WSPÓLNA POLITYKA BEZPIECZEŃSTWA INFORMACJI

KONSORCJUM BEZPIECZEŃSTWO GOSPODARCZE POLSKI

oraz

FUNDACJI BEZPIECZEŃSTWO GOSPODARCZE POLSKI. INSTYTUT DIALOGU I ANALIZ PRAWNO -GOSPODARCZYCH

KONSORCJUM
BEZPIECZEŃSTWO
GOSPODARCZE
POLSKI

FUNDACJA
BEZPIECZEŃSTWO
GOSPODARCZE
POLSKI

Lublin, 2019

SPIS TREŚCI

Wstęp

Celem Konsorcjum Bezpieczeństwo Gospodarcze Polski jest zbudowanie platformy współpracy między nauką a przedsiębiorcami wraz z instytucjami otoczenia biznesu, poprzez inicjowanie i prowadzenie wspólnych badań, komercjalizację wyników prac oraz podnoszenie konkurencyjności polskiej gospodarki.

Celem Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno -Gospodarczych jest wszechstronna działalność, w tym społeczna, informacyjna, naukowa i oświatowa, na rzecz szeroko rozumianego bezpieczeństwa gospodarczego Polski i polskich przedsiębiorstw oraz podnoszenia ich konkurencyjności i wspomagania rozwoju gospodarczego, w tym promowania rozwoju przedsiębiorczości i inicjatywy.

Gwarancją realizacji celów zarówno Konsorcjum Bezpieczeństwo Gospodarcze Polski jak i Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych jest sprawna i skuteczna ochrona informacji i danych osobowych poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych. Konsorcjum oraz Fundacja świadome wagi problemów związanych z bezpieczeństwem informacji i ochroną prawa do prywatności, w tym w szczególności praw osób fizycznych powierzających w Konsorcjum i Fundacji swoje dane osobowe do właściwej i skutecznej ochrony tych danych, wspólnie deklarują:

- zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
- zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Konsorcjum i Fundacji *w* zakresie problematyki bezpieczeństwa informacji,
- zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
- zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

Współadministratorami danych przetwarzanych w ramach Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych są:

Konsorcjum Bezpieczeństwo Gospodarcze Polski (dalej jako: Współadministrator pierwszy)
oraz
Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych z siedzibą przy ul. Chopina 29/9A , 20-023 Lublin (Współadministrator drugi)

dalej łącznie określani jako współadministratorzy.

W ramach Wspólnej Wspólna Polityka Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych uzgodniony został zakres wypełniania obowiązków wynikających z RODO, w tym w szczególności uzgodniono, że:

1) **Współadministrator drugi, w imieniu Współadministratorów realizuje zadania w sprawach z zakresu ochrony danych osobowych, w szczególności**:

a) jest odpowiedzialny za zapewnienie osobom, których dane dotyczą, realizacji jej praw wynikających z RODO. Niezależnie od takiego ustalenia, osoba taka może wykonywać swoje prawa również wobec współadministratora pierwszego. W takim przypadku Współadministrator pierwszy niezwłocznie przekaże żądanie osoby, której dane osobowe dotyczą, Współadministratorowi drugiemu, który zrealizuje żądanie takiej osoby.

b) jest odpowiedzialny za wdrożenie środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, a także identyfikuje ryzyka naruszenia praw lub wolności osób fizycznych przy procesach przetwarzania danych osobowych w Fundacji, o których mowa w ust. 1 oraz § 1 ust. 9, a także dokonuje oceny skutków ich przetwarzania zgodnie z przepisami RODO.

c) Współadministrator drugi zapewnia udokumentowany przebieg wdrażania przepisów o ochronie danych osobowych oraz wykazuje w ten sam sposób przestrzeganie wszystkich ciążących na nim obowiązków, zgodnie z przepisami powszechnie obowiązującymi.

§ 1
Cel i zakres unormowań

1. Wspólna Polityka Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-gospodarczych określa strukturę organizacyjną zapewniającą optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem adekwatnego i proporcjonalnego stopnia bezpieczeństwa informacji i danych osobowych administrowanych przez Konsorcjum i Fundację, przetwarzanych metodami tradycyjnymi.
2. Niniejszy dokument wyznacza podmioty odpowiedzialne za przetwarzanie danych osobowych i informacji oraz zobowiązuje je do zapewnienia możliwie najwyższego poziomu bezpieczeństwa.
3. Integralną częścią Polityki są następujące załączniki:

1) wzór klauzuli zgody na przetwarzanie danych osobowych,
2) wzór klauzuli informacyjnej Administratora Danych,
3) rejestr czynności przetwarzania danych,
4) upoważnienie do przetwarzania danych,
5) oświadczenie o zachowaniu w tajemnicy danych osobowych i informacji oraz sposobów ich zabezpieczenia,
6) ewidencja osób upoważnionych do przetwarzania danych,
7) wzór umowy na powierzenie przetwarzania danych osobowych,
8) rejestr naruszeń ochrony danych osobowych i bezpieczeństwa informacji,
9) wzór polityki cookies,
10) wzór klauzuli informacyjnej dotyczącej korespondencji mailowej,
11) wzór odwołania zgody na przetwarzanie danych osobowych.

4. Opracowane w dokumencie zasady, prawa oraz procedury opierają się na przepisach powszechnie obowiązujących, przy czym pierwszeństwo w stosowaniu mają zawsze te drugie. Wspólna Polityka ma na celu zgromadzenie i opisanie w sposób przystępny podstawowych zasad postępowania z danymi osobowymi i informacjami w celu zapewnienia odpowiedniego poziomu ich ochrony.
5. Wspólna Polityka została opracowana w celu spełnienia wymogów wynikających z przepisów prawa, w szczególności:
   1) 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 (Dz. Urz. UE L 119);
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   3) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113).
6. Zakres obowiązywania Wspólnej Polityki obejmuje:
   1) wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne dokumenty (papierowe), w których przetwarzane są lub będą dane osobowe i informacje;
   2) informacje będące własnością Fundacji, partnerów lub osób korzystających z usług Fundacji, o ile zostały przekazane na podstawie umów;
   3) wszystkie typy nośników (np. papierowych, magnetycznych, optycznych, itp.), na których są lub będą znajdować się dane osobowe lub informacje;
   4) wszystkie lokalizacje – pomieszczenia i części pomieszczeń, w których są lub będą przetwarzane dane osobowe lub informacje;
   5) wszystkich pracowników w rozumieniu przepisów Kodeksu pracy oraz inne osoby mające dostęp do danych osobowych lub informacji.
7. Ponadto, celem opracowania i wdrożenia Wspólnej Polityki jest osiągnięcie poziomu organizacyjnego i technicznego, który:
   1) będzie gwarantem pełnej ochrony osób, których dane dotyczą oraz ciągłości procesu ich przetwarzania;

2) zapewni zachowanie poufności informacji chronionych oraz legalności, przejrzystości, rzetelności, celowości, adekwatności, prawidłowości, czasowości, integralności i poufności przetwarzania danych osobowych osób fizycznych;
3) zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach i formach jej przetwarzania;
4) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji i danych osobowych, wynikających z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Konsorcjum bądź Fundacji;
5) zapewni gotowość do podjęcia działań w sytuacjach zagrożenia dla bezpieczeństwa Konsorcjum lub Fundacji, ich interesów oraz posiadanych i powierzonych jej informacji i danych osobowych.

8. Organizacyjne, techniczne oraz informatyczne środki ochrony informacji i danych osobowych przewidziane we Wspólnej Polityce formułowane są w oparciu o występujące ryzyko związane z zagrożeniami, takimi jak:
1) błędy i nieprawidłowości w postępowaniu własnych pracowników lub członków organów Fundacji bądź Konsorcjum,
2) naturalne katastrofy,
3) działalność przestępcza,
4) infekcje systemów informatycznych, które mogą wykradać zasoby komputera,
5) korzystanie z witryn internetowych na których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
6) przerwy i zakłócenia w działaniu systemu,
7) inne zagrożenia mogące wystąpić w związku z socjotechnicznymi metodami kradzieży informacji oraz dynamicznie rozwijającymi się technikami i metodami przetwarzania danych.

§ 2
Skróty i definicje

1. ***Konsorcjum*** – oznacza Konsorcjum Bezpieczeństwo Gospodarcze Polski
2. ***Fundacja*** – oznacza Fundację Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych.
3. ***Zarząd Fundacji*** – oznacza organ o którym mowa w § 10 i następnych Statutu Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych przyjęty uchwałą nr 1/2019 Zgromadzenia Fundatorów z dnia 18 czerwca 2019 r.
4. ***Wspólna Polityka –*** oznacza Wspólną Politykę Bezpieczeństwa Informacji, określoną w niniejszym dokumencie.
5. ***Administrator Pierwszy –*** Konsorcjum Bezpieczeństwo Gospodarcze Polski.
6. ***Administrator Drugi –*** Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych decydująca o celach i środkach przetwarzania danych osobowych.
7. ***RODO –*** Rozporządzenie 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.

8. ***Pracownik –*** osoba zatrudniona w Fundacji w oparciu o umowę o pracę, akt mianowania lub realizująca zlecone czynności na podstawie umowy cywilnoprawnej.
9. ***Pozostali członkowie organów Fundacji –*** osoba powołana do organu Fundacji w drodze uchwały kompetentnego organu Fundacji
10. ***Dane osobowe –*** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Przy czym możliwa do zidentyfikowania **osoba fizyczna** to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość **osoby fizycznej.**
11. ***Przetwarzanie*** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalenie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
12. ***Naruszenie ochrony danych osobowych lub incydent –*** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, lub nieuprawnionego dostępu do danych osobowych lub informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
13. ***Informacja*** – niestanowiąca tajemnicy państwowej wiadomość, z którą zobowiązany Wspólną Polityką zapoznał się w związku z wykonywaną pracą, a której ujawnienie może narazić na szkodę uzasadniony interes Konsorcjum lub Fundacji, interes publiczny lub prawnie chroniony interes obywateli, z wyłączeniem informacji niejawnych, których zasady ochrony normowane są odrębnie.
14. ***Zbiór danych –*** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
15. ***Pseudonimizacja*** – przetwarzanie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

§ 3
Zasady ogólne

1. Filarami ochrony danych osobowych w Konsorcjum i Fundacji są:
   1) **Legalizm** – Fundacja, w imieniu Konsorcjum dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
   2) **Bezpieczeństwo** – Fundacja, w imieniu Konsorcjum zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie,

3) **Prawa jednostki** – Fundacja, w imieniu Konsorcjum umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
4) **Rozliczalność** – Fundacja, w imieniu Konsorcjum dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z RODO.

2. **Zasada zgodności z prawem:**
   1) Zasada zgodności z prawem składa się z trzech pomniejszych zasad, jakimi są:
      a) **legalność** – oznacza zgodność dokumentacji i procedur z przepisami RODO oraz obowiązującymi ustawami i wydanymi na ich podstawie aktami wykonawczymi, a także poprzez wdrożenie odpowiednich środków organizacyjnych i technicznych do obsługi praw podmiotów danych,
      b) **rzetelność** – oznacza uczciwe i lojalne przetwarzanie danych w stosunku do osób, których dane dotyczą,
      c) **przejrzystość** – oznacza czytelną i zrozumiałą komunikację współadministratorów z osobą, której dane dotyczą. Przejrzystość przejawia się zarówno poprzez jasne i czytelnym językiem formułowanie m.in. zgód na przetwarzanie danych i klauzul informacyjnych, jak i zrozumiałą komunikację w przedmiocie podania podstaw żądania poszczególnych danych osobowych.
   2) Przetwarzanie danych osobowych uważa się za zgodne z prawem, z zastrzeżeniem pkt 5, wyłącznie w przypadkach i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
      a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, wzór zgody stanowi załącznik nr 1;
      b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
      c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na współadministratorach wspólnie albo oddzielnie;
      d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
      e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej współadministratorom wspólnie albo oddzielnie.
   3) Współadministrator drugi w każdym przypadku jest w stanie wykazać, że posiada zgodę o której mowa w pkt 2 lit. a wyrażoną zarówno w formie pisemnej, jak i elektronicznej.

3. **Zasada celowości:**
   1) Zbieranie danych osobowych powinno być dokonywane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   2) Niedopuszczalne jest pominięcie albo zatajenie jakiegokolwiek z celów, do którego będą przetwarzane dane osobowe.
   3) Cele przetwarzania nie mogą być podane w sposób ogólnikowy.
   4) Istnieje generalny zakaz przetwarzania danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane.

5) W przypadku, gdy wyniknie potrzeba przetwarzania danych w nowym celu niż dotychczas, należy o nim poinformować w trybie, o którym mowa w § 4 ust. 1 i upewnić się, że istnieje do niego podstawa prawna.
6) Dalsze przetwarzanie danych osobowych lub szczególnych kategorii danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych uznawane jest za operacje przetwarzania zgodne z prawem i z pierwotnymi celami, jednak z poszanowaniem zasady adekwatności wyrażonej w ust. 4.

4. **Zasada adekwatności (minimalizacji, proporcjonalności):**
   1) Zbierane dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Współadministratorzy powinni przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych.
   2) Adekwatność danych powinna być oceniana najpóźniej w momencie ich zbierania.
   3) Zbieranie danych, które nie są potrzebne, ale mogą być użyteczne w przyszłości jest niedopuszczalne.
5. **Zasada prawidłowości (poprawności):**
   1) Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane.
   2) Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Tym samym przetwarzane dane muszą być aktualne i zgodne z prawdą.
   3) Współadministratorzy umożliwiają realizacje prawa do sprostowania i aktualizacji danych.
6. **Zasada ograniczenia czasowego (retencji danych):**
   1) Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to wyrażone w przepisach powszechnie obowiązujących lub aktach wewnętrznych, z zastrzeżeniem pkt 3.
   2) W przypadku, gdy przepisy odrębne nie ustanawiają okresu przechowywania, przechowywanie następuje według własnej oceny z zachowaniem odpowiedniej równowagi między prawami jednostki wynikającymi z obowiązujących przepisów a własnymi potrzebami związanymi z przetwarzaniem danych i osiągnięciem określonych celów przetwarzania, z zastrzeżeniem pkt 3.
   3) Dopuszcza się możliwość wyłączenia spod zasady czasowości przechowywanie danych w formie umożliwiającej identyfikację przez czas dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, jednak z poszanowaniem zasady adekwatności wyrażonej w ust. 4.
7. **Zasada bezpieczeństwa (integralności, poufności, dostępności i odpowiedniości danych):**
   1) Współadministrator drugi wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
   2) Współadministrator drugi identyfikuje ryzyka naruszenia praw lub wolności osób fizycznych przy procesach przetwarzania danych osobowych w Konsorcjum i Fundacji, o

których mowa w ust. 1 oraz dokonuje oceny skutków ich przetwarzania zgodnie z przepisami RODO.

3) Środki techniczne i organizacyjne, o których mowa w pkt 1, zakładają m.in.:
   a) pseudonimizację i szyfrowanie danych osobowych,
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) regularne testowanie, mierzenie i ocenianie skuteczności tych środków.
4) Procedury postępowania opisane w niniejszym dokumencie mają zapewnić odpowiedni stopień bezpieczeństwa danych osobowych gwarantując ich:
   a) integralność, czyli właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   b) poufność, czyli właściwość zapewniająca, że dane osobowe i informacje nie są udostępniane nieupoważnionym podmiotom;
   c) dostępność, czyli właściwość zapewniająca, że dane osobowe dostępne są w danym czasie osobom upoważnionym.

8. **Zasada domyślnej ochrony danych i ochrony danych w fazie projektowania:**
   1) Z uwzględnieniem zasad wymienionych w niniejszym paragrafie, Współadministratorzy zapewniają, że w Konsorcjum i Fundacji realizowane są domyślne zasady ochrony danych, co oznacza że domyślnie przetwarzane są tylko te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Domyślna ochrona danych osobowych odnosi się do następujących obszarów:
      a) ilości zbieranych danych osobowych,
      b) zakresu przetwarzania danych osobowych,
      c) okresu przechowywania danych osobowych,
      d) dostępności do danych osobowych,
      e) reglamentacji dostępu do danych.
   2) W celu skutecznej realizacji niniejszej zasady, Współadministratorzy zapewniają, że już na etapie projektowania nowych procedur, pojawienia się nowych procesów przetwarzania, wyboru nowych technologii związanych z przetwarzaniem danych osobowych, podpisywaniu nowych umów i innych podobnych sytuacji, wdrożą odpowiednie środki techniczne i organizacyjne odpowiadające ryzyku naruszenia praw i wolności osób, w tym pseudonimizację i szyfrowanie, a co najmniej zweryfikuje ich przydatność.
   3) Środki techniczne i organizacyjne o których mowa w pkt 2 wynikać będą z ustalonego wcześniej ryzyka.

9. **Zasada rozliczalności:**
   1) Współadministrator drugi zapewnia udokumentowany przebieg wdrażania przepisów o ochronie danych osobowych oraz wykazuje w ten sam sposób przestrzeganie wszystkich ciążących na nim obowiązków, zgodnie z przepisami powszechnie obowiązującymi.

§ 4
Obsługa praw jednostek

1. Współadministratorzy spełniają obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, poprzez:
   1) przekazywanie osobom wymaganych prawem informacji przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
   2) zapewnienie możliwości efektywnego wykonania każdego typu żądania;
   3) zapewnienie odpowiednich nakładów i procedur, aby żądania były realizowane w terminach i w sposób wymagany przez RODO;
   4) zastosowanie procedur określających tryb zgłaszania naruszeń ochrony danych i realizacji obowiązku notyfikacyjnego, zgodnie z § 10.
2. Obowiązek informacyjny o którym mowa w ust. 1 realizowany jest także wtedy, gdy:
   1) zbierane są dane o osobie z innego źródła niż ta osoba,
   2) zmieniają się cele przetwarzania danych lub dodaje się nowy cel przetwarzania,
   3) realizuje się żądanie dostępu do danych.
3. Wzór klauzuli informacyjnej stanowi załącznik nr 2.
4. Potwierdzenie tożsamości wnioskodawcy następuje w formie elektronicznej lub papierowej poprzez weryfikację co najmniej dwóch dodatkowych danych dotyczących wnioskodawcy.
5. **Dostęp do informacji:**
   1) Współadministratorzy realizując prawo dostępu do informacji na wniosek osoby, której dane dotyczą, potwierdzają lub zaprzeczają przetwarzaniu danych wnioskodawcy. W przypadku potwierdzenia, przekazuje informacje, takie jak:
      a) cele przetwarzania danych oraz podstawę prawną przetwarzania dla każdego celu,
      b) kategorie danych,
      c) odbiorcy danych osobowych lub o kategoriach odbiorców,
      d) planowany okres przechowywania danych lub kryteria jego ustalania,
      e) informacje o przysługujących prawach do sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu względem przetwarzania, skargi do organu nadzorczego,
      f) źródło pozyskania danych – w przypadku, gdy dane nie pochodzą od osoby, której dotyczą,
      g) informacje o zautomatyzowanym podejmowaniu decyzji, profilowaniu.
   2) W przypadku, gdy dane osobowe przekazywane są do państwa trzeciego lub organizacji międzynarodowej (tj. poza Europejski Obszar Gospodarczy), Współadministratorzy powiadamiają również osoby, których dane dotyczą o zastosowanych zabezpieczeniach związanych z przekazaniem.
   3) W uzasadnionych przypadkach Współadministratorzy wspólnie lub osobno mogą zwrócić się do wnioskodawcy o sprecyzowanie zakresu żądania dostępu.
   4) Na wniosek osoby, której dane dotyczą Współadministrator drugi dostarcza kopię danych podlegających przetwarzaniu realizując przy tym samym prawo dostępu do informacji. Za wszelkie kolejne kopie, Fundacja pobiera opłatę w wysokości 20 zł od kopii.
   5) W uzasadnionych przypadkach, a zwłaszcza gdy wnioskodawca składa tożsame żądanie częściej niż raz na pół roku, Współadministratorzy mają prawo odmówić realizacji prawa jednostki do dostępu lub kopii danych.
   6) Wniosek o dostęp do danych osobowych wnioskodawcy oraz o udzielenie informacji dotyczących przetwarzania danych Współadministrator Drugi realizuje niezwłocznie, jednak nie później niż w ciągu 30 dni od daty wpływu wniosku, przy czym w przypadku

udzielenia informacji o przetwarzaniu danych osobowych wnioskodawcy, termin na pełną odpowiedź może w uzasadnionych przypadkach ulec przedłużeniu o kolejne 2 miesiące.

7) Przekazanie informacji może nastąpić zarówno w formie elektronicznej, jak i papierowej.

6. **Sprostowanie danych:**
   1) Osobie, której dane dotyczą przysługuje prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
   2) Osobie, której dane dotyczą przysługuje prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
7. **Prawo do bycia zapomnianym:**
   1) Osobie, której dane dotyczą przysługuje prawo żądania od współadministratorów niezwłocznego usunięcia jej danych osobowych, w przypadku gdy:
      a) dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
      b) nastąpi cofnięcie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy jednoczesnym braku innej podstawy prawnej przetwarzania;
      c) nastąpi wniesienie sprzeciwu wobec przetwarzania przy jednoczesnym braku nadrzędnych uzasadnionych podstaw prawnych przetwarzania;
      d) dane osobowe były przetwarzane niezgodnie z prawem;
   2) W przypadku realizacji prawa do bycia zapomnianym, Współadministrator drugi ma obowiązek:
      a) usunąć dane osobowe wnioskodawcy;
      b) poinformowania o usunięciu odbiorców danych, jeżeli dane te zostały im przekazane;
      c) domagania się usunięcia danych od innych administratorów przetwarzających te dane, gdy dane te zostały upublicznione;
      d) na żądanie osoby poinformować ją o odbiorcach którym zostały przekazane dane podlegające usunięciu.
8. **Ograniczenie przetwarzania:**
   1) Osoba, której dane dotyczą może żądać od Współadministratorów ograniczenia przetwarzania w następujących przypadkach:
      a) osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić Współadministratorom prawidłowość tych danych;
      b) przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania;
      c) Współadministratorzy nie potrzebują już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
      d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia czy istnieją prawnie uzasadnione podstawy po stronie Współadministratorów, nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
   2) Dane osobowe, co do których nastąpiło ograniczenie przetwarzania można przetwarzać w następujących przypadkach:
      a) wyłącznie za zgodą osoby, której dane dotyczą;
      b) w celu ustalenia, dochodzenia lub obrony roszczeń;

c) w celu ochrony praw innej osoby fizycznej lub prawnej;
d) z uwagi na ważne względy interesu publicznego.

3) Przed uchyleniem ograniczenia przetwarzania Współadministrator drugi informuje o tym osobę, której dane dotyczą, a która żądała ograniczenia przetwarzania danych.
4) Ograniczenie przetwarzania nie obejmuje procesu przechowywania danych osobowych.

9. **Przenoszenie danych:**
   1) Osoba, której dane dotyczą ma prawo:
      a) otrzymać w formie papierowej lub elektronicznej dane osobowe jej dotyczące, które dostarczyła Współadministratorom;
      b) przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Współadministratorów.
   2) Z prawa do przenoszenia danych osoba, której dane dotyczą może skorzystać w przypadku:
      a) przetwarzania danych odbywającego się na podstawie zgody na przetwarzanie danych osobowych lub na podstawie umowy, której stroną jest wnioskodawca;
      b) przetwarzania danych w sposób zautomatyzowany.
   3) Wykonując prawo do przenoszenia danych wnioskodawca ma prawo żądania, aby dane osobowe zostały przesłane przez Współadministratorów bezpośrednio innemu administratorowi (w przypadku gdy jest to technicznie możliwe).

10. **Sprzeciw wobec przetwarzania:**
    1) Osoba, której dane dotyczą ma prawo, z przyczyn związanych z jej szczególną sytuacją, z zastrzeżeniem pkt 2, wnieść sprzeciw wobec przetwarzania danych osobowych w jednym z następujących przypadków:
       a) przetwarzania niezbędnego do wykonania zadania realizowanego w interesie publicznym;
       b) przetwarzania w ramach sprawowania władzy publicznej powierzonej Współadministratorom;
       c) przetwarzania niezbędnego do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Współadministratorów lub przez stronę trzecią.
    2) Wnioskodawca nie może skutecznie wnieść sprzeciwu wobec przetwarzania w sytuacji, gdy jego interesy lub podstawowe prawa i wolności mają charakter podrzędny nad interesami wskazanymi w pkt 1.
    3) W przypadku wniesienia sprzeciwu Współadministratorom nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

§ 5
Uprawnienia i odpowiedzialność

1. Współadministratorzy reprezentowani przez Współadministratora Drugiego realizują zadania w sprawach z zakresu ochrony danych osobowych. Do najważniejszych obowiązków Współadministratora drugiego należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z przepisami powszechnie obowiązującymi;

2) zapewnienie przetwarzania danych zgodnie z prawem oraz uregulowaniami Wspólnej Polityki i innymi dokumentami wewnętrznymi;
3) zapewnienie adekwatnych do zagrożeń i kategorii przetwarzanych danych osobowych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w Konsorcjum i Fundacji;
4) wydawanie i cofanie upoważnień do przetwarzania danych osobowych;
5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
6) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
7) nadzór nad bezpieczeństwem danych osobowych;
8) kontrola działań jednostek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
9) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

2. Do prowadzenia rejestru czynności przetwarzania stanowiącego załącznik nr 3, który jest zbiorem wszystkich związanych z przetwarzaniem danych działań, zobowiązani są:
   1) kierownicy podstawowych jednostek organizacyjnych;
   2) kierownicy jednostek organizacyjnych administracji centralnej, jednostek ogólnouczelnianych i jednostek międzywydziałowych;

§ 6
Upoważnienie do przetwarzania danych osobowych

1. Upoważnienie do przetwarzania danych osobowych.
   1) Do przetwarzania danych osobowych w systemie tradycyjnym mogą być dopuszczone osoby posiadające upoważnienie wydane przez współadministratorów.
   2) Upoważnienia wydawane są:
      a) pracownikom;
      b) członkom organów statutowych Fundacji lub Konsorcjum
      c) innym osobom, które na mocy stosunku prawnego, łączącego ich z Współadministratorami, przetwarzają dane osobowe w systemach informatycznych.
   3) Osobom, o których mowa w pkt 2, upoważnienie wydaje się przy łącznym spełnieniu następujących przesłanek:
      a) przed przystąpieniem do przetwarzania danych osobowych;
      b) po podpisaniu oświadczenia, którego treść zobowiązuje do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Tajemnica obowiązuje zarówno w trakcie trwania stosunku prawnego ze Współadministratorami, jak i po jego ustaniu. Wzór oświadczenia stanowi załącznik nr 5;
   4) Upoważnienie ważne jest na obszarze całego Konsorcjum i Fundacji. Obowiązuje ono na czas trwania stosunku prawnego łączącego osobę, o której mowa w pkt 2 z ze Współadministratorami.
   5) Wzór upoważnienia stanowi załącznik nr 4.

6) Istnieje generalny zakaz przetwarzania danych osobowych w zakresie szerszym niż wynika to z realizacji czynności zleconych przez Współadministratorów.
7) Cofnięcie upoważnienia do przetwarzania danych następuje:
   a) wraz z rozwiązaniem stosunku prawnego łączącego ze Współadministratorami;
   b) na umotywowany wniosek bezpośredniego przełożonego;
   c) w przypadku stwierdzenia zawinionego naruszenia ochrony danych osobowych.
8) Współadministratorzy zlecają prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych osobie do tego wyznaczonej.
9) Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie papierowej lub elektronicznej. Zawiera ona aktualny stan nadanych i cofniętych upoważnień do przetwarzania danych. Ewidencja powinna zawierać:
   a) imię i nazwisko osoby upoważnionej;
   b) stanowisko lub funkcję;
   c) datę nadania i cofnięcia upoważnienia;
10) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 6.

§ 7
Powierzenie przetwarzania danych

1. W celu powierzenia podmiotom zewnętrznym przetwarzania danych osobowych będących w posiadaniu Współadministratorów, zawierane są umowy na powierzenie przetwarzania danych osobowych. Wzór umowy stanowi załącznik nr 6.
2. Uprawniony do zawierania umów powierzenia przetwarzania danych osobowych jest Zarząd Fundacji.

§ 8
Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych i informacji w systemie tradycyjnym

1. **Zabezpieczenie danych osobowych i informacji:**
   1) Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i informacje odpowiedzialne są osoby je przetwarzające oraz zarząd fundacji.
   2) Wszystkie dane, o których mowa w ust. 1, powinny być zabezpieczone fizycznie przed osobami nieupoważnionymi oraz przechowywane w urządzeniach gwarantujących dostęp do nich wyłącznie uprawnionych pracowników, tj. przynajmniej w pomieszczeniach zamykanych na klucz, z zastosowaniem dodatkowego zabezpieczenia w postaci szafy drewnianej zamykanej na klucz lub szafy metalowej - w odniesieniu do szczególnie istotnych dla działalności Konsorcjum i Fundacji danych.
   3) Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu członków zarządu fundacji, którzy ponoszą pełną odpowiedzialność za ich odpowiednie zabezpieczenie.
   4) Pomieszczenia, w których przetwarzane są dane osobowe i informacje, zabezpieczone są na czas nieobecności osób uprawnionych do przetwarzani danych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

5) Dostęp do kluczy od pomieszczeń, w których przetwarzane są dane osobowe i informacje, posiadają wyłącznie osoby uprawnione przez zarząd fundacji.

2. **Postępowanie z danymi osobowym i informacjami:**
   1) Współadministratorzy zobowiązani są stosować „politykę czystego biurka". Polega ona na utrzymywaniu porządku na stanowisku pracy pod ich nieobecność, poprzez umieszczanie dokumentów w szafie lub szufladzie zamykanej na klucz.
   2) Dokumentacja zawierająca dane osobowe lub informacje podlega archiwizacji zgodnie z przepisami powszechnie obowiązującymi i aktami wewnątrzzakładowymi.
   3) Współadministratorzy zobowiązani są porządkować dokumentację pod względem jej użyteczności. Polega to na niszczeniu wszelkiej dokumentacji roboczej lub tymczasowej, zawierającej dane osobowe lub informacje niezwłocznie po ustaniu celu przetwarzania. Niszczenie polega w szczególności na:
      a) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami przy użyciu niszczarki lub innych skutecznych metod w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane,
      b) anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
   4) Współadministratorzy zobowiązani są do przewożenia, przenoszenia i przekazywania dokumentów w sposób zapobiegający ich kradzieży, zagubieniu, utracie i dostępu osób nieupoważnionych.

§ 9

Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych i informacji w systemie informatycznym

1. **Zabezpieczenie systemów informatycznych przed osobami nieupoważnionymi:**
   1) Wszelkie urządzenia i nośniki zawierające dane osobowe lub informacje, takie jak serwery, komputery główne, urządzenia teletransmisyjne, szafy z nośnikami magnetycznymi zawierające kopie danych powinny być usytuowane w pomieszczeniach uniemożliwiających dostęp do nich osób nieupoważnionych.
   2) Wyłączniki oraz zabezpieczenia zasilania elektrycznego, w już użytkowanych obiektach, powinny być zabezpieczone przed dostępem osób nieupoważnionych. W obiektach nowobudowanych lub modernizowanych wymaga się zabezpieczenia tablic zgodnie z obowiązującymi przepisami nadrzędnymi.
   3) Dostęp do pomieszczeń, w których odbywa się przetwarzanie danych osobowych i informacji winien być ściśle kontrolowany poprzez stosowane zabezpieczenia organizacyjne i mechaniczne oraz zainstalowane systemy alarmowe.
   4) System informatyczny służący do przetwarzania danych osobowych i informacji zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

5) System informatyczny służący do przetwarzania danych osobowych i informacji chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
6) W przypadku zastosowania zabezpieczeń logicznych obejmują one:
   a) kontrolę przepływu informacji pomiędzy systemem informatycznym wykorzystywanym w Konsorcjum i Fundacji a siecią publiczną;
   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
7) Współadministratorzy wdrażają odpowiednie środki techniczne, aby witryny internetowe za pośrednictwem których uzyskuje się zgody na przetwarzanie danych osobowych odpowiadały wymogom o których mowa w § 3 ust. 2 pkt 5. [M1]
8) W przypadku wykorzystywania do przetwarzania danych osobowych lub informacji komputerów przenośnych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i używania, w tym stosowania środków ochrony kryptograficznej. Użytkownik komputera przenośnego odpowiada za powierzone mu urządzenie oraz wszelkie operacje wykonywane przy jego użyciu.
9) Komputery przenośne wykorzystywane do przetwarzania danych osobowych lub informacji, po zakończonej pracy, powinny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Za właściwe zabezpieczenie przedmiotowych urządzeń odpowiedzialni są ich użytkownicy.
10) Usytuowanie urządzeń komputerowych (komputerów typu PC, drukarek) powinno uniemożliwiać dostęp do nich osób nieuprawnionych oraz wgląd do danych wyświetlanych na monitorach komputerowych.
11) W przypadku oddalenia się pracownika od stanowiska pracy należy pozostawić system w takim stanie, aby osoby nieupoważnione nie miały do niego dostępu. W tym celu konieczne jest zablokowanie ekranu komputera oraz stosowanie chronionych hasłem wygaszaczy ekranu z odpowiednim czasem nieaktywności do ich uruchomienia (nie dłuższym niż 10 minut).
12) W przypadku naprawy sprzętu komputerowego dane osobowe lub informacje należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza jednostką, w której przetwarzane są dane osobowe, po zabezpieczeniu należy je usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną do przetwarzania danych.
13) Szczególnemu nadzorowi podlegają w Fundacji urządzenia umożliwiające tworzenie i przenoszenie dużych ilości danych, w tym nagrywarki DVD oraz nośniki typu pendrive, a także nośniki komputerowe zawierające dane osobowe lub informacje. Do ich ochrony i zabezpieczenia zobowiązani są wszyscy ich użytkownicy.
14) W przypadku uszkodzenia nośników komputerowych, o których mowa w pkt 13, użytkownicy zobowiązani są do ich przekazania do właściwych służb informatycznych w celu ich zniszczenia.
15) Uszkodzone nośniki komputerowe (w tym dyski twarde), zawierające dane osobowe lub informacje, powinny być fizyczne niszczone w sposób uniemożliwiający dostęp do danych osób nieupoważnionych. Do czasu zniszczenia nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.
16) Dopuszcza się ponowne wykorzystanie urządzeń i nośników komputerowych zawierających dane osobowe lub informacje.

17) Urządzenia i nośniki komputerowe zawierające dane osobowe i informacje, przeznaczone do ponownego wykorzystania lub przekazania innemu podmiotowi należy – przed ich wykorzystaniem lub przekazaniem – pozbawić zapisu w sposób gwarantujący trwałe usunięcie danych (za pomocą specjalistycznego oprogramowania).

2. **Wymogi dotyczące haseł:**
   1) Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.
   2) Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
   3) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
   4) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
   5) W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
   6) Przy wyborze hasła obowiązują następujące zasady:
      a) minimalna długość hasła – 8 znaków,
      b) właściwa złożoność hasła – litery wielkie i małe oraz cyfry i znaki specjalne, o ile system informatyczny na to pozwala.
   7) Zakazuje się stosować haseł:
      a) które użytkownik stosował uprzednio,
      b) będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
      c) analogicznych jak identyfikator,
      d) zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci, itp.,
      e) stanowiące przewidywalne sekwencje znaków, np. 12345678 lub qwertyui.
   8) Zmiany hasła nie należy zlecać innym osobom.
   9) W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

3. **Tworzenie i przesyłanie plików:**
   1) Nie tworzy się plików o charakterze baz danych (np. pliku excel) bez powodów.
   2) Przed wysłaniem pliku zawierającego dane osobowe należy go odpowiednio zabezpieczyć poprzez zaszyfrowanie hasłem. Hasło należy przesłać odbiorcy pliku inną drogą komunikacji.
   3) Zabrania się podłączania do służbowego sprzętu komputerowego obcych nośników danych. O znalezionym lub zgubionym wymiennym nośniku danych typu Pendrive, zawierającym dane osobowe należy powiadomić Współadministratorów.
   4) Zobowiązuje się pracowników do przesyłania elektronicznej korespondencji służbowej wyłącznie za pośrednictwem fundacyjnej skrzynki pocztowej.
   5) W przypadku przesyłania korespondencji elektronicznej należy ukrywać listę innych odbiorców poprzez wpisywanie adresu w polu UDW lub BCC.

§ 10

Postępowanie w przypadku naruszenia ochrony danych osobowych lub bezpieczeństwa informacji

1. Do zdarzeń mogących prowadzić do naruszenia ochrony danych osobowych i informacji zalicza się m.in.:
   1) kradzież danych w każdej formie,
   2) nieumyślną lub celową modyfikację danych, zarówno w formie elektronicznej i papierowej,
   3) utratę danych,
   4) włamania do systemu poprzez programy, takie jak:
      a) wirus,
      b) koń trojański,
      c) makro,
      d) bomba logiczna,
   5) awarie sprzętu lub uszkodzenie oprogramowania,
   6) utratę zasilania powodującą przerwę w pracy systemów,
   7) zabór sprzętu lub nośników z ważnymi danymi,
   8) nieprzestrzeganie postanowień Wspólnej Polityki,
   9) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych, zjawiska takie jak: naturalne katastrofy, działania silnych pól elektromagnetycznych, przechwycenie transmisji danych, odczyt z monitora komputera przez osoby nieuprawnione, zauważenie śladów usiłowania lub dokonania włamania do pomieszczenia lub szafy z danymi.
2. Współadministratorzy w przypadku pozyskania wiedzy o fakcie bezprawnego przetwarzania, ujawnienia lub nienależytego zabezpieczenia danych osobowych przed osobami nieuprawnionymi, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo wystąpienia naruszenia, o którym mowa w ust. 1, lub zasad ochrony danych osobowych, o których mowa w § 3, zobowiązany jest niezwłocznie poinformować Prezesa Zarządu Fundacji lub bezpośredniego przełożonego.
3. Z chwilą uzyskania informacji, o której mowa w ust. 2, bezpośredni przełożony niezwłocznie informuje o tym Prezesa Zarządu, a także:
   a) podejmuje czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
   b) podejmuje czynności zmierzające do ustalenia przyczyn zdarzenia i sprawców,
   c) rozważa wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   d) zaniecha dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie zdarzenia i jego analizę, o ile to możliwe,
   e) dokumentuje w formie notatki służbowej zaistniałe zdarzenie, w której wskazuje na podjęte w tej kwestii czynności.
4. Obowiązek informacyjny, o którym mowa w ust. 2 i 3, powinien zostać zrealizowany najpóźniej następnego dnia roboczego po dniu powzięcia informacji o potencjalnym lub zaistniałym naruszeniu ochrony danych osobowych.
5. Dopuszcza się możliwość przeprowadzenia postępowania wyjaśniającego przez Prezesa Zarządu przy czym po uzyskaniu informacji, o której mowa w ust. 2, w pierwszej kolejności ustala, czy zaistniałe zdarzenie skutkuje naruszeniem praw lub wolności osób fizycznych.
6. W ramach postępowania wyjaśniającego podejmowane są czynności mające na celu wyjaśnienie okoliczności danego zdarzenia, w szczególności:

1) ustalenie czasu wystąpienia naruszenia, jego zakresu, przyczyn, skutków oraz wielkości szkód, które zaistniały;
2) ustalenie osoby odpowiedzialnej za naruszenie;
3) podjęcie działań w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości;
4) wyciągnięcie konsekwencji w stosunku do osoby ponoszącej odpowiedzialność za zdarzenie, przy czym zgodnie z przepisami powszechnie obowiązującymi z tytułu przedmiotowych naruszeń możliwa jest odpowiedzialność dyscyplinarna, cywilna lub karna;
5) zaopiniowanie czy Współadministratorzy są zobowiązani zgłosić sprawę organom ścigania.

7. Współadministratorzy po uzyskaniu informacji o stwierdzonym naruszeniu ochrony danych osobowych lub incydencie, które skutkuje naruszeniem praw i wolności osób fizycznych albo jest wysoce prawdopodobne, w terminie 72 godzin od stwierdzenia naruszenia ochrony danych zawiadamiają Prezesa Urzędu Ochrony Danych.
8. Osoba wyznaczona przez Prezesa Zarządu prowadzi rejestr naruszeń ochrony danych i bezpieczeństwa informacji, stanowiący złącznik nr 8.

§ 11
Postanowienia końcowe

1. Do kontroli stanu ochrony danych osobowych w jednostkach organizacyjnych Konsorcjum i Fundacji uprawnieni są:
    1) Współadministratorzy,
    2) Prezes Zarządu Fundacji
    3) Członek zarządu Fundacji
    4) Pozostali członkowie organów statutowych fundacji upoważnieni przez osoby wymienione w pkt 2-4.
2. Współadministratorzy dbają o zapoznanie pracowników ze Wspólną Polityką i jej przestrzeganie.

Załącznik Nr 1
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Projekt klauzuli zgody na przetwarzanie danych osobowych zwykłych

Zgoda na przetwarzanie danych osobowych zwykłych

Wyrażam zgodę na przetwarzanie danych osobowych przez **Konsorcjum Bezpieczeństwo Gospodarcze Polski** oraz **Fundację Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych** z siedzibą przy ul. Chopina 29/9A , 20-023 Lublin w związku z członkostwem w Konsorcjum Bezpieczeństwo Gospodarcze Polski, w celu podtrzymania kontaktu z Państwem, przygotowania oferty i realizacji celów statutowych Fundacji jak i Konsorcjum. Podstawą przetwarzania Państwa danych jest wyrażona dobrowolnie zgoda.

Informujemy, że Państwa zgoda może zostać cofnięta w dowolnym momencie przez dostarczenie wypełnionego i własnoręcznie podpisanego formularza cofnięcia zgody do siedziby (w formie tradycyjnej lub w formie skanu) Fundacji, który można pobrać ze strony www.konsorcjumbgp.pl/think-thank/rodo. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie Państwa zgody przed jej wycofaniem.

……
data, własnoręczny podpis

Załącznik Nr 2
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Informacja o przetwarzaniu danych osobowych

I. Administrator danych osobowych:
Współadministratorami Państwa danych osobowych są Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych z siedzibą w Lublinie przy Chopina 29/9A , 20-023 Lublin. Ze Współadministratorami można się skontaktować pod wskazanym wyżej adresem korespondencyjnym lub pod adresem poczty elektronicznej: fundacja@konsorcjumbgp.pl.

II. Cele i podstawy przetwarzania:
1) w związku z członkostwem w Konsorcjum Bezpieczeństwo Gospodarcze Polski w celu podtrzymania kontaktu z Państwem, przygotowania oferty i realizacji celów statutowych Fundacji jak i Konsorcjum, w takim wypadku podstawą przetwarzania jest realizacja prawnie dopuszczalnych celów administratora.
2) w celu podtrzymania kontaktu z Państwem w związku z zapytaniem, które skierowaliście Państwo drogą elektroniczną lub tradycyjną, w tym także w celu przygotowania oferty i realizacji umowy, w takim wypadku podstawą przetwarzania jest realizacja prawnie dopuszczalnych celów administratora oraz Państwa zgoda,
3) w przypadku pozyskania kontaktu od osoby trzeciej (np. członka Konsorcjum) lub z powszechnie dostępnych źródeł w celu realizacji prawnie usprawiedliwionych celów Fundacji, w tym realizacji usług na rzecz członków Fundacji, zgodnie z umową,
4) w przypadku pozyskania danych od Państwa pracodawcy lub zleceniodawcy, w celu kontaktu z Państwem w związku z realizacją usług,

III. Kategorie przetwarzanych danych:
Podstawowe dane identyfikacyjne, dane identyfikacyjne przyznane przez organy publiczne, elektroniczne dane identyfikacyjne, funkcje społeczne, wyróżnienia, dane kontaktowe, doświadczenie zawodowe, edukacja i szkolenia, nauczanie akademickie, publikacje, aktualne zatrudnienie, nagrania wideo, wizerunek, nagrania dźwięku.

IV. Odbiorca danych:
marketingowe i innym niezależnym odbiorcom, których oferta uzupełnia naszą; partnerom, których oferta uzupełnia naszą lub którzy są partnerami organizowanych przez nas przedsięwzięć; sponsorom organizowanych przez nas przedsięwzięć; członkom Konsorcjum Bezpieczeństwo Gospodarcze Polski.

V. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych:
Nie przekazujemy Państwa danych poza teren Polski, Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego.

VI. Okres przechowywania danych:
Państwa dane pozyskane w celu złożenia deklaracji członkostwa w Konsorcjum Bezpieczeństwo Gospodarcze Polski przechowujemy przez okres trwania członkostwa oraz do końca roku kalendarzowego następującego po roku, w którym ostatni raz się Państwo z nami kontaktowali;

Państwa dane pozyskane w celu zawarcia umowy współpracy przechowujemy przez okres negocjowania umowy oraz do końca roku kalendarzowego następującego po roku, w którym ostatni raz się z nami Państwo kontaktowali w sprawie jej zawarcia;

Państwa dane pozyskane w związku z zawarciem umowy przetwarzamy do końca okresu przedawnienia potencjalnych roszczeń z umowy;

Państwa podstawowe dane kontaktowe przechowujemy dla potrzeb marketingu bezpośredniego naszych produktów i usług do czasu, aż zgłoszą Państwo sprzeciw względem ich przetwarzania w tym celu, cofną zgodę, jeśli przetwarzaliśmy je na podstawie tzw. zgody marketingowej, lub sami ustalimy, że się zdezaktualizowały.

VII. Przysługujące Państwu prawa:
a) dostępu do wglądu do swoich danych oraz otrzymania ich kopii,
b) sprostowania danych,
c) usunięcia danych,

Bez Państwa wiedzy i zgody nie udostępniamy nikomu danych osobowych. Jednak, w niezbędnym zakresie, w trosce o najwyższą jakość świadczonych przez Konsorcjum i Fundację usług, mogą one zostać udostępnione: podmiotom, z których usług korzystamy przy ich przetwarzaniu: np. firmy księgowe, prawnicze, informatyczne, likwidatorzy szkód, agencje

d) ograniczenia przetwarzania danych,
e) wniesienia sprzeciwu wobec przetwarzania danych,
f) przenoszenia danych,
g) wniesienia skargi do organu nadzorczego,
h) cofnięcia zgody na przetwarzanie danych osobowych.

W celu realizacji wymienionych praw, prosimy aby Państwo zgłosili przysługujące żądanie Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogi i Analiz Prawno-Gospodarczych. Na stronie: www.konsorcjumbgp.pl/think-thank/rodo znajdą Państwo przewidziane ku temu procedury.

VIII. Informacja o wymogu/dobrowolności podania danych

Podanie przez Państwa danych jest:

- warunkiem złożenia deklaracji członkostwa w Konsorcjum
- wymogiem zawarcia umowy współpracy,
- dobrowolne

Jeżeli nie podasz danych:

- możemy odmówić przyjęcia Cię w poczet członków Konsorcjum
- możemy odmówić zawarcia umowy,
- możemy odmówić naszego świadczenia.

IX. Informacja o źródle danych

Państwa dane uzyskaliśmy bezpośrednio od Państwa, od firmy będącej członkiem Konsorcjum, jego partnera, a także ze strony internetowej Państwa firmy, Państwa publicznego profilu LinkedIn, Państwa publicznego profilu Facebook oraz z przeglądu Krajowego Rejestru Sądowego, CEIDG oraz innych publicznych źródeł.

X. Zmiany polityki prywatności

Zastrzegamy sobie prawo do zmiany powyższej polityki prywatności poprzez przesłanie do Państwa nowej polityki prywatności za pośrednictwem poczty mail.

Załącznik Nr 3
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Rejestr czynności przetwarzania - wzór

Lp.	Czynność przetwarzania	Cel przetwa-rzania	Kategorie osób	Kategorie danych	Kategorie odbiorców	Termin usunięcia danych	Transfer do kraju trzeciego lub organizacji międzynarodowej	Środki bezpieczeństwa
1								
2								
3								
4								
5								

Załącznik Nr 4
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Lublin, dnia …….

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
Nr …….

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – zwanym dalej RODO – upoważniam Panią/Pana:

……
(imię i nazwisko)

……

(stanowisko/funkcja)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku/w ramach członkostwa w organach Konsorcjum/Fundacji*.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z przepisami o ochronie danych osobowych (RODO i ustawą o ochronie danych osobowych), przepisami Kodeksu pracy, a także Wspólną Polityką Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych.

Upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych.

Niniejsze upoważnienie ważne jest na czas trwania stosunku prawnego/członkostwa w organach statutowych Konsorcjum lub Fundacji* łączącego Panią/Pana z Konsorcjum lub Fundacją Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych., na mocy którego zostało wydane niniejsze upoważnienie.

*** Niepotrzebne skreślić.**

……
(Podpis osoby uprawnionej do nadania upoważnienia)

Cofnięto, dnia …….

……
(Podpis osoby uprawnionej do cofnięcia upoważnienia)

Załącznik Nr 5
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Lublin, dnia …….

OŚWIADCZENIE O ZACHOWANIU W TAJEMNICY DANYCH OSOBOWYCH I INFORMACJI ORAZ SPOSOBÓW ICH ZABEZPIECZENIA

W związku z dopuszczeniem do przetwarzania danych osobowych i informacji oświadczam, że:

1. Zapoznałem się i zobowiązuję się do przestrzegania obowiązków wynikających z przepisów powszechnie obowiązujących z zakresu ochronnych danych osobowych, a także regulacji wewnętrznych Współadministratorów obowiązujących w obszarze przetwarzania danych osobowych, a w szczególności Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych.
2. Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją i zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
3. Zachowam w tajemnicy dane osobowe i informacje oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z administratorem danych, jak i po jej zakończeniu.
4. Znane mi są zasady odpowiedzialności prawnej za niezgodne z prawem przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u Administratora Danych, a także Kodeksu Pracy i Kodeksu Cywilnego.
5. Oświadczam, że treść niniejszego oświadczenia jest mi znana i zrozumiała, a także zobowiązuję się do jego przestrzegania.

……..…….
(podpis osoby składającej oświadczenie)

Załącznik Nr 6
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Ewidencja osób upoważnionych do przetwarzania danych

Imię i nazwisko	Data nadania	Data cofnięcia	Stanowisko/Funkcja

Załącznik Nr 7
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Wzór umowy powierzenia przetwarzania danych osobowych

zawarta w Lublinie w dniu ……. r. pomiędzy:

Fundacją Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych, siedzibą przy ul. Chopina 29/9A , 20-023 Lublin, zwanym w dalszej części umowy „**Administratorem**”**,** reprezentowanym przez:

……

a

……..(dane podmiotu który umowę zawiera), zwanym w dalszej części umowy „**Podmiotem przetwarzającym**”, reprezentowanym przez:

……

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane:…….. (należy podać rodzaj danych np. dane zwykłe oraz dane

szczególnych kategorii, należy podać kategorię osób, których dane dotyczą oraz w jakiej są postaci np. imion i nazwisk, nr PESEL itp.).

2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu :……..(należy podać cel przetwarzania danych przez podmiot przetwarzający np. realizacji umowy nr …… z dnia……..).

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem **usuwa/ zwraca** Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. Strony zobowiązują się do wzajemnej współpracy w zakresie przetwarzania danych osobowych objętych niniejszą Umową, w szczególności Strony zobowiązują się do współpracy w zakresie realizacji obowiązku udzielania odpowiedzi na zapytania osób, których dane osobowe są przetwarzane oraz wywiązywania się z obowiązków, o których mowa w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.

§ 4

Kontrola

1. Administrator ma prawo przeprowadzenia kontroli, czy środki bezpieczeństwa, o których mowa w § 3 ust.1, spełniają umowne i ustawowe warunki. O skorzystaniu z prawa przeprowadzenia kontroli, Administrator powinien uprzedzić Podmiot przetwarzający z co najmniej 3-dniowym wyprzedzeniem kierując w tym celu do Podmiotu przetwarzającego stosowne pisemne zawiadomienie. Po otrzymaniu zawiadomienia, Podmiot przetwarzający

może wystąpić z wnioskiem o przeprowadzenie kontroli w terminie szybszym niż wyznaczony.
2. Kontrolę, o której mowa w ust. 1, Administrator winien przeprowadzić mając na uwadze godziny pracy Podmiotu przetwarzającego, w sposób możliwie niezakłócający pracy.
3. Podczas kontroli, Podmiot przetwarzający zobowiązuje się udostępnić Administratorowi wszelkie dane pozwalające na ocenę adekwatności zastosowanych środków bezpieczeństwa do istniejącego ryzyka, w szczególności udostępnić: kartoteki, bazy danych itp.
4. Podmiot przetwarzający zobowiązuje się do usunięcia wszelkich uchybień stwierdzonych podczas kontroli i opisanych w pokontrolnym protokole. Usunięcie uchybień powinno nastąpić nie później niż w terminie 7 dni od zakończenia kontroli i przedstawienia przez Administratora protokołu pokontrolnego.

§ 5

Podpowierzenie danych osobowych

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Umowa o dalsze powierzenie danych osobowych może zostać zawarta wyłącznie w celu wykonania niniejszej Umowy i może obejmować jedynie te dane - ich rodzaj, zakres oraz cel przetwarzania - o których mowa w umowie zawartej z Podmiotem przetwarzającym.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot Przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego Unii Europejskiej, któremu podlega Podmiot przetwarzający. W takim przypadku, przed rozpoczęciem przetwarzania, Podmiot przetwarzający informuje Administratora o tym obowiązku, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie, a także dawać gwarancję należytego wykonania obowiązków ochrony danych osobowych.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią niniejszej Umowy, a w szczególności za udostępnienie powierzonych danych do przetwarzania osobom nieuprawnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych

określonych w niniejszej Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania w ramach niniejszej Umowy danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.

3. W przypadku podjęcia przez osobę trzecią działań prawnych wobec Podmiotu przetwarzającego i/lub Administratora związanych z naruszenia zasad przetwarzania danych osobowych, Podmiot przetwarzający będzie współpracować z Administratorem w celu podjęcia stosownych kroków prawnych zmierzających w szczególności do oddalenia bądź odrzucenia przez właściwy sąd roszczeń osoby trzeciej, wniesienia środka odwoławczego lub zawarcia ugody, jak również innych działań prawnych.

§ 7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony od ….. do …../obowiązywania umowy podstawowej nr ……..

2. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem miesięcznego okresu wypowiedzenia/razem z umową podstawową nr …. z dnia ……. w przewidzianym przez nią terminie.
3. Administrator może rozwiązać niniejszą Umowę wraz z umową podstawową nr … z dnia …… ze skutkiem natychmiastowym, w przypadku gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, o której mowa w § 4 niniejszej Umowy nie usunie ich w wyznaczonym terminie,
b) przetwarza dane osobowe niezgodnie z postanowieniami niniejszej Umowy,
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, a które to dane są związane z niniejszą Umową (dalej zwane **„Informacjami Poufnymi”**).
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy Informacji Poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów jak i z niniejszej Umowy.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do obioru, przekazywania oraz przechowywania Informacji Poufnych gwarantowały ich zabezpieczenie, w tym w szczególności zabezpieczenie danych osobowych powierzonych do przetwarzania przed dostępem osób trzeci nieupoważnionych do zapoznania się z ich treścią.

§ 9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych w niniejszej Umowie zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla Administratora.

Załącznik Nr 8
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Rejestr naruszeń ochrony danych osobowych i bezpieczeństwa informacji – wzór

Lp.	Naruszenie (opis)	Data i godzina zgłoszenia podejrzenia naruszenia	Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres którego naruszenie dotyczy	Kategoria i liczba osób, których naruszenie dotyczy	Zakres danych i kategorie danych, których dotyczy naruszenie	Źródło informacji o naruszeniu	Miejsce naruszenia	Opis skutków-konsekwencji naruszenia	Opis możliwego naruszenia praw lub wolności	Okoliczności naruszenia (opis naruszenia, przyczyny, analiza zdarzenia)
1											
2											
3											
4											
5											

Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania naprawcze (opis środków zastosowanych lub proponowanych do wdrożenia)	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania UODO? (data i godzina zgłoszenia, jeżeli dotyczy - wyjaśnienie)	Czy poinformowano organy ścigania? (data zawiadomienia)	Czy zachodzi obowiązek poinformowania osoby/osób, których dotyczy naruszenie (sposób przekazania informacji)	Monitoring działań naprawczych

Załącznik Nr 9
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Polityka Cookies

1. Strona internetowa www.konsorcjumbgp.pl nie zbiera w sposób automatyczny żadnych informacji, z wyjątkiem informacji zawartych w plikach cookies.
2. Pliki cookies (tzw. „ciasteczka") stanowią dane informatyczne, w szczególności pliki tekstowe, które przechowywane są w urządzeniu końcowym Użytkownika Serwisu i przeznaczone są do korzystania ze stron internetowych Serwisu. Cookies zazwyczaj zawierają nazwę strony internetowej, z której pochodzą, czas przechowywania ich na urządzeniu końcowym oraz unikalny numer.
3. Podmiotem zamieszczającym na urządzeniu końcowym Użytkownika Serwisu pliki cookies oraz uzyskującym do nich dostęp jest operator Serwisu Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych z siedzibą pod adresem ul. Chopina 29/9A , 20-023 Lublin.
4. Pliki cookies wykorzystywane są w celu:
    a. dostosowania zawartości stron internetowych Serwisu do preferencji Użytkownika oraz optymalizacji korzystania ze stron internetowych; w szczególności pliki te pozwalają rozpoznać urządzenie Użytkownika Serwisu i odpowiednio wyświetlić stronę internetową, dostosowaną do jego indywidualnych potrzeb;
    b. tworzenia statystyk, które pomagają zrozumieć, w jaki sposób Użytkownicy Serwisu korzystają ze stron internetowych, co umożliwia ulepszanie ich struktury i zawartości.
5. W ramach Serwisu stosowane są następujące rodzaje plików cookies:
    a. „niezbędne" pliki cookies, umożliwiające korzystanie z usług dostępnych w ramach Serwisu, np. uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania w ramach Serwisu;
    b. pliki cookies służące do zapewnienia bezpieczeństwa, np. wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania w ramach Serwisu;
    c. „wydajnościowe" pliki cookies, umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych Serwisu;
    d. „funkcjonalne" pliki cookies, umożliwiające „zapamiętanie" wybranych przez Użytkownika ustawień i personalizację interfejsu Użytkownika, np. w zakresie wybranego języka lub regionu, z którego pochodzi Użytkownik, rozmiaru czcionki, wyglądu strony internetowej itp.

W wielu przypadkach oprogramowanie służące do przeglądania stron internetowych (przeglądarka internetowa) domyślnie dopuszcza przechowywanie plików cookies w urządzeniu końcowym Użytkownika. Użytkownicy Serwisu mogą dokonać w każdym czasie zmiany ustawień dotyczących plików cookies. Ustawienia te mogą zostać zmienione w szczególności w taki sposób, aby blokować automatyczną obsługę plików cookies w ustawieniach przeglądarki internetowej bądź informować o ich każdorazowym

zamieszczeniu w urządzeniu Użytkownika Serwisu. Szczegółowe informacje o możliwości i sposobach obsługi plików cookies dostępne są w ustawieniach oprogramowania (przeglądarki internetowej).

Operator Serwisu informuje, że ograniczenia stosowania plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronach internetowych Serwisu.

Pliki cookies zamieszczane w urządzeniu końcowym Użytkownika Serwisu i wykorzystywane mogą być również przez współpracujących z operatorem Serwisu reklamodawców oraz partnerów.

Załącznik Nr 10
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

Klauzula informacyjna dotycząca korespondencji mailowej

Ta korespondencja, wraz z załącznikami może zawierać informacje prawnie chronione. Informujemy, iż ujawnienie tych informacji osobom trzecim lub nieuprawnione wykorzystanie ich do własnych celów jest zabronione. Jeśli nie jesteście Państwo adresatami tej wiadomości lub otrzymaliście ją przez pomyłkę, prosimy o usunięcie wszelkich kopii tej wiadomości oraz o powiadomienie o tym nadawcy przedmiotowej wiadomości. Ponadto informujemy, że w sieci publicznej zachowanie 100% bezpieczeństwa obrotu informacji jest w zasadzie niemożliwe. Korzystając z poczty elektronicznej w kontaktach z Konsorcjum i Fundacją wyrażacie Państwo zgodę na tę formę komunikacji. Jednocześnie informujmy, że zarówno Konsorcjum jak i Fundacja podejmują wszelkie niezbędne środki celem zabezpieczenia przekazywanych informacji oraz zabezpieczenia ich przed dostępem niepowołanych osób trzecich.

Administratorem danych osobowych, w tym imienia, nazwiska, adresu poczty elektronicznej, numeru telefonu, adresu IP, jest Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych, ul. Chopina 29/9A, 20-023 Lublin, NIP 7123304184.

Państwa dane osobowe są przetwarzane zależnie od sposobu ich uzyskania:

a) w celu podtrzymania kontaktu z Państwem w związku z zapytaniem, które skierowaliście Państwo drogą elektroniczną, w tym także w celu przygotowania oferty i realizacji umowy, w takim wypadku podstawą przetwarzania jest realizacja prawnie dopuszczalnych celów administratora oraz Państwa zgoda,
b) w przypadku pozyskania kontaktu od osoby trzeciej (np. członka Konsorcjum) lub z powszechnie dostępnych źródeł w celu realizacji prawnie usprawiedliwionych celów Konsorcjum i Fundacji, w tym realizacji usług na rzecz członków Konsorcjum, zgodnie z umową,
c) w przypadku pozyskania danych od Państwa pracodawcy lub zleceniodawcy, w celu kontaktu z Państwem w związku z realizacją usług,
d) w związku z członkostwem w Konsorcjum Bezpieczeństwo Gospodarcze Polski w celu podtrzymania kontaktu z Państwem, przygotowania oferty i realizacji celów statutowych Fundacji jak i Konsorcjum, w takim wypadku podstawą przetwarzania jest realizacja prawnie dopuszczalnych celów administratora.

Dane przechowywane będą do zakończenia okresu przedawnienia wszelkich roszczeń wynikłych w związku z ich pozyskaniem. Na warunkach określonych przepisami prawa macie Państwo prawo do żądania dostępu do danych osobowych, sprostowania ich, usunięcia, ograniczenia ich przetwarzania, prawo sprzeciwu wobec przetwarzania oraz prawo do żądania przeniesienia danych, prawa te mogą być ograniczone w zakresie przewidzianym przez

przepisy prawa. W celu uzyskania bardziej szczegółowej informacji zapraszamy do kontaktu pod adresem: fundacja@konsorcjumbgp.pl. Organem nadzorczym, do którego przysługuje Państwu prawo wniesienia skargi, jest Prezes Urzędu Ochrony Danych Osobowych.

Załącznik Nr 11
do Wspólnej Polityki Bezpieczeństwa Informacji Konsorcjum Bezpieczeństwo Gospodarcze Polski oraz Fundacji Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz-Prawno-Gospodarczych.

……..

(Miejscowość i data)

……

(Imię i nazwisko wnioskodawcy)

……

(Adres wnioskodawy)

……

Fundacja Bezpieczeństwo Gospodarcze Polski. Instytut Dialogu i Analiz Prawno-Gospodarczych
ul. Chopina 29/9A
20-026 Lublin

Odwołanie zgody na przetwarzanie danych osobowych

Zgodnie z art. 7 ust. 3 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 odwołuję wyrażoną przeze mnie zgodę na przetwarzanie moich danych osobowych w związku z członkostwem w Konsorcjum Bezpieczeństwo Gospodarcze Polski, w celu podtrzymania kontaktu , przygotowania oferty i realizacji celów statutowych Fundacji jak i Konsorcjum.

……

(Imię i nazwisko wnioskodawcy)