tym celu Przetwarzający ma obowiązek zawarcia stosownych postanowień w umowach zawieranych z dalszymi przetwarzającymi. 2. Przetwarzający nie ma prawa przekazać jakichkolwiek danych przetwarzanych na podstawie niniejszej Umowy podmiotowi trzeciemu przed wpisaniem go na listę zaakceptowanych Dalszych podmiotów przetwarzających. 3. Przekazanie powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie FRSE chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje FRSE o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny oraz wdroży wymagane prawem zabezpieczenia aby zapewnić że przekazanie danych będzie wykonane zgodnie z obowiązującymi przepisami. 4. Dalsze podmioty przetwarzające, o których mowa w §7 ust. 1 Umowy winny spełniać  co najmniej te same gwarancje i obowiązki, jakie zostały nałożone na Przetwarzającego  w niniejszej Umowie. 5. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie  się ze spoczywających na Dalszych podmiotach przetwarzających obowiązków ochrony danych.   **§ 8**  **Prawa osób, których dane dotyczą**   1. FRSE jest odpowiedzialna za udzielanie odpowiedzi na wnioski o skorzystanie z prawa przyznanego osobie, której prawa dotyczą na mocy Rozporządzenia oraz Rozporządzenia 1725 („prawa osób, których dane dotyczą”). Przetwarzający może udzielić odpowiedzi na wnioski złożone przez osoby, których dane dotyczą, oraz może poprawiać, zmieniać lub usuwać dane oraz spełniać wszelkie inne żądania osób, których dane dotyczą wyłącznie po wcześniejszym uzyskaniu zgody FRSE. 2. W przypadku, w którym osoba, której dane dotyczą, bezpośrednio kontaktuje się  z Przetwarzającym w celu skorzystania z przyznanych jej praw, Przetwarzający niezwłocznie, nie później niż w terminie 48 godzin od chwili otrzymania żądania, przekaże taki wniosek FRSE oraz będzie postępować zgodnie z instrukcjami otrzymanymi od FRSE. 3. Przetwarzający zobowiązany jest do udzielenia FRSE wsparcia przy udzielaniu odpowiedzi  na wnioski dotyczące korzystania z praw przez osoby, których dane dotyczą, na jego żądanie  i w uzasadnionym zakresie. 4. Powyższe zasady stosuje się odpowiednio w przypadku gdy FRSE lub Przetwarzający otrzymają żądanie organu nadzorczego lub innego organu państwowego dotyczące powierzonych danych lub niniejszej Umowy.   **§ 9**  **Odpowiedzialność Przetwarzającego**   1. Przetwarzający przyjmuje do wiadomości, iż podczas realizacji Umowy w zakresie powierzonych czynności przetwarzania, ponosi odpowiedzialność za wdrożenie właściwych  w stosunku do występującego ryzyka środków technicznych i organizacyjnych oraz zapewnienie przetwarzania zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności Rozporządzenia albo Rozporządzenia 1725. 2. Przetwarzający przyjmuje do wiadomości, iż w związku z realizacją Umowy może być poddany kontroli zgodności przetwarzania danych przez organ nadzorczy sprawujący kontrolę zgodności przetwarzania danych z obowiązującymi przepisami prawa. 3. Przetwarzający zobowiązuje się do niezwłocznego poinformowania FRSE o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, a także o wszelkich planowanych - o ile są wiadome - lub realizowanych kontrolach i inspekcjach dotyczących czynności przetwarzania danych przez Przetwarzającego. 4. Przetwarzający odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały  w związku z nienależytym przetwarzaniem przez niego powierzonych danych osobowych. 5. W przypadku naruszenia obowiązków Przetwarzającego związanych z przetwarzaniem danych osobowych powierzonych mu do przetwarzania na podstawie niniejszej Umowy,  w następstwie którego FRSE zostanie zobowiązana do wypłaty odszkodowania lub ukarana grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Przetwarzający zobowiązuje się do zwrócenia równowartości odszkodowania, kary lub grzywny poniesionych przez FRSE jeżeli naruszenie obowiązków nastąpiło z przyczyn leżących po stronie Przetwarzającego.   **§ 10**  **Czas obowiązywania umowy**  Niniejsza Umowa obowiązuje od dnia jej podpisania przez ostatnią ze Stron przez czas obowiązywania Umowy Głównej.  **§ 11**  **Rozwiązanie umowy**  FRSE 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 osobowe w sposób niezgodny z Umową lub właściwymi przepisami powszechnie obowiązującego prawa, 3. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody FRSE, 4. dopuści się rażącego naruszenia postanowień niniejszej Umowy, 5. jest przedmiotem postępowania wszczętego przez Organ nadzorczy w związku z naruszeniem przez niego ochrony danych osobowych.   **§ 12**  **Zasady zachowania poufności**   1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od FRSE 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 FRSE w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy. 3. Zobowiązania dotyczące poufności obowiązują do momentu rozwiązania Umowy i 5 lat po jej rozwiązaniu.   **§ 13**  **Postanowienia końcowe**   1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron. 2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych, Rozporządzenia oraz Rozporządzenia 1725. 3. Umowę sporządzono w dwóch wersjach językowych – polskiej i angielskiej. W razie rozbieżności, wersja polska jest wiążąca. 4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy FRSE. 5. Wszelkie zawiadomienia, których wymaga niniejsza Umowa wykonywane są na adres e-mail: [adres e-mail] lub za pomocą innych danych kontaktowych wskazanych przez FRSE. 6. Załączniki: 7. Załącznik nr 1 – Środki bezpieczeństwa 8. Załącznik nr 2 - Lista zaakceptowanych dalszych podmiotów przetwarzających, z których usług Przetwarzający ma prawo korzystać przy przetwarzaniu danych osobowych 9. Załącznik nr 3 – Rejestr kategorii czynności przetwarzania Przetwarzającego -  ma zastosowanie w przypadku gdy Administratorem danych jest Komisja Europejska. | **Personal Data Processing Agreement**  (hereinafter referred to as 'the Agreement')  concluded in Warsaw by and between  **The Foundation for the Development of the Education System** seated in Warsaw, Al. Jerozolimskie 142A, (02- 305) Warsaw, Poland, entered in the Register of Associations, Other Social and Professional Organisations, Foundations and Independent Public Health Care Institutions - National Court Register (KRS) kept by the District Court for the City of Warsaw, 12th Business Department of the National Court Register, entry no. KRS: 0000024777, holding taxpayer identification number (NIP) 5261000645, hereinafter referred to as **"FRSE",** represented in accordance with the legal representation indicated at signature,  and  **[Data Processor],** hereinafter referred to as “**Data Processor**” represented in accordance with the legal representation indicated at signature:  hereinafter referred to as Parties, and each separately as a Party  with the following content:  **Article 1**  **General Provisions**   * + - 1. Whenever the Agreement concerns data processing activities as part of tasks related to the launching, implementation and settlement of the  1. **Erasmus+, SALTO, European Solidarity Corps** programme, the European Commission is the controller of personal data entrusted under the Agreement;   In such a situation, the processing of data will be governed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('**Regulation 1725**').  In the case referred to above, on the basis of concluded contracts, FRSE is entitled to process personal data in the capacity as a data processor and to outsource such services to Data Processor.  **b) POWER:** **PMU, VET, HE, SE, AE**  - the Ministry of Development Funds and Regional Policy is the controller of personal data entrusted under the Agreement;  In such a situation, personal data will be processed in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**the Regulation**).  c**) Education-EEA, Polish-Lithuanian Youth Exchange Fund (PLFWM), Polish-Ukrainian Youth Exchange Council (PURWM), National Recovery Plan (NRP), European Funds for Social Development (EFSD**) - The controller of the personal data to be entrusted under the Agreement is FRSE and the processing of the data takes place in accordance with the provisions of the Regulation.   * + - 1. In other cases, FRSE acts as the personal data controller entitled to determine the purposes and manner of data processing, and data processing is carried out with the observance of the provisions of the Regulation.       2. The performance of the Agreement takes place in connection with the implementation, execution and settlement of the Erasmus+ and European Solidarity Corps programmes, and in this situation the European Commission is the Personal Data Controller.   **Article 2**  **Declarations by the Parties**   1. FRSE declares that it is the personal data Controller or processor authorised to entrust its processing within the scope of the Agreement and on the basis of an authorisation granted by the controller of such data. 2. Data Processor declares that it is familiar with the provisions of the Regulation and Regulation 1725 and that all actions taken by it are consistent with the obligations resulting from the above mentioned regulations and other generally applicable legislation. 3. Data Processor declares that it has made risk analysis within its organisation in connection with the performance of the Agreement and it applies security measures adequate to existing risks of data breach, which allow for safe processing. In particular, Data Processor declares that security measures it applies minimise the risks of data breaches and enable it to exercise control over the processing operations and their security.   **Article 3**  **Entrusting Personal Data Processing**   1. FRSE entrusts Data Processor with the processing of personal data in accordance with the rules and for the purpose specified in the Agreement. 2. Data Processor undertakes to process personal data entrusted to it in accordance with the provisions of the Agreement and generally applicable legislation, in particular the Regulation and Regulation 1725, which protect the rights of data subjects. 3. Data entrusted under the Agreement is divided into the following categories:   1) categories of individuals:  a) contact persons identified in ECS Quality Label applications or applications for the coaching programme submitted to the SALTO EECA Resource Center at Polish NA by organisations from the EECA region and Norway or provided by the SALTO EECA representative responsible for that area.  b) legal representatives identified in ECS Quality Label applications or applications for the coaching programme submitted to the SALTO EECA Resource Center at Polish NA by organisations from the EECA region and Norway or provided by the SALTO EECA representative responsible for that area.  2) categories of data:  a) name,  b) surname,  c) name of applicant organization,  d) e-mail address,  e) phone number.  **Article 4**  **Scope and purpose of data processing**   1. Data Processor will process personal data entrusted by FRSE solely for the purpose of performing contract no. **…………………………. of …………………… for** theprovision of services consisting inconducting the accreditation of organisations from the Eastern Partnership countries, the Russian Federation and Norway as well as from other countries named by the EC applying for Quality Label as part of ESC; monitoring of already accredited organisations; carrying out a coaching programme (support to new organisations from the Eastern Partnership countries interested in obtaining the ESC Quality Label) consisting of a series of seminars and meetings to prepare organisations in Eastern Partnership countries for accreditation with the European Solidarity Corps Quality Label("**The** **Main Contract**"). 2. Data Processor shall process the entrusted data only on behalf of and based on recorded instructions (in particular with regard to the type, scope, place and procedure of processing and the sending of data to third countries and international organisations) given by FRSE and in accordance with such instructions and the provisions of this Agreement, which constitutes an instruction of FRSE. The only exception to the foregoing is the situation when an obligation to process is imposed on Data Processor by an applicable EU or Member State law, in which case the Data Processor shall inform FRSE of such a legal obligation before processing commences, unless that law prohibits such information on the grounds of an important public interest. 3. Under the Agreement, Data Processor will process personal data specified in Article 3(3) of the Agreement. 4. Data Processor is entitled to undertake the processing activities including: collecting, entering, storing, inspecting, organising, erasing or destructing, recording, organising, structuring, adapting or modifying, downloading, viewing, using, disclosing by transmitting, disseminating or otherwise making available, matching or linking, restricting data. 5. In the case of data processing within IT systems made available to Data Processor by FRSE, Data Processor is obliged to perform processing activities only within the IT system made available to it. Data Processor is not entitled to save data outside FRSE’s IT system or to transfer it to other systems, except for situations where the transfer of data to another IT system is inseparable from the essence of the processing operation undertaken and is necessary for the performance of the obligations under the Main Contract. 6. Data Processor is obliged to delete data received from FRSE referred to in Article 3(3) of the Agreement immediately after the completion of provision of services referred to in Article 4(1) of the Agreement**.**   **Article 5**  **Data Processor's Obligations**   1. Data Processor undertakes to properly secure personal data entrusted to it by applying appropriate technical and organisational measures that ensure a degree of security corresponding to the risks associated with personal data processing. 2. When applying technical measures aimed at securing data, Data Processor is guided primarily by the principle of minimising data processing activities that require the achievement of a specific purpose and strives to undertake processing activities to the extent that ensures:    1. pseudonymisation and encryption of personal data;    2. capability to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services;    3. capability to quickly restore the availability of and access to personal data in the event of a physical or technical incident;    4. regular testing, measuring and evaluating the effectiveness of technical and organisational measures aimed to ensure the security of processing. 3. Data Processor warrants that it has implemented the technical and organisational measures set out in **Annex 1** to the Agreement prior to the start of processing of the entrusted data. In case the European Commission is the controller of personal data entrusted under the Agreement, the Data Processor undertakes to fill in **Annex 3** to the Agreement. When filling in **Annex 1** and **Annex 3** (if applicable) the Data Processor has to comply with the requirements of FRSE. 4. The Data Processor warrants that it will maintain measures set out in **Annex 1** and **Annex 3** (if applicable) for the duration of the Agreement and that it will monitor the adequacy of these measures in the course of processing the entrusted data, and amend them if they prove insufficient, in accordance with clause (4). An amendment to **Annex 1** and **Annex 3** (if applicable) does not require an amendment to the Agreement, but only a notification sent to FRSE. 5. As technical and organisational measures are subject to technical progress, Data Processor shall be allowed to implement alternative adequate measures, provided that the level of protection provided by them is not lower than the level of protection of the measures set out in **Annex 1** and Annex 3 (if applicable). At the request of FRSE, Data Processor shall implement effective technical and organisational measures over and above those specified if the technical and organisational measures set out in **Annex 1** and **Annex 3** (if applicable) prove insufficient or if technical progress or legislative changes so require. If Data Processor determines that the measures implemented are insufficient or that technical advances or legislative changes require more extensive protection, Data Processor shall inform FRSE about this fact immediately, but not later than within 10 working days. 6. Data Processor undertakes to exercise due diligence when processing entrusted personal data that is required of a professional service provider. 7. Data Processor undertakes to grant authorisations to process personal data to all persons who will process the entrusted data in order to perform the Agreement. 8. Data Processor is obliged to keep the confidentiality of personal data and methods to secure it. Moreover, Data Processor declares that any person (e.g. a full-time employee, a person performing activities on the basis of civil law contracts, other persons working on behalf of Data Processor) who will be allowed to process personal data entrusted by the processor will be obliged to keep the confidentiality of such data. The obligation to keep data confidential specified above will apply to entities referred to in this paragraph for an unlimited period of time, i.e. also after the termination of the Agreement. Data Processor is obliged to apply confidentiality provisions referred to in this paragraph also to its Subcontractors and persons authorised by the Subcontractors to process personal data. 9. In the event of an identified or suspected personal data breach, the Data Processor shall notify FRSE of the identified or suspected breach without undue delay, but not later than within 24 hours after the identification of the breach or the occurrence of the suspected breach. The notification referred to in the preceding sentence must at least contain: 10. a description of the nature of the personal data breach, including, as far as possible, an indication of the category and approximate number of data subjects and the category and approximate number of personal data entries concerned; 11. full name and contact details of a data protection officer; 12. description of possible consequences of the personal data breach; 13. a description of measures taken or proposed to repair personal data breach, including, where appropriate, measures to minimise its possible adverse effects.   In the event of not having all the indicated information at the time of notification, Data Processor may send a notification without the missing information and then, once the information is obtained, send a supplement to the notification immediately, but not later than within 24 hours after obtaining the missing information.   1. Taking into account the nature of the processing and information available to it, Data Processor shall assist FRSE in complying with the obligations set out in Articles 32 to 36 of the Regulation and Articles 33 to 41 of Regulation 1725. 2. For the avoidance of doubt, in addition to the remuneration set out in the Main Contract, Data Processor shall not be entitled to any additional remuneration for being entrusted by FRSE with the processing of data and the performance of the Agreement.   **Article 6**  **Audit Rights**   1. FRSE and the auditors authorised by FRSE shall have the right to verify if measures applied by Data Processor when processing and securing the entrusted personal data comply with the provisions of the Agreement and the generally applicable legislation, in particular the Regulation or Regulation 1725. 2. FRSE will exercise its audit rights during Data Processor's working hours and with a three days' notice at minimum. 3. Data Processor undertakes to remove non-compliance found during the audit within a deadline indicated by FRSE, which will not exceed seven days, unless such non-compliance requires immediate action. In such a situation, Data Processor will immediately take measures aimed at ensuring data security until processing in compliance with the Agreement is restored. 4. Data Processor will document compliance with its obligations under the Agreement. Data Processor is obliged to make available to FRSE all information and documents allowing for the verification of the scope of applied security measures, processing activities undertaken and demonstrating compliance with the obligations imposed on Data Processor on the basis of generally applicable legislation, in particular the Regulation, Regulation 1725 and the Agreement, as soon as possible and no later than within three days after receiving a request from FRSE.   **Article 7**  **Sub-processing**   1. Data Processor will subcontract the processing of personal data covered by the Agreement only to "**Sub-processors**" previously approved by FRSE in writing and entered on the list of approved Sub-processors forming **Annex 2** to the Agreement. This applies both to entities entrusted by Data Processor with the data on a contractual basis and to further entities to which the data has been transferred by entities entrusted by Data Processor. For this purpose, Data Processor is obliged to include appropriate provisions in the contracts concluded with sub-processors. 2. Data Processor does not have a right to transfer any data processed under the Agreement to a third party prior to its entry on the list of approved Sub-processors whose services Data Processor can use in relation to personal data processing. 3. The transfer of entrusted data to a third country or an international organisation can take place only on a written instruction from FRSE, unless such an obligation is imposed on Data Processor by EU law or law of the Member State in which Data Processor is established. In such a case, prior to the commencement of processing, Data Processor shall inform FRSE about such a legal obligation, unless such information is prohibited by law because of important public interest and shall implement the safeguards required by law to ensure that the transfer is carried out in accordance with the applicable legislation. 4. Sub-processors referred to in Article 7(1) of the Agreement will provide at least the same guarantees and meet the same obligations as those imposed on Data Processor in the Agreement. 5. Data Processor shall be fully liable to Data Controller for failure to meet data protection obligations imposed on Sub-processorss.   **Article 8**  **Data subjects’ rights**   1. FRSE is responsible for responding to requests to exercise a right granted to data subjects under the Regulation and Regulation 1725 ("data subject rights"). Data Processor may respond to requests made by data subjects and may correct, amend or erase data and comply with any other requests made by data subjects only with the prior consent of FRSE. 2. In the event that a data subject directly contacts Data Processor in order to exercise his or her rights, the Processor shall promptly, no later than 48 hours after receipt of the request, forward such request to FRSE and follow the instructions received from FRSE. 3. Data Processor is obliged to provide FRSE with support in responding to requests concerning the exercise of rights by data subjects at its request and to the extent reasonably requested. 4. The above rules shall apply *mutatis mutandis* if FRSE or Data Processor receives a request from a supervisory authority or other state authority concerning the entrusted data or this Agreement.   **Article 9**  **Data Processor's Liability**   1. Data Processor acknowledges that during the performance of the Agreement in the scope of processing activities outsourced to it, it is liable for implementing technical and organisational measures appropriate to the risks involved and for ensuring processing in accordance with the provisions of generally applicable legislation, in particular the Regulation and Regulation 1725. 2. Data Processor acknowledges that in connection with the performance of the Agreement, it may be subject to a data processing audit by a supervisory authority, which inspects the compliance of data processing with applicable laws. 3. Data Processor undertakes to immediately inform FRSE about any proceedings, in particular administrative and judicial proceedings, about any administrative decision or ruling concerning data processing, as well as about any planned - if known - or implemented audits and inspections concerning data processing activities by Data Processor. 4. Data Processor will be liable for any damage caused to third parties, which they have suffered in connection with improper processing of personal data entrusted to it. 5. In the event of a breach of obligations committed by Data Processor related to the processing of personal data entrusted to it under the Agreement, as a result of which FRSE will be obliged to pay damages or will be fined by a final judgement or decision of a competent authority, Data Processor undertakes to reimburse the equivalent of the damages or fine incurred by FRSE if the breach of obligations is attributable to Data Processor.   **Article 10**  **Term of the Agreement**  The Agreement is concluded for a definite period of time from the date the last of the two Parties sign till the end of the Main Contract.  **Article 11**  **Termination of the Agreement**  FRSE can terminate the Agreement with immediate effect, if Data Processor:   1. despite the request to remedy the misconduct found during an audit, does not remedy it within the time limit set, 2. processes personal data in a manner, which is non-compliant with the Agreement or relevant provisions of generally applicable legislation, 3. has subcontracted the processing of personal data to another entity without the consent of FRSE, 4. commits a gross breach of the Agreement, 5. is the subject of proceedings brought by a Supervisory Authority for a breach of personal data protection obligation.   **Article 12**  **Confidentiality Clause**   1. Data Processor undertakes to keep the confidentiality of any and all information, data, materials, documents and personal data received from FRSE and its collaborators, as well as data obtained in any other way, whether intended or accidental, in oral, written or electronic form ("confidential data"). 2. Data Processor declares that because of the obligation to keep personal data confidential, such data will not be used, disclosed or made available without written consent of FRSE for any purpose other than the performance of the Agreement, unless the need to disclose information held results from applicable laws or the Agreement. 3. Confidentiality obligations shall apply until the termination of the Agreement and 5 years thereafter.   **Article 13**  **Miscellaneous Provisions**   1. This Agreement has been made in duplicate, one copy for each Party. 2. In matters not regulated herein, the provisions of Polish Civil Code, the Act of 10 May 2018 on personal data protection, the Regulation and Regulation 1725 will apply. 3. The Agreement has been drawn up in two counterparts, in Polish and English language versions, one for each Party. In case of discrepancies the Polish version shall prevail. 4. The court having jurisdiction over FRSE will settle disputes arising from the Agreement. 5. All notices required by this Agreement shall be made to the e-mail address: [adres e-mail] or via other contact details indicated by FRSE. 6. Annexes: 7. Annex 1 - Security measures 8. Annex 2 - List of approved Sub-processors whose services Data Processor can use to process personal data 9. Annex 3 – Record of categories of processing activities – applicable if European Commission is the controller. |
| ***FRSE:***  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Data / date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ***Data Processor/ Przetwarzający:***  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Data / date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| Załącznik nr 1  do umowy powierzenia | Annex 1  to the Personal Data Processing Agreement |
| **Środki bezpieczeństwa**  Prosimy o wskazanie stosowanych środków zabezpieczeń poprzez wskazanie środków z listy przykładowych zabezpieczeń poniżej lub uzupełnienie listy stosowanymi zabezpieczeniami. Stosowane zabezpieczenia powinny odpowiadać ryzyku naruszenia praw lub wolności osób, których dane dotyczą. | **Security measures**  Please indicate the security measures in place by indicating the measures from the list of sample security measures below or by completing the list with the security measures in place. The security measures in place should correspond to the risk of violation of the rights or freedoms of data subjects. |

|  |  |  |
| --- | --- | --- |
| **Środki zastosowane w celu zabezpieczenia danych:/ Measures taken to secure the data:** | | |
| * **Środki organizacyjne/ Organisational measures** |  | **Przeprowadzanie analizy i oceny ryzyka / Carrying out risk analysis and assessment** |
|  | **Nadawanie pracownikom i współpracownikom upoważnień do przetwarzania danych osobowych / Granting authorisations to employees and collaborators to process personal data** |
|  | Pisemne zobowiązanie pracowników/współpracowników do przestrzegania tajemnicy danych i obowiązków w zakresie poufności / Written commitment by employees/co-workers to observe data secrecy and confidentiality obligations |
|  | Regularne szkolenia pracowników w zakresie ochrony informacji, w tym przepisów ochrony danych osobowych / Regular training of employees on data protection, including personal data protection regulations |
|  | Stosowanie zasady minimalizacji i adekwatności danych / Application of the principle of data minimisation and adequacy |
|  | Zapewnienie kontroli nad powierzaniem danych / Ensuring control over entrusted data |
|  | Stosowanie anonimizacji i pseudonimizacji danych / Using anonymisation and pseudonymisation of data |
|  | **Niełączenie urządzeń zawierających dane osobowe z publicznymi sieciami wifi, np. na lotnisku, w hotelu itp. / Not connecting devices containing personal data to public Wi-Fi networks, e.g. at the airport, hotel, etc.** |
|  | **Unikanie przechowywania danych osobowych na pen-drive’ach / Avoiding storing personal data on pen drives** |
|  | **Unikanie drukowania dokumentów zawierających dane osobowe / Avoiding the printing of documents containing personal data** |
|  | **Stosowanie wewnętrznych regulacji (procedur, instrukcji i polityk) / Following internal regulations (procedures, instructions and policies)** |
|  | Wyznaczenie Inspektora Ochrony Danych / Appointing a Data Protection Officer |
|  | Regularne monitorowanie stosowanych zabezpieczeń / Regular monitoring of security measures in place |
|  | Rejestrowanie incydentów bezpieczeństwa informacji oraz monitorowanie prób nieautoryzowanego dostępu / Recording data security incidents and monitoring unauthorised access attempts |
|  | Kontrolowane i skuteczne niszczenie wszystkich danych i nośników danych / Controlled and efficient destruction of all data and data media |
|  | Korzystanie z kwalifikowanych podpisów elektronicznych i/lub podpisów profilem zaufanym ePUAP / Use of qualified electronic signatures and/or ePUAP trusted profile signatures |
|  | inne:………………………………………… / other: …………………………………………………….. |
| * **Środki ochrony fizycznej danych / Physical data protection measures** |  | **Dostęp do pomieszczeń służbowych, w których przetwarzane są dane osobowe, oraz kluczy do tych pomieszczeń, tylko dla osób upoważnionych / Providing access to business premises where personal data is processed and keys to those premises only to authorised persons** |
|  | Zapewnienie kontroli nad przemieszczaniem się osób trzecich w obszarze przetwarzania danych / Ensuring control of the movement of third parties in the data processing area |
|  | Sprzęt i urządzenia zabezpieczające budynek (kamery CCTV, ochrona 24h, kontrola dostępu do budynku, zamknięte drzwi, bramy i okna itp.) / Building security equipment and devices (CCTV cameras, 24-hour security, building access control, locked doors, gates and windows, etc.) |
|  | Zabezpieczenie obszarów, w których przechowywane są nośniki danych, np. zamykanie na klucz pomieszczeń i szaf zawierających dokumenty z danymi osobowymi / Securing areas where data media are stored, e.g. locking rooms and cabinets containing documents with personal data |
|  | Zapewnienie ochrony przeciwpożarowej / Providing fire protection |
|  | inne:………………………………………… / other: …………………………………………………….. |
| * **Środki sprzętowe infrastruktury informatycznej i telekomunika-cyjnej / Measures concerning IT and telecommunications infrastructure hardware** |  | Dostęp do kluczowych elementów infrastruktury teleinformatycznej wyłącznie dla osób upoważnionych / Providing access to key elements of the ICT infrastructure to authorised persons only |
|  | Zapewnienie nadzoru nad drukarkami i skanerami / Providing supervision over printers and scanners |
|  | Stosowanie urządzeń służących do niszczenia danych (niszczarki dokumentów papierowych/ płyt CD/DVD) / Using data destruction equipment (printed document/ CD/DVD shredders) |
|  | Cykliczne monitorowanie nośników kopii zapasowych w zakresie poprawności ich działania / Cyclical monitoring of backup media for their proper operation |
|  | Zapewnienie właściwych warunków klimatyzacyjnych w serwerowni / Ensuring proper air-conditioning conditions in the server room |
|  | Ustawienie ekranu monitora w sposób uniemożliwiający wgląd przez osoby postronne / Positing monitor screens so that it cannot be viewed by outsiders |
|  | Nadzór nad wydawaniem użytkownikom sprzętu teleinformatycznego / Supervising the release of ICT equipment to users |
|  | inne:………………………………………… / other: …………………………………………………….. |
| * **Środki ochrony w ramach systemów i baz danych / Security measures concerning databases and database systems** |  | **Stosowanie silnych haseł uwierzytelniających / Using strong authentication passwords** |
|  | Stosowanie zabezpieczeń kryptograficznych (np. korzystanie z szyfrowanych transmisji, szyfrowanie plików wysyłanych mailem, szyfrowanie danych na nośnikach przenośnych typu pendrive’y, dyski twarde laptopów) / Using cryptographic security features (e.g. using encrypted transmissions, encryption of files sent by e-mail, encryption of data on portable media such as memory sticks, laptop hard drives) |
|  | Stosowanie zabezpieczeń chroniących dane przed szkodliwym oprogramowaniem (antywirus) / Security measures to protect data from malware (anti-virus) |
|  | Zabezpieczenie danych za pomocą kopii zapasowych / Securing data by making back-up copies |
|  | Stosowanie zabezpieczeń chroniących infrastrukturę logiczną sieci komputerowej przed zagrożeniami z zewnątrz (np. firewall, IDS/IPS, filtry URL) / Applying security measures to protect the logical infrastructure of the computer network from external threats (e.g. firewall, IDS/IPS, URL filters) |
|  | Aktualizowanie oprogramowania użytkowego / Regular updating of application software |
|  | Stosowanie indywidualnych kont użytkowników (np. w systemie operacyjnym) / Using individual user accounts (e.g. in the operating system) |
|  | Definiowanie uprawnień użytkowników zgodnie z zakresem obowiązków / Defining user rights in accordance with the scope of their responsibilities |
|  | Zapewnienie kontroli nad tym, kto, kiedy i w jakim zakresie wprowadził dane do systemu informatycznego / Ensuring control over who entered data into the IT system, when and to what extent |
|  | **Używanie funkcji UDW w przypadku wysyłania maili / Using the BCC function when sending emails** |
|  | **Stosowanie wygaszaczy ekranu z opcją hasła włączających się po zdefiniowanym czasie / Using password-controlled screen savers that switch on after a defined period of time** |
|  | Automatyczne blokowanie konta użytkownika po kilkukrotnym wprowadzeniu niewłaściwego hasła / Automatic blocking of user accounts after several incorrect password entries |
|  | inne:………………………………………… / other: …………………………………………………….. |
| * **Inne**.…….(np. ISO 27001)/ **Other** ...................(e.g. ISO 27001) | | |

|  |  |
| --- | --- |
| Załącznik nr 2  do umowy powierzenia | Annex 2  to the Personal Data Processing Agreement |
| **Lista zaakceptowanych dalszych podmiotów przetwarzających, z których usług Przetwarzający ma prawo korzystać przy przetwarzaniu danych osobowych** | **List of approved Sub-processors whose services Data Processor can use to process personal data** |

|  |  |
| --- | --- |
| **Nazwa dalszego podmiotu przetwarzającego (instytucji, firmy) / Name of the subprocessor (institution, company)** |  |
| **Adres / Address** |  |
| **Data powierzenia / Date of entrusting data** |  |
| **Przedmiot / Subject** |  |
| **Cel przetwarzania / Purpose of processing** |  |