**Wzór Umowy powierzenia przetwarzania danych osobowych**

zawarta dnia \_\_\_\_\_\_\_\_\_\_\_\_ pomiędzy:

(zwana dalej „Umową”)

**[x]**

zwanym w dalszej części umowy **„Przetwarzającym”**

reprezentowanym przez:

-------------------------------------------------------

oraz

Fundacją Rozwoju Systemu Edukacji

zwaną w dalszej części umowy **„FRSE”**

reprezentowaną przez:

-------------------------------------------------------

**§ 1**

**Postanowienia ogólne**

1. Ilekroć Umowa dotyczy podejmowania czynności przetwarzania danych w ramach zadań związanych z wdrożeniem, wykonaniem i rozliczeniem programu:
2. **Erasmus+, SALTO, ECVET, eTwinning, Europass, EPALE, Eurydice, 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 umowy zawartej z FRSE jako beneficjentem, 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, SZANSA** - 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) -** Administratorem danych osobowych podlegających powierzeniu w ramach Umowy jest FRSE .

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**

**Oświadczenia Stron**

1. FRSE oświadcza, że jest administratorem danych osobowych oraz 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 naruszenia danych 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 określone w § 1 pkt 1 umowy obejmują następujące kategorie:
4. kategorie osób: uczestnicy wydarzenia,
5. kategorie danych:

• imię i nazwisko

• płeć

• nazwa i adres zamieszkania

• e-mail

• nr telefonu

• wizerunek małoletniego oraz osoby dorosłej

• data urodzenia małoletniego oraz osoby dorosłej

• obywatelstwa

1. Dane będą przekazywane Przetwarzającemu e-mailem, telefonicznie lub za pośrednictwem systemu szkolenia.eks.org.pl. Przetwarzający może także samodzielnie pozyskiwać te dane w toku wykonywania usług na rzecz FRSE.

**§ 4**

**Zakres i cel przetwarzania danych**

1. 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.
2. Powierzone przez FRSE dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji umowy nr ……… z dnia …… w przedmiocie **usługi trenerskiej: przygotowanie i przeprowadzenie szkoleń dla młodzieży i osób pracujących z młodzieżą w kontekście realizacji Projektów Solidarności (ESC30) w Europejskim Korpusie Solidarności w roku 2023.** „Umowa Główna”.
3. Na podstawie niniejszej Umowy, Przetwarzający będzie przetwarzał, dane osobowe wyszczególnione w §3 ust. 3 Umowy.
4. Przetwarzający uprawniony jest do podejmowania czynności przetwarzania w zakresie: przechowywania, wglądu, organizowania danych i ich usunięcia.
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. 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 i będzie je utrzymywał 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 poniżej.
8. 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** do niniejszej Umowy. Na żądanie FRSE, Przetwarzający wdroży skuteczne środki techniczne i organizacyjne wykraczające poza środki określone, jeżeli środki techniczne i organizacyjne wymienione w **Załączniku nr 1** 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.
9. Ust. 3 i ust. 4 nie mają zastosowania w przypadku przetwarzania danych w ramach systemów informatycznych udostępnionych Przetwarzającemu przez 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 5 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.

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:

1. 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;
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych;
3. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4. 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.
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. Dalszy podmiot przetwarzający, o którym mowa w §3 ust. 1 Umowy winien 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 Dalszym podmiocie przetwarzającym 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 i 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 zawarcia przez czas *obowiązywania* Umowy Głównej.

**§ 11**

**Rozwiązanie umowy**

1. FRSE może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Przetwarzający:
2. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
3. przetwarza dane osobowe w sposób niezgodny z Umową lub właściwymi przepisami powszechnie obowiązującego prawa;
4. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody FRSE;
5. dopuści się rażącego naruszenia postanowień niniejszej Umowy;
6. 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. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy FRSE.
4. Załączniki:
5. Załącznik nr 1 – Środki bezpieczeństwa
6. Załącznik nr 2 - Lista zaakceptowanych dalszych podmiotów przetwarzających, z których usług Przetwarzający ma prawo korzystać przy przetwarzaniu danych osobowych

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FRSE Przetwarzający

**Załącznik nr 1**

do umowy

powierzenia

|  |  |
| --- | --- |
| **Pseudonimizacja i szyfrowanie** | |
| Pseudonimizacja  Podmiot przetwarzający zastosuje odpowiednie środki w celu zapewnienia, że w trakcie przetwarzania danych nie będą one mogły zostać przypisane konkretnej osobie bez dodatkowych informacji, a takie dodatkowe informacje przechowywane będą oddzielnie i podlegać będą technicznym i organizacyjnym środkom ochrony. | Szyfrowanie |
| **Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania** | |
| **Kontrola wstępu**  Przetwarzający zobowiązany jest do przedsięwzięcia środków mających na celu uniemożliwienie nieuprawnionym osobom uzyskania dostępu do systemów przetwarzania danych lub dostępu do danych osobowych.  Regulowanie wydawania zezwoleń uprawniających do wstępu dla pracowników, odwiedzających, osób trzecich (zewnętrznych), w tym dokumentacja  Magnetyczne karty dostępu  Urządzenia zamykające drzwi (zamki elektryczne itp.)  Regulamin dotyczący osób trzecich (odwiedzających, klientów, pracowników osób sprzątających, pracowników obsługi technicznej itp.)  Przepustki dla gości/osób trzecich  Identyfikacja zezwoleń uprawniających do wstępu  Ocena zezwoleń uprawniających do wstępu  System alarmowy lub inne odpowiednie środki bezpieczeństwa, w tym działające po godzinach pracy  Zabezpieczenie i ograniczenie punktów dostępu  Sprzęt i urządzenia zabezpieczające budynek (kamery CCTV, ochrona 24h, kontrola dostępu do budynku, zamknięte drzwi, bramy i okna itp.)  Określone bezpieczne obszary ze specjalną kontrolą dostępu („zamknięte obiekty”) | **Kontrola dostępu do danych**  Dla celów kontroli dostępu do danych należy wdrożyć takie środki, które zapewnią, że dostęp do danych osobowych będzie ograniczony do osób posiadających prawo dostępu do tych konkretnych danych. Zapewnia to, że – podczas przetwarzania, użytkowania i po składowaniu – dane osobowe nie będą mogły być przedmiotem nieuprawnionego dostępu, kopiowania, zmian lub usunięcia.  Ustanowienie uprawnień dostępu dla pracowników, w tym odpowiednia dokumentacja  Identyfikacja urządzenia końcowego i/lub użytkownika w systemie Podmiotu przetwarzającego  Automatyczne blokowanie konta użytkownika, które nie było używane przez pewien okres czasu  Utworzenie i bezpieczne przechowywanie numeru identyfikacyjnego użytkownika  Przydzielanie indywidualnych urządzeń końcowych i/lub użytkowników  Zróżnicowane zasady dostępu (np. częściowe blokowanie, precyzyjnie określone role użytkowników lub profile)  Uwierzytelnianie upoważnionego personelu  Zabezpieczenia wprowadzania danych, które mają być przechowywane oraz zabezpieczenia odczytu, blokowania i usuwania danych zapisanych w pamięci  Stosowanie szyfrowania danych krytycznych dla bezpieczeństwa  Identyfikator i hasło użytkownika  Wytyczne dotyczące utworzenia bezpiecznego hasła  Dokumentowanie wykorzystywania danych  Oddzielenie środowiska produkcyjnego i środowiska testowego dla bibliotek i plików  Możliwość zablokowania wejść do obiektów, w których przetwarzane są dane (pomieszczenia, obudowy, sprzęt komputerowy i podobne urządzenia)  Monitorowanie niszczenia nośników danych  Zabezpieczenie obszarów, w których przechowywane są nośniki danych  Udostępnianie nośników danych wyłącznie osobom upoważnionym  Monitorowanie plików, kontrolowane i udokumentowane niszczenie nośników danych  Wytyczne dotyczące tworzenia kopii zapasowych |
| **Kontrola dostępu do serwera**  Przetwarzający zastosuje następujące środki w celu zapobiegania wykorzystywaniu systemów przetwarzania danych bez zezwolenia.  Ustanowienie uprawnień dostępu dla pracowników, w tym odpowiednia dokumentacja  Uprawnienia dostępu dla określonych osób  Regulamin dotyczący osób trzecich (np. dostawców usług IT)  Blokowane urządzenia końcowe  Przydzielanie indywidualnych urządzeń końcowych i/lub użytkowników urządzeń końcowych oraz cech identyfikacyjnych wyłącznie do pełnienia określonych funkcji  Dostęp do urządzeń końcowych i/lub użytkownika ograniczony co do czasu i/lub celu oraz cechy identyfikacyjne  Kod użytkownika do danych i programów  Zróżnicowane zasady dostępu (np. częściowe blokowanie)  Identyfikatory i hasła użytkownika  Wytyczne dotyczące utworzenia bezpiecznego hasła  Automatyczne blokowanie konta użytkownika po kilkukrotnym wprowadzeniu niewłaściwego hasła  Automatyczne blokowanie kont użytkownika, które nie były używane przez pewien okres czasu  Automatyczne blokowanie ekranu po pewnym czasie  Ocena praw dostępu  Rejestrowanie incydentów (monitorowanie prób włamania)  Rejestrowanie i analiza wykorzystania plików  Usuwanie wszelkich usuwalnych danych i nośników elektronicznych (np. notebooków i laptopów, dysków twardych, płyt CD, DVD, pamięci USB, taśm magnetycznych, dyskietek, kart pamięci itp.)  Kontrolowane niszczenie wszystkich danych i nośników danych  Procesy przeglądu i dopuszczania programów  Szyfrowanie danych w przypadku, gdy są one przekazywane online lub przewożone na ruchomych nośnikach danych (np. na notebookach i laptopach, dyskach twardych, płytach CD, DVD, pamięciach USB, taśmach magnetycznych, dyskietkach, kartach pamięci itp.)  Ochrona kanałów komunikacji przed nieuprawnionym dostępem  Ochrona wewnętrznych sieci przed nieuprawnionym dostępem (np. poprzez firewall)  Stosowanie skanerów antywirusowych | **Kontrola przekazywania**  Środki zapewniające, że dane osobowe nie mogą zostać odczytane, skopiowane, zmienione lub usunięte bez zezwolenia podczas ich przekazywania lub przechowywania na nośnikach danych. Należy zapewnić sprawdzanie i określenie planowanych odbiorców przekazania danych osobowych.  Uwierzytelnianie osób upoważnionych  Wymogi dotyczące weryfikacji wewnętrznej (zasada podwójnej kontroli)  Specyfikacja obowiązkowych lub możliwych lokalizacji przechowywania danych  Monitorowanie usuwania nośników danych  Dla każdego właściwego obszaru: wyznaczenie osób upoważnionych do niszczenia nośników danych  Monitorowanie plików  Szafa bezpieczeństwa  Kontrola niszczenia nośników danych  Wytyczne dotyczące tworzenia kopii zapasowych  Dokumentacja dotycząca programów odpowiedzialnych za przesyłanie i odbieranie danych  Dokumentacja celów, dla których przekazywane są dane oraz ścieżka przekazania (ścieżka logiczna)  Szyfrowanie danych w przypadku, gdy są one przekazywane online lub przewożone na ruchomych nośnikach danych (np. na notebookach, dyskach twardych, płytach CD, DVD, pamięciach USB, kartach pamięci, taśmach, dyskietkach itp.)  Nadzór nad kompletnością i prawidłowością przekazywania danych (pełna kontrola)  Sprawdzanie kompletności i poprawności  Usunięcie pozostałych danych przy wymianie nośnika danych  Zabezpieczenie wewnętrznych sieci przed nieuprawnionym dostępem (np. poprzez firewall)  Wdrożenie skanerów antywirusowych  Wdrożenie filtrów (np. filtrów URL, filtrów załączników e-mail itp.)  Dostępność i odporność systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności |
| **Kontrola wprowadzania danych**  Środki dotyczące późniejszej weryfikacji czy i przez kogo dane zostały wprowadzone, zmienione lub usunięte.  możliwość weryfikacji poprzez logi, pełny monitoring | **Rozdzielność danych**  Środki zapewniające, że dane, które zostały zebrane w różnych celach, mogą być przetwarzane oddzielnie.  Oddzielenie danych, które zostały zapisane pod aliasem (pseudonimem) od pierwotnych danych  Oddzielenie danych testowych i danych produkcyjnych |
| **Dostępność**  Środki zapewniające ochronę danych osobowych przed przypadkowym zniszczeniem lub utratą.  Przeprowadzanie oceny ryzyka i analiza słabych punktów  Rozdział funkcjonalny między działem IT, a innymi departamentami  Centralne zamówienia sprzętu i oprogramowania  Sformalizowane procedury zatwierdzania sprzętu i oprogramowania, jak również procesów informatycznych  Stała aktualizacja stosowanego oprogramowania (np. poprzez aktualizacje, łaty, poprawki itp.)  Wytyczne dotyczące dokumentacji procesów oprogramowania i procesów informatycznych  Wewnętrzne i globalne wytyczne i procesy przetwarzania danych, wytyczne, instrukcje dotyczące pracy, opisy procesów oraz zasady programowania, badania i rozliczania danych | **Przywrócenie dostępności**  Środki zapewniające zdolność do szybkiego przywrócenia dostępności i dostępu do danych osobowych w razie incydentu fizycznego lub technicznego.  Istnienie planu awaryjnego (rezerwowy plan awaryjny)  Tworzenie kopii zapasowych w regularnych odstępach czasu  Przechowywanie kopii zapasowych w bezpiecznej lokalizacji, poza działem IT  Regularnie prowadzona ocena zdolności przywrócenia z kopii zapasowych  Wyznaczenie inspektora ochrony danych  Regularne szkolenie pracowników w zakresie ochrony danych  Instalacja serwerów w osobnych i bezpiecznych serwerowniach lub centrach danych  Środki ostrożności w zakresie bezpieczeństwa pożarowego  System ostrzegania przed pożarem/zalaniem  Awaryjny generator zasilający  Procedury przywracania dostępności  Tworzenie lustrzanych kopii danych  Proces regularnego testowania, mierzenia i oceny skuteczności |
| **Kontrola organizacyjna**  Wewnętrzne i globalne wytyczne i procedury dotyczące przetwarzania danych; wytyczne, instrukcje pracy, opisy procedur i zasad programowania, oceny oraz publikacji danych  Istnienie koncepcji zabezpieczenia danych  Ocena systemów i programów zgodnie z normami branżowymi  Istnienie planu awaryjnego (zapasowy plan kryzysowy)  Pracownicy zobowiązują się na piśmie do przestrzegania tajemnicy danych i obowiązków w zakresie poufności  Regularne szkolenie pracowników w zakresie ochrony danych  Wyznaczenie inspektora ochrony danych  Certyfikacja – certyfikat PKJBI (Program Kontroli Jakości Bezpieczeństwa Informacji) - standard wdrożony przez OFBOR na wzór normy ISO 27001. | **Kontrola przetwarzania danych**  Środki zapewniające przetwarzanie danych osobowych przez Przetwarzającego dane zgodnie z instrukcjami FRSE.  Wytyczne i procesy obowiązujące pracowników Podmiotu przetwarzającego  Sformalizowane przetwarzanie danych  Na żądanie FRSE otrzyma on od Podmiotu przetwarzającego niezbędne informacje w celu monitorowania zgodności Przetwarzającego z niniejszą Umową  Wyraźne rozgraniczenie pomiędzy obszarami odpowiedzialności Przetwarzającego, a FRSE |
| **Niezależna weryfikacja lub certyfikacja przez renomowaną stronę trzecią** | |
| Niezależna weryfikacja lub certyfikacja przez renomowaną stronę trzecią może być wiarygodnym sposobem wykazania zgodności z wymogami określonymi w punkcie 6 Umowy powierzenia. Taka certyfikacja wskazywałaby, jako minimum, że środki kontroli ochrony danych były przedmiotem audytu lub przeglądu zgodnie z uznanym standardem. W przypadku, w którym Przetwarzający zainicjował taki rodzaj kontroli, Przetwarzający powinien umieścić kopię wystawionego przez stronę trzecią świadectwa kontroli lub sprawozdania z kontroli potwierdzającego certyfikację jako załącznik do niniejszego Załącznika 1. Takie standardy i certyfikaty powinny odnosić się do środków technicznych (takich jak lokalizacja danych lub szyfrowanie), jak również procesów w ramach organizacji Przetwarzającego, które gwarantują ochronę danych (takie jak polityka kontroli dostępu, kontrola dostępu lub kopie zapasowe).  Proszę wymienić przeprowadzone przez renomowaną osobę trzecią niezależne weryfikacje lub certyfikacje:  1. […] | |

**Załącznik nr 2**

do umowy

powierzenia

**Lista zaakceptowanych dalszych podmiotów przetwarzających, z których usług Przetwarzający ma prawo korzystać przy przetwarzaniu danych osobowych**

|  |  |
| --- | --- |
| **Nazwa firmy/instytucji** |  |
| **Adres** |  |
| **Data powierzenia** |  |
| **Przedmiot** |  |
| **Cel przetwarzania** |  |
| **Lokalizacja przetwarzania** |  |

|  |  |
| --- | --- |
| **Nazwa firmy/instytucji** |  |
| **Adres** |  |
| **Data powierzenia** |  |
| **Przedmiot** |  |
| **Cel przetwarzania** |  |
| **Lokalizacja przetwarzania** |  |