„WZÓR"

Umowa powierzenia przetwarzania danych osobowych

(zwana dalej **„Umową powierzenia"**)

zawarta w Warszawie, ... roku między:

Prezesem Prokuratorii Generalnej Rzeczypospolitej Polskiej

- adres: Urząd Prokuratorii Generalnej Rzeczypospolitej Polskiej, ul. Hoża 76/78, 00-682 Warszawa,
- w imieniu którego działa ....., ..., na podstawie upoważnienia nr ...../..... z ..... roku, (załącznik nr ..... do Umowy powierzenia),
- zwanym dalej **„Administratorem"**

a

.....

- posługującym/-ą się w obrocie numerem NIP .....
- zwanym/-ą dalej „**Podmiotem przetwarzającym**",

zwanymi dalej łącznie **„Stronami"** a każda z osobna **„Stroną"**,

w związku z zawarciem między Skarbem Państwa - Urzędem Prokuratorii Generalnej Rzeczypospolitej Polskiej a Podmiotem przetwarzającym umowy nr ....., której przedmiotem jest .....
.....,
zwaną dalej **„Umową główną**", dla której wykonania konieczne jest przetwarzanie danych osobowych, Strony postanawiają, co następuje:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych), zwanego dalej **„Rozporządzeniem"**, dane osobowe do przetwarzania, na podstawie Umowy powierzenia.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową powierzenia.
3. Przetwarzanie danych osobowych oraz wykonanie przez Podmiot przetwarzający innych zobowiązań opisanych w Umowie powierzenia odbywają się w ramach wynagrodzenia Podmiotu przetwarzającego określonego w Umowie głównej.
4. Podmiot przetwarzający oświadcza, że podczas przetwarzania powierzonych danych osobowych stosuje środki techniczne i organizacyjne spełniające wymogi Umowy powierzenia oraz Rozporządzenia.
5. Przetwarzanie danych osobowych przez Podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie Administratora. Za udokumentowane polecenie uznaje się Umowę powierzenia, w tym dodatkowe zadania lub czynności zlecone do wykonywania Podmiotowi przetwarzającemu Umową główną, związane z koniecznością dokonywania czynności przetwarzania danych osobowych.

§ 2

Charakter i cel przetwarzania danych osobowych

1. W okresie obowiązywania Umowy powierzenia przetwarzanie będzie miało charakter ....., a czynności przetwarzania będą dokonywane w sposób ..... Przetwarzanie powierzonych danych osobowych będzie obejmować następujące operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych:
   1) .....;
   2) .....
2. Powierzone przez Administratora dane osobowe będą przetwarzane wyłącznie w celu wykonania Umowy głównej.

§ 3

Rodzaje danych osobowych oraz kategorie osób, których dane dotyczą

Podmiot przetwarzający będzie przetwarzał niżej wymienione rodzaje danych osobowych, dotyczące następującej/następujących kategorii osób:

1) .....;
2) .....

§ 4

Sposób wykonania Umowy powierzenia

1. Podmiot przetwarzający zobowiązuje się:
   1) zabezpieczyć powierzone dane osobowe poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia. Opis technicznych i organizacyjnych środków ochrony danych osobowych stosowanych przez Podmiot przetwarzający określa załącznik nr ..... do Umowy powierzenia;
   2) dołożyć należytej staranności związanej z zapewnieniem ochrony danych;
   3) nadać upoważnienia do przetwarzania powierzonych danych osobowych wyłącznie osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy powierzenia i zobowiązały się do zachowania tajemnicy w czasie i po ustaniu łączącego upoważnionych z Podmiotem przetwarzającym stosunku prawnego.
2. Podmiot przetwarzający uwzględniając charakter przetwarzania pomaga Administratorowi:
   1) wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie jej praw wymienionych w rozdziale III Rozporządzenia, poprzez odpowiednie środki techniczne i organizacyjne;
   2) wywiązywać się z obowiązków określonych w art. 32-36 Rozporządzenia, przy uwzględnieniu posiadanych informacji.
3. W przypadku stwierdzenia incydentu bezpieczeństwa, którego następstwem może być naruszenie ochrony powierzonych do przetwarzania danych osobowych, Podmiot przetwarzający:
   1) zgłasza go Administratorowi bez zbędnej zwłoki, nie później niż w ciągu 12 godzin od stwierdzenia incydentu,
   2) umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających,
   3) niezwłocznie, lecz nie później niż w ciągu 24 godzin od stwierdzenia incydentu, informuje Administratora o dalszych ustaleniach, w szczególności co do charakteru incydentu, kategorii danych osobowych, liczby podmiotów danych oraz o możliwych konsekwencjach incydentu.

4. Zgłoszenie o stwierdzeniu incydentu powinno być przesłane wraz z wszelką dotyczącą go dokumentacją, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzorczego oraz zawiadomienia podmiotów danych.
5. Niezależnie od obowiązków wynikających z ust. 3 i 4, Podmiot przetwarzający jest także zobowiązany do niezwłocznego poinformowania Administratora o:
   1) każdym naruszeniu ochrony danych osobowych zgłoszonym przez Podmiot przetwarzający do Prezesa Urzędu Ochrony Danych Osobowych lub innego organu nadzorczego;
   2) postępowaniu administracyjnym, przygotowawczym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych, w tym o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych skierowanych do Podmiotu przetwarzającego;
   3) wszelkich planowanych lub realizowanych kontrolach prowadzonych przez organ nadzorczy (art. 31 Rozporządzenia), dotyczących przetwarzania przez Podmiot przetwarzający danych osobowych.
6. Podmiot przetwarzający, po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, niezwłocznie, lecz nie później niż w ciągu:
   1) 7 dni, usuwa wszelkie powierzone mu dane osobowe/zwraca Administratorowi wszelkie powierzone mu dane osobowe oraz usuwa wszelkie istniejące ich kopie, chyba że prawo Unii Europejskiej lub prawo polskie nakazują przechowywanie danych osobowych; Podmiot przetwarzający jest zobowiązany do niezwłocznego poinformowania Administratora o obciążającym go obowiązku dalszego przechowywania danych osobowych;
   2) 30 dni, doręcza Administratorowi dokument potwierdzający fakt usunięcia/zwrócenia wszelkich powierzonych mu danych osobowych.

§ 5
Audyt

1. Podmiot przetwarzający udostępnia na żądanie Administratora wszelkie informacje potwierdzające spełnianie przez Podmiot przetwarzający obowiązków wynikających z Rozporządzenia, w tym informacje (wypis) z rejestru kategorii czynności przetwarzania dokonywanych w imieniu Administratora.
2. Podmiot przetwarzający umożliwia Administratorowi przeprowadzanie audytów, w tym inspekcji, w miejscach przetwarzania danych osobowych przez Podmiot przetwarzający oraz wszystkie podmioty, którym dalej powierzy przetwarzanie danych oraz uczestniczy w tych czynnościach. Audyt, w tym inspekcja, obejmuje w szczególności ocenę wykonywania czynności przetwarzania danych osobowych i ich ochrony.
3. Audyt, w tym inspekcję, przeprowadza Administrator lub upoważniony przez niego audytor.
4. Administrator przeprowadza audyt, w tym inspekcję, w uzgodnionym z Podmiotem przetwarzającym terminie oraz miejscu. W przypadku braku takich uzgodnień Administrator przeprowadza za minimum 7-dniowym uprzedzeniem audyt lub inspekcję w dni robocze, w godzinach 9:00-17:00, w miejscach przetwarzania danych.
5. W przypadku zgłoszenia przez Podmiot przetwarzający incydentu bezpieczeństwa lub powzięcia przez Administratora informacji o incydencie bezpieczeństwa, którego następstwem może być naruszenie ochrony powierzonych do przetwarzania danych osobowych, termin, o którym mowa w ust. 4, ulega skróceniu do 1 dnia.
6. Z przeprowadzonego audytu lub inspekcji Administrator lub upoważniony przez niego audytor sporządza sprawozdanie i doręcza je za potwierdzeniem Podmiotowi przetwarzającemu.
7. Jeżeli z dokonanego audytu lub inspekcji wynikają uchybienia lub potrzeba wprowadzenia dodatkowych zabezpieczeń, Administrator kieruje do Podmiotu przetwarzającego polecenie

usunięcia uchybień lub wdrożenia dodatkowych zabezpieczeń, ze wskazaniem terminu wykonania.

8. O usunięciu uchybień lub wprowadzeniu dodatkowych zabezpieczeń Podmiot przetwarzający zawiadamia niezwłocznie Administratora.
9. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii Europejskiej lub przepisów prawa polskiego o ochronie danych.

§ 6

Podpowierzenie

1. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. Jednocześnie Administrator wyraża zgodę na korzystanie przez Podmiot przetwarzający z usług dalszych podmiotów przetwarzających, wskazanych w Wykazie stanowiącym załącznik nr ..... do Umowy powierzenia. Podmioty wymienione w wykazie nie mogą udzielać dalszych podpowierzeń danych osobowych bez pisemnej lub elektronicznej zgody Administratora.
2. Przekazanie powierzonych danych osobowych do:
   1) państw spoza Europejskiego Obszaru Gospodarczego;
   2) organizacji międzynarodowej

   - może nastąpić jedynie na polecenie Administratora w formie pisemnej lub elektronicznej chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo polskie. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Inny podmiot przetwarzający, o którym mowa w ust. 1, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w Umowie powierzenia. Podmiot przetwarzający jest zobowiązany do dostarczenia Administratorowi:
   1) kopii już zawartej umowy dalszego powierzenia przetwarzania danych osobowych z innym podmiotem przetwarzającym, nie później niż w dniu zawarcia Umowy powierzenia lub w dniu wystąpienia do Administratora o zgodę na korzystanie z usług innego podmiotu przetwarzającego albo,
   2) projektu istotnych postanowień umowy powierzenia przetwarzania danych osobowych z innym podmiotem przetwarzającym, nie później niż w dniu wystąpienia do Administratora o zgodę na korzystanie z usług innego podmiotu przetwarzającego, a następnie, po jej zawarciu – zobowiązany jest do niezwłocznego przekazania Administratorowi kopii tej umowy.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na innych podmiotach przetwarzających obowiązków ochrony danych osobowych.

§ 7

Czas obowiązywania Umowy powierzenia

Umowa powierzenia obowiązuje od dnia jej zawarcia przez czas obowiązywania Umowy głównej, z zastrzeżeniem, że Podmiot przetwarzający jest zobowiązany do zwrotu/usunięcia danych osobowych oraz doręczenia potwierdzenia tej czynności zgodnie z § 4 ust. 6.

§ 8

Rozwiązanie Umowy powierzenia

1. Rozwiązanie, wypowiedzenie, wygaśnięcie Umowy głównej lub odstąpienie od niej, wywołuje taki sam skutek prawny w stosunku do Umowy powierzenia, z zastrzeżeniem § 7 in fine.

2. Administrator może wypowiedzieć Umowę powierzenia ze skutkiem natychmiastowym[1], gdy Podmiot przetwarzający przetwarza dane osobowe w sposób niezgodny z Umową powierzenia, w szczególności:
   1) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora;
   2) uniemożliwił Administratorowi, w tym upoważnionemu przez Administratora audytorowi, przeprowadzenie audytu lub inspekcji, o którym mowa w § 5;
   3) pomimo skierowania polecenia, nie usunął uchybień, nie wdrożył dodatkowych zabezpieczeń lub nie wykonał ustalonych w poleceniu czynności w uzgodnionym lub wyznaczonym przez Administratora terminie;
   4) przekazał powierzone dane osobowe do państwa spoza Europejskiego Obszaru Gospodarczego lub organizacji międzynarodowej bez polecenia Administratora,
   5) nie zgłosił Administratorowi w terminie incydentu bezpieczeństwa, którego następstwem może być naruszenie ochrony powierzonych do przetwarzania danych osobowych.

§ 9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, pozyskanych w związku z zawarciem Umowy powierzenia lub jej wykonywaniem.
2. Obowiązek, o którym mowa w ust. 1 wiąże strony przez czas wykonywania Umowy powierzenia oraz przez 5 lat po zakończeniu jej wykonywania.

§ 10

Postanowienia końcowe

1. Jeżeli Podmiot przetwarzający naruszy Rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.
2. Strony wyznaczają następujące osoby do kontaktu w sprawach związanych z wykonywaniem Umowy powierzenia:
   1) ze strony Administratora: .....;
   2) ze strony Podmiotu przetwarzającego: .....
3. Strony wskazują dane kontaktowe inspektorów ochrony danych wyznaczonych przez:
   1) Administratora:
      a) inspektor ochrony danych, ..., tel. 22 ....., e-mail: .....@prokuratoria.gov.pl,
      b) zastępca inspektora ochrony danych, ..., tel. 22 ....., e-mail.: .....@prokuratoria.gov.pl;
   2) Podmiot przetwarzający:
      inspektor ochrony danych, ..., tel. ....., e-mail: .....@.....
4. Zmiany danych podanych w ust. 2 i 3 nie wymagają zmiany Umowy powierzenia i następują w drodze pisemnego lub mailowego poinformowania drugiej Strony.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy powierzenia będzie sąd właściwy dla siedziby Administratora.
6. Integralną część Umowy powierzenia stanowią załączniki:
   1) upoważnienie nr ...../..... z ..... roku;
   2) wydruk .....;

3) szczegółowy opis technicznych i organizacyjnych środków ochrony danych osobowych wprowadzonych przez Podmiot przetwarzający;
4) wykaz podmiotów, którym Podmiot przetwarzający powierza dalsze przetwarzanie danych osobowych;
5) .....

7. Zmiana Umowy powierzenia wymaga formy pisemnej pod rygorem nieważności.
8. Umowa powierzenia została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....	.....
Administrator	Podmiot przetwarzający

Załącznik nr ..... do Umowy powierzenia

OPIS TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW OCHRONY DANYCH OSOBOWYCH WPROWADZONYCH PRZEZ PODMIOT PRZETWARZAJĄCY

Techniczne środki ochrony stosowane w związku z przetwarzaniem danych osobowych

1. Miejsca przetwarzania danych osobowych znajdują się:
   1) .....,
   2) ..... .
2. Służba ochrony prowadzi całodobową, fizyczną ochronę budynku, w którym są przetwarzane dane osobowe.
3. Budynek [.....pomieszczenie], w którym są przetwarzane dane osobowe, jest zabezpieczony systemem alarmowym.
4. Wejścia do budynku, w który przetwarzane są dane osobowe i teren wokół niego, jest objęty monitoringiem wizyjnym.
5. Dokumenty zawierające dane osobowe są przechowywane w szafach zamykanych na klucz.
6. Dokumenty zawierające dane osobowe, po ustaniu przydatności, są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów o właściwych parametrach niszczenia.
7. Zastosowano urządzenia typu: UPS, generator prądu lub wydzielona sieć elektroenergetyczna, chroniące system teleinformatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
8. Dostęp do systemu operacyjnego komputera lub serwera, w którym przetwarzane są dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia, w szczególności z wykorzystaniem identyfikatora użytkownika (login) oraz hasła.
9. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych, przetwarzanych przy użyciu systemów teleinformatycznych.
10. Zastosowano systemowe mechanizmy wymuszające na osobach przetwarzających dane osobowe okresową zmianę haseł uwierzytelniających.
11. Zastosowano system rejestracji dostępu do danych osobowych.
12. Przy transmisji teleinformatycznej danych zastosowano: .....
13. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji a dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
14. Zastosowano macierz dyskową dyskowej (sprzętowy RAID .....), rozwiązania hiperkonwergentne oraz są regularnie wykonywane kopie zapasowe danych w celu ochrony danych osobowych przed skutkami awarii pamięci.
15. Aktualizacja systemów operacyjnych oraz kluczowego dla przetwarzania danych osobowych oprogramowania jest dokonywana niezwłocznie po jej wydaniu przez producentów.
16. Zastosowano środki ochrony przed oprogramowaniem zawierającym wirusy komputerowe, niechcianą korespondencją (spamem) oraz złośliwym oprogramowaniem (malware) m.in. takim jak robaki, wirusy, konie trojańskie, rootkity, posiadające funkcjonalność ściągania aktualnych sygnatur wirusów.
17. Zastosowano rozwiązanie zapory ogniowej (firewall) do ochrony dostępu do sieci teleinformatycznej oraz segmentację sieci.

18. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
19. Zainstalowano wygaszacze ekranów na sprzęt przy pomocy którego przetwarzane są dane osobowe.
20. Zastosowano mechanizm automatycznej blokady dostępu do systemu teleinformatycznego służącego do przetwarzania danych osobowych w przypadku braku dłuższej aktywności użytkownika.

Techniczne środki ochrony stosowane w związku z przetwarzaniem danych osobowych przy pomocy urządzeń przenośnych, w szczególności laptopów

1. Miejsce przetwarzania danych osobowych znajduje się na terytorium ..... .
2. Przetwarzanie danych odbywa się w miejscu uniemożliwiającym swobodny dostęp osób postronnych.
3. Dostęp do systemu operacyjnego urządzeń przenośnych, w którym przetwarzane są dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia, w szczególności z wykorzystaniem identyfikatora użytkownika (login) oraz hasła.
4. Zastosowano środki ochrony przed oprogramowaniem zawierającym wirusy komputerowe, niechcianą korespondencją (spamem) oraz złośliwym oprogramowaniem (malware) m.in. takim jak robaki, wirusy, konie trojańskie, rootkity, posiadające funkcjonalność ściągania aktualnych sygnatur wirusów.
5. Zainstalowano wygaszacze ekranów na urządzeniach przenośnych, przy pomocy których przetwarzane są dane osobowe.
6. Urządzenie przenośne nie łączy się poprzez publiczne (np. hotelowe) punkty dostępowe z siecią Internet, w tym przez sieć Wi-Fi lub za pomocą połączenia kablowego.
7. Połączenie z siecią Internet odbywa się za pomocą prywatnego łącza internetowego.
8. Połączenie z zasobami informacyjnymi odbywa się przez tunel VPN.
9. Dysk twardy urządzenia, na którym przetwarzane są dane osobowe został zaszyfrowany przy pomocy ..... .
10. Zastosowano mechanizm automatycznej blokady dostępu do systemu teleinformatycznego służącego do przetwarzania danych osobowych w przypadku braku dłuższej aktywności użytkownika.

Organizacyjne środki ochrony stosowane w związku z przetwarzaniem danych osobowych

1. Wyznaczono inspektora danych osobowych, z którym można skontaktować się telefonicznie pod numerem: ....., za pomocą poczty elektronicznej pod adresem e-mail: ....., korespondencyjnie pod adresem: ..... .
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, jest ograniczony zasadami zarządzania dostępem do kluczy do pomieszczeń lub elektroniczną kontrola dostępu.
3. Dostęp do danych mają tylko wyznaczone osoby .....
4. Osoby upoważnione do przetwarzania danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych .....
5. Osoby upoważnione do przetwarzania danych osobowych zostały przeszkolone w zakresie zabezpieczeń systemu teleinformatycznego w zakresie ich właściwości.
6. Osoby upoważnione do przetwarzania danych osobowych zostały obowiązane do zachowania ich w tajemnicy, także po ustaniu zatrudnienia lub innej podstawy prawnej współpracy.

Załącznik nr ..... do Umowy powierzenia

WYKAZ DALSZYCH PODMIOTÓW PRZETWARZAJĄCYCH

Administrator wyraża zgodę na korzystanie przez Podmiot przetwarzający z usług:

1) [firma podmiotu], [adres podmiotu] w zakresie przetwarzania danych osobowych niezbędnych do ..... [tutaj wskazać zakres usług świadczonych na rzecz Podmiotu przetwarzającego], z zastrzeżeniem, że dane muszą być przetwarzane na terenie Europejskiego Obszaru Gospodarczego,
2) [firma podmiotu], [adres podmiotu] w zakresie przetwarzania danych osobowych niezbędnych do ..... [tutaj wskazać zakres usług świadczonych na rzecz Podmiotu przetwarzającego], z zastrzeżeniem, że dane muszą być przetwarzane na terenie Europejskiego Obszaru Gospodarczego,
3) spółki Zoom Video Communications, Inc. z siedzibą w Stanach Zjednoczonych Ameryki – w zakresie przetwarzania danych osobowych niezbędnych do przeprowadzenia transmisji obrazu i dźwięku, o której mowa w Umowie głównej, z zastrzeżeniem, że dane z transmisji muszą być przetwarzane na terenie Europejskiego Obszaru Gospodarczego.
4) spółki Microsoft Ireland Operations Ltd. z siedzibą w Republice Irlandii - w zakresie przetwarzania danych osobowych niezbędnych do :
   a) przeprowadzenia transmisji obrazu i dźwięku, o której mowa w Umowie głównej (w tym MS Teams), z zastrzeżeniem, że dane z transmisji muszą być przetwarzane na terenie Europejskiego Obszaru Gospodarczego,
   b) przetwarzania, w tym zapisywania, modyfikowania, usuwania i przechowywania danych na serwerach tej spółki (w tym One Drive, Microsoft 365), z zastrzeżeniem, że dane muszą być przetwarzane na terenie Europejskiego Obszaru Gospodarczego.