ZARZĄDZENIE NR 2
PRZEWODNICZĄCEGO NACZELNEJ KOMISJI BIOETYCZNEJ
z dnia 18.07.2023 r.
w sprawie ustalenia Polityki Ochrony Danych Osobowych
w Naczelnej Komisji Bioetycznej

Na podstawie art. 15 ust. 9 ustawy z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi (Dz. U. 2023 poz. 605) zarządza się co następuje:

§ 1 1. Ustala się politykę Danych Osobowych Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych stanowiącej załącznik do niniejszego Zarządzenia.

§ 2 1. Zarządzenie wchodzi w życie z dniem podpisania.

PRZEWODNICZĄCY NACZELNEJ KOMISJI BIOETYCZNEJ

Załącznik do Zarządzenia Nr 2
Przewodniczącego Naczelnej
Komisji Bioetycznej z dnia
18.07.2023 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH W NACZELNEJ KOMISJI BIOETYCZNEJ DO SPRAW BADAŃ KLINICZNYCH

Rozdział 1
Postanowienia ogólne

§ 1.

1. Polityka Ochrony Danych Osobowych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych, zwana dalej „Polityką", określa sposób przetwarzania danych osobowych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych, zwaną dalej „NKB", oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, dla których przewodniczący NKB jest administratorem, współadministratorem lub podmiotem przetwarzającym.

2. Celem Polityki jest zapewnienie szczególnej ochrony interesów osób, których dane osobowe są przetwarzane w NKB lub dla których przewodniczący NKB jest administratorem, współadministratorem lub podmiotem przetwarzającym, a w szczególności zapewnienie, aby dane te były:
   1) przetwarzane zgodnie z prawem;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnie z tymi celami;
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

3. Dopuszcza się tworzenie odrębnych regulacji wewnętrznych związanych z ochroną danych osobowych zgodnych z postanowieniami Polityki, których administratorem, współadministratorem lub podmiotem przetwarzającym jest przewodniczący NKB.

4. Przetwarzanie danych osobowych w NKB odbywa się, w szczególności zgodnie z:
   1) rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 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 (ogólne rozporządzenie o ochronie danych), zwanym dalej „RODO";
   2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, zwaną dalej „UODO";
   3) ustawą z dnia 21 lutego 2019 r. o Agencji Badań Medycznych;
   4) ustawą z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi;
   5) ustawą z dnia 19 kwietnia 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych);
   6) rozporządzeniem PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE; zwanym dalej „rozporządzeniem 536/2014"
   7) rekomendacjami Prezesa Urzędu Ochrony Danych Osobowych (także organu poprzedzającego);
   8) wytycznymi, zaleceniami, określonymi dobrymi praktykami Europejskiej Rady Ochrony Danych oraz wytycznymi Grupy Roboczej Art. 29.

§ 2.

Użyte w Polityce określenia i skróty oznaczają:

1) ABM – Agencję Badań Medycznych,

2) administrator (ADO) –przewodniczącego Naczelnej Komisji Bioetyczna;

3) analiza ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych (inaczej: ryzyka prywatności w związku z przetwarzaniem danych osobowych) - analizę możliwości nieosiągnięcia celów ochrony danych osobowych;

4) członek NKB –przewodniczącego NKB lub innego członka NKB;

5) dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); 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;

6) identyfikator - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika w systemie teleinformatycznym;

7) inspektor ochrony danych (IOD) - osobę wyznaczoną przez ADO, która posiada kwalifikacje zawodowe do pełnienia tej funkcji, a w szczególności posiada wiedzę, wykształcenie i praktykę w zakresie ochrony danych osobowych;

8) komórka organizacyjna właściwa do spraw kadr i płac – biuro, dział, wydział, do którego należy realizacja spraw kadrowo-pracowniczych ABM;

9) naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

10) ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych - analizę DPIA (Data Protection Impact Assessment) - której dokonuje administrator przed rozpoczęciem przetwarzania, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;

11) osoba upoważniona - użytkownika, któremu administrator udzielił imiennego upoważnienia do przetwarzania danych osobowych;

12) podmiot przetwarzający (procesor) - osobę fizyczną lub prawną, organ administracji publicznej, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

13) portal Unii Europejskiej (CTIS) - określony w art. 80 rozporządzenia 536/2014, jeden punkt na poziomie Unii Europejskiej, za pośrednictwem którego przekazywane są dane i informacje dotyczące badań klinicznych zgodnie z rozporządzeniem 536/2014;

14) przetwarzanie danych osobowych- operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie,

dopasowywanie, łączenie, ograniczanie, usuwanie oraz niszczenie;

15) przewodniczący NKB – przewodniczącego NKB, zastępcę przewodniczącego NKB lub osobę przez niego upoważnioną;

16) pseudonimizacja - przetworzenie 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 oraz są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

17) PUODO - Prezesa Urzędu Ochrony Danych Osobowych;

18) ryzyko - możliwość niezrealizowania celu w kontekście ochrony danych osobowych;

19) system teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie danych osobowych, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. System teleinformatyczny obejmuje między innymi sprzęt komputerowy, urządzenia przenośne, oprogramowanie systemowe, systemy (podsystemy), sieć, aplikacje;

20) usuwanie danych osobowych - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

21) użytkownik – członka NKB lub inną osobę realizującą zadania na rzecz NKB na podstawie umowy lub innego stosunku prawnego, która w związku z realizacją tych zadań przetwarza dane osobowe;

22) współadministrator - jednego z co najmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania danych osobowych;

23) zabezpieczenie danych osobowych - wdrożenie i eksploatację środków organizacyjnych, technicznych i fizycznych, w celu zabezpieczenia zasobów technicznych, ochrony przed zniszczeniem, nieuprawnionym dostępem, modyfikacją, ujawnieniem, pozyskaniem danych osobowych bądź ich utratą;

24) zgoda - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

25)

Rozdział 2

Zasady przetwarzania danych osobowych

§ 3.

1. Administrator przetwarza dane osobowe zgodnie z następującymi zasadami:
   1) legalności;
   2) rzetelności;
   3) przejrzystości;
   4) ograniczenia celu;
   5) minimalizacji danych;

6) prawidłowości danych;

7) ograniczenia przechowywania;

8) integralności i poufności;

9) ochrony danych osobowych w fazie projektowania;

10) domyślnej ochrony danych osobowych.

2. Zasada legalności oznacza przetwarzanie danych osobowych zgodnie z prawem. Realizując tę zasadę, dane osobowe przetwarzane są na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych.

3. Zasada rzetelności wymaga, by dane osobowe były przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane osobowe dotyczą.

4. Zasada przejrzystości wymaga by osoba, której dane osobowe dotyczą została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania, tj. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

5. Zasada ograniczenia celu polega na przetwarzaniu danych osobowych jedynie w celu zgodnym z odpowiednią przesłanką dopuszczalności przetwarzania danych osobowych.

6. Zasada minimalizacji danych oznacza, że administrator przetwarza tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

7. Zasada prawidłowości danych oznacza, że administrator przetwarza dane osobowe prawidłowe i uaktualnia, prostuje lub usuwa je w razie potrzeby.

8. Zasada ograniczenia przechowywania oznacza, że administrator przechowuje dane osobowe w dokumentacji tworzącej akta spraw przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

9. Zasada integralności i poufności jest realizowana przez dopuszczenie do przetwarzania danych osobowych jedynie osób upoważnionych oraz zastosowanie takich środków technicznych i organizacyjnych, by dane te nie były zmieniane przez osoby nieupoważnione lub by dane te nie były udostępniane osobom nieupoważnionym.

10. Zasada ochrony danych osobowych w fazie projektowania oznacza, że ochrona prywatności jest realizowana na etapie projektowanych działań skutkujących przetwarzaniem danych osobowych.

11. Zasada domyślnej ochrony danych osobowych oznacza, że domyślne ustawienia przetwarzania danych osobowych umożliwią przetwarzanie jedynie danych niezbędnych do osiągnięcia każdego konkretnego celu przetwarzania. Jednocześnie ustawienia systemów przetwarzania danych osobowych nie powinny umożliwiać udostępnienia danych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której te dane dotyczą.

12. Przetwarzanie danych osobowych, dla których administratorem lub współadministratorem jest przewodniczący NKB oraz danych osobowych przetwarzanych na podstawie umowy powierzenia przetwarzania danych osobowych w NKB jest dopuszczalne, jeżeli jest spełniona przynajmniej jedna z następujących przesłanek legalności przetwarzania danych osobowych:

    1) osoba, której dane osobowe dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych osobowych;

    2) jest to konieczne do realizacji umowy, gdy osoba, której dane osobowe dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby,

której te dane dotyczą;

3) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

4) jest to niezbędne do ochrony żywotnych interesów osoby, której dane osobowe dotyczą lub innej osoby fizycznej;

5) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego w ramach sprawowania władzy publicznej powierzonej administratorowi;

6) niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane osobowe dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której te dane dotyczą, jest dzieckiem.

§ 4.

1. Zabrania się przetwarzania danych osobowych, dla których administratorem lub współadministratorem jest przewodniczący NKB, ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, biometrycznych, dotyczących zdrowia, seksualności lub orientacji seksualnej, z zastrzeżeniem ust. 2.
2. Przetwarzanie danych osobowych, o których mowa w ust. 1, jest dopuszczalne w przypadkach określonych w art. 9 ust. 2 RODO.
3. Przetwarzanie danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa jest dopuszczalne wyłącznie w przypadku, gdy jest ono dozwolone przepisami prawa powszechnie obowiązującego.

§ 5.

1. Warunki wyrażenia zgody, o której mowa w § 3 ust. 12 oraz § 4 ust. 2 Polityki, powinny spełniać wymogi określone w art. 7 RODO.
2. Za przygotowanie treści oświadczenia o udzieleniu zgody osoby, której dane dotyczą, odpowiedzialny jest członek NKB realizujący dany proces przetwarzania danych osobowych w porozumieniu z IOD.
3. Jeżeli osoba, której dane osobowe dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy również innych kwestii, oświadczenie zgody musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii.
4. Wyrażenie zgody powinno zostać należycie udokumentowane dla celów rozliczalności. Przed odebraniem zgody podmiot danych osobowych powinien zostać należycie poinformowany stosowanie do postanowień art. 13 RODO.
5. Wycofanie zgody musi być równie łatwe jak jej wyrażenie i pozostawać bez negatywnych konsekwencji dla wycofującego zgodę.

§ 6.

1. W przypadku zbierania na rzecz NKB jakichkolwiek danych osobowych od osoby, której te dane dotyczą, konieczne jest spełnienie wobec tej osoby obowiązku informacyjnego i przekazanie tej osobie informacji (klauzuli informacyjnej), o których mowa w art. 13 RODO, w szczególności o:

   1) administratorze oraz pełnej nazwie administratora i jego adresie;

2) danych kontaktowych IOD;

3) celu przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;

4) prawie dostępu do treści swoich danych osobowych oraz prawie ich sprostowania, usunięcia, ograniczenia przetwarzania oraz prawie do wniesienia sprzeciwu wobec przetwarzania, oraz prawie do przenoszenia tych danych;

5) dobrowolności albo obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;

6) odbiorcach danych osobowych;

7) możliwości wycofania zgody, w przypadku gdy dane osobowe są przetwarzane na jej podstawie;

8) możliwości wniesienia skargi do PUODO;

9) okresie przechowywania danych osobowych.

2. Klauzula informacyjna, o której mowa w ust. 1 powinna być dostosowana do procesu realizowanego przez NKB, w szczególności w zakresie określonym w ust. 1 pkt 3, 4, 6 i 9. Wzór klauzuli jest określony w **załączniku nr 2** do Polityki.

3. Spełnienie obowiązku, o którym mowa w ust. 1, powinno nastąpić w momencie zbierania danych osobowych w sposób dostosowany do kanału komunikacji.

4. Członek NKB realizujący proces, z którym wiąże się konieczność spełnienia obowiązku, o którym mowa w ust. 1, jest obowiązany do dokumentowania jego realizacji.

5. Przepisu ust. 1 nie stosuje się, jeżeli osoba, której dane osobowe dotyczą, posiada już te informacje.

6. W przypadku zbierania na rzecz NKB danych osobowych, w sposób inny niż od osoby, której one dotyczą, konieczne jest spełnienie wobec tej osoby obowiązku informacyjnego i przekazanie tej osobie informacji (klauzuli informacyjnej), o których mowa w art. 14 RODO, w szczególności o:

   1) administratorze oraz o pełnej nazwie administratora i jego adresie;

   2) danych kontaktowych IOD;

   3) celu i zakresie zbierania danych osobowych;

   4) odbiorcach lub kategoriach odbiorców danych osobowych;

   5) źródle danych osobowych;

   6) prawie dostępu do treści swoich danych osobowych oraz możliwości ich poprawienia;

   7) uprawnieniach, o których mowa w § 10 Polityki.

7. Wzór klauzuli informacyjnej, o której mowa w ust. 6, określa **załącznik nr 3** do Polityki.

8. Informacje o których mowa w ust. 6 podaje się;

   1) nie później niż w terminie 30 dni od momentu pozyskania danych osobowych, w celu dalszego ich przetwarzania lub

   2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której te dane dotyczą - przy pierwszej takiej komunikacji z tą osobą lub

   3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – przy ich pierwszym ujawnieniu.

9. Przepisu ust. 6 nie stosuje się, jeżeli:

   1) przepis ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której te dane dotyczą;

2) dane osobowe są przetwarzane na podstawie przepisów prawa;

3) dane osobowe są niezbędne do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych lub do celów statystycznych na podstawie przepisów prawa;

4) osoba, której dane osobowe dotyczą, posiada informacje, o których mowa w ust. 6.

10. Za wypełnianie obowiązków informacyjnych odpowiedzialny jest członek NKB lub podmiot, któremu powierzono przetwarzanie danych osobowych zgodnie z § 8 Polityki, jeżeli umowa lub porozumienie taki obowiązek określa.

11. Za aktualność i zgodność z przepisami prawa klauzul informacyjnych funkcjonujących na portalach i serwisach, których administratorem jest przewodniczący NKB odpowiedzialny jest IOD wraz z administratorami merytorycznymi i technicznymi stron.

12. Projekty klauzul informacyjnych, o których mowa w ust. 1 i 6, są akceptowane przez IOD za pośrednictwem poczty elektronicznej. Zaakceptowane projekty klauzul informacyjnych są dopuszczone do stosowania.

13. Obowiązek informacyjny wobec interesantów NKB realizowany jest w szczególności przez:

1) przekazanie klauzuli informacyjnej;

2) umieszczenie stosownej informacji na stronie internetowej NKB;

3) umieszczenie stosownej informacji w punkcie kancelaryjnym;

4) umieszczenie stosownej informacji przy formularzach elektronicznych mających związek z przetwarzaniem danych osobowych;

5) zamieszczenie stosownej informacji w stopce wiadomości wysyłanych przez osoby upoważnione za pośrednictwem poczty elektronicznej, w sposób określony w ust. 14.

14. Spełnienie obowiązku, o którym mowa w ust. 1 i 6 może nastąpić warstwowo, tj. najważniejsze informacje (oznaczenie administratora, cele przetwarzania danych osobowych, opis praw przysługujących osobie, do której należą dane osobowe, – z jednoczesnym odesłaniem do pełnej treści klauzuli informacyjnej) przekazywane są w momencie kontaktu z osobą, której dane osobowe dotyczą. Pozostałe informacje przekazywane są poprzez stronę internetową.

§ 7.

1. Udostępnienie danych osobowych, których administratorem lub współadministratorem jest przewodniczący NKB oraz danych osobowych przetwarzanych w NKB na podstawie umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych, może nastąpić na podstawie przepisów prawa lub w oparciu o umotywowany wniosek, o ile nie narusza to praw i wolności osób, których dane dotyczą.

2. Członkowie NKB, do których wpływają wnioski o udostępnienie danych, zobowiązani są każdorazowo do przeanalizowania możliwości oraz zakresu udostępnienia danych osobowych.

3. O udostępnieniu danych osobowych, o którym mowa w ust. 1, członek NKB który te dane zgromadził, informuje IOD.

4. W celu zapewnienia przez NKB kontroli nad tym, komu dane osobowe są przekazywane, udostępnienie danych osobowych powinno odbywać się w formie pisemnej, co pozwoli w szczególności na udokumentowanie podstawy prawnej udostępnienia tych danych i podmiotu, który o to się zwróci.

§ 8.

1. Przetwarzanie danych osobowych, których administratorem jest przewodniczący NKB, może zostać powierzone innemu podmiotowi pod warunkiem zawarcia z tym podmiotem pisemnej umowy powierzenia przetwarzania danych osobowych, której wzór jest określony w **załączniku nr 4** do

Polityki. Wzór ten zawiera zakres postanowień, które powinny być zawarte w umowie i wymaga każdorazowo ewentualnego dostosowania lub rozbudowania jego treści do konkretnych okoliczności faktycznych.

2. Umowy powierzenia przetwarzania danych osobowych, o których mowa w ust. 1 zawierane są w przez przewodniczącego NKB.
3. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych osobowych w imieniu administratora jest poddanie planowanego zlecenia usług zewnętrznemu podmiotowi analizie, która powinna wykazać, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych osobowych, zgodnie z arkuszem oceny podmiotu przetwarzającego dane osobowe, stanowiącym **załącznik nr 5** do Polityki.
4. Podmiot przetwarzający, któremu powierzono przetwarzanie danych osobowych na podstawie umowy lub porozumienia zobowiązany jest do informowania administratora o naruszeniach dotyczących powierzonych danych osobowych, a także do współpracy przy wyjaśnianiu okoliczności naruszenia.
5. Projekt umowy lub porozumienia lub aneksów w sprawie powierzenia przetwarzania danych osobowych wraz z arkuszem oceny, o którym mowa w ust. 3, jest akceptowany przez IOD.
6. Jeżeli zawarcie umowy powierzenia następuje na wzorze podmiotu przetwarzającego lub zmienionym wzorze określonym w Załączniku nr 4, to przewodniczący NKB powinien go, bezzwłocznie przesłać do IOD celem sprawdzenia zgodności formalno-prawnej.
7. Każda umowa lub porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych powinien być zaparafowany własnoręcznie przez IOD lub w formie elektronicznego podpisu kwalifikowanego.
8. Oryginały umów lub porozumień lub aneksów w sprawie powierzenia przetwarzania danych osobowych, przechowuje przewodniczący NKB lub wyznaczona przez niego osoba.
9. Informacja na temat zawartej umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych oraz skan umowy i arkusz oceny są niezwłocznie przekazywane IOD poprzez e-mail. Informacja powinna obejmować zakres danych osobowych określony w rejestrze umów powierzenia przetwarzania danych osobowych, którego wzór jest określony w **załączniku nr 6** do Polityki.
10. IOD prowadzi rejestr umów powierzenia przetwarzania danych osobowych w formie elektronicznej.
11. Przewodniczący NKB w przypadku, gdy w ramach zawartej umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych są zawierane kolejne umowy powierzenia (umowy podpowierzenia przetwarzania danych osobowych), monitoruje ich realizację. Informacja na temat kolejnych umów powierzenia powinna obejmować zakres danych osobowych określony w rejestrze, o którym mowa w ust. 10.

§ 9.

1. Rejestr czynności przetwarzania danych osobowych, którego wzór jest określony w **załączniku nr 7** do Polityki, jest prowadzony, uzupełniany oraz aktualizowany na bieżąco przez IOD.
2. Rejestr, o którym mowa w ust. 1 zawiera informacje o procesach realizowanych przez NKB związanych z czynnościami przetwarzania danych osobowych rozumianych jako zespół powiązanych ze sobą operacji na danych osobowych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim czynności te są podejmowane.
3. W przypadku zmian w realizowanych procesach, których przedmiotem są czynności przetwarzania danych osobowych, polegających na ich rozszerzeniu lub ograniczeniu wynikających ze zmian przepisów prawa powszechnie obowiązującego lub zmian w organizacji, członek NKB niezwłocznie przekazuje tę informację IOD.

4. W przypadku, w którym NKB powierzono przetwarzanie danych osobowych na podstawie umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego prowadzony jest rejestr kategorii czynności przetwarzania danych osobowych, którego wzór jest określony w **załączniku nr 8** do Polityki.
5. Rejestr cząstkowy kategorii czynności przetwarzania danych osobowych jest prowadzony, uzupełniany i aktualizowany na bieżąco przez IOD.
6. Rejestry, o których mowa w ust. 1 i 4, są prowadzone w formie elektronicznej.
7. Za sporządzenie rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania danych osobowych dla NKB odpowiada IOD.
8. IOD nie rzadziej niż co 6 miesięcy występuje do członków NKB w celu ustalenia, czy rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych NKB jest kompletny.
9. Każdy Członek NKB ma obowiązek na bieżąco informować IOD o wszelkich zmianach w procesach przetwarzania danych osobowych, w szczególności dotyczących:
   1) celów przetwarzania danych osobowych;
   2) kategorii osób, których dane osobowe są przetwarzane;
   3) zakresu przetwarzania danych osobowych;
   4) podmiotów przetwarzających, którym dane osobowe są powierzane;
   5) odbiorców danych osobowych, którym te dane są udostępnione.

§ 10.

Każdej osobie, której dane osobowe są przetwarzane w NKB i dla których przewodniczący NKB jest administratorem, współadministratorem, przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) ustalenia administratora, adresu jego siedziby i pełnej nazwy;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy przetwarza się dane osobowe jej dotyczące, oraz podania informacji w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące, chyba że administrator jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
5) uzyskania informacji o sposobie udostępniania danych osobowych, w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów o ochronie danych osobowych albo są już zbędne do realizacji celu, dla którego zostały zebrane, z zachowaniem warunków, a także wniesienia sprzeciwu wobec przetwarzania, zachowaniem warunków dopuszczalności skorzystania z tych praw przewidzianych w RODO;
7) odwołania w każdym czasie zgody na przetwarzanie danych osobowych jej dotyczących;
8) wniesienia skargi do PUODO.

§ 11.

1. Na wniosek osoby, której dane osobowe dotyczą, istnieje obowiązek udzielenia tej osobie, w terminie 30 dni, informacji o przysługujących jej prawach oraz udzielenia, w odniesieniu do jej danych osobowych, informacji, o których mowa w § 10 pkt 1 - 5 Polityki oraz przekazania tej osobie kopii przetwarzanych danych osobowych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię danych osobowych drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.
2. Za przygotowanie odpowiedzi na wniosek, o którym mowa w ust. 1, oraz przekazanie wnioskodawcy kopii danych osobowych, odpowiedzialny jest członek NKB, przetwarzający te dane.
3. Projekt odpowiedzi, o której mowa w ust. 2 i 3, wymaga uzyskania akceptacji IOD.
4. Niezbędne informacje dotyczące trybu korzystania i realizacji praw zostały przedstawione na stronie internetowej NKB.

§ 12.

1. W przypadku wykazania przez osobę, której dane osobowe dotyczą, że dane osobowe przetwarzane przez NKB lub dla których przewodniczący NKB jest administratorem są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są zbędne do realizacji celu, dla którego zostały zebrane, członek NKB realizujący dany proces przetwarzania danych osobowych jest zobowiązany do niezwłocznego uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia ze zbioru, zgodnie z żądaniem osoby, której dane osobowe dotyczą.
2. O dokonanym uaktualnieniu lub sprostowaniu danych osobowych przewodniczący NKB informuje innych administratorów, którym udostępnione zostały dane osobowe.

Rozdział 3
Zakres i zasady ochrony danych osobowych

§ 13.

Zasady ochrony danych osobowych określone Polityką stosuje się w odniesieniu do danych osobowych przetwarzanych:

1) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych NKB;
2) w systemach teleinformatycznych.

§ 14.

1. Obszar, w którym są przetwarzane dane osobowe na terenie NKB, obejmuje pomieszczenia znajdujące się w budynku zlokalizowanym w Warszawie, do których tytuł prawny ma ABM.
2. Dodatkowo miejsca przetwarzania danych osobowych stanowią wszystkie komputery oraz inne nośniki danych członków NKB znajdujące się poza obszarem wskazanym w ust. 1, w tym w miejscu pobytu stanowiącym miejsce wykonywania zadań w ramach prac NKB.

§ 15.

Dokumentacja opisująca sposób przetwarzania danych osobowych oraz sposoby ich zabezpieczenia, w tym zabezpieczenia w systemach teleinformatycznych służących do przetwarzania danych osobowych w NKB stanowi wewnętrzną regulację ADO i nie może być udostępniana w żadnej formie, z wyłączeniem ABM lub w przypadkach określonych przepisami prawa.

§ 16.

W doborze i stosowaniu środków ochrony przetwarzanych danych osobowych szczególną uwagę należy zwracać na należyte ich zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

§ 17.

1. Do przetwarzania danych osobowych, których administratorem jest przewodniczący NKB mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, którego wzór jest określony w **załączniku nr 9** do Polityki. Dopuszczenie użytkownika do przetwarzania danych osobowych bez ważnego upoważnienia stanowi naruszenie ochrony danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych wydawane jest na podstawie informacji zawierającej listę osób, z którymi nawiązany zostanie stosunek prawny, przekazanej przez komórkę organizacyjną właściwą do spraw kadr i płac ABM do IOD.
3. Informacja, o której mowa w ust. 2 powinna zostać niezwłocznie przekazana do IOD, lecz nie później niż 7 dni przed dopuszczeniem danej osoby do przetwarzania danych osobowych. Przygotowane upoważnienia przez IOD przekazywane są do komórki organizacyjnej właściwej do spraw kadr i płac ABM celem ich wydania.
4. Upoważnienie do przetwarzania danych osobowych wydawane jest przez ADO lub osobę przez niego upoważnioną, podpisywane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub poprzez podpis tradycyjny składany na dokumencie i przekazywany osobiście osobie upoważnionej bądź przy pomocy poczty elektronicznej. Upoważnienie przekazywane jest osobie upoważnionej za pośrednictwem komórki organizacyjną właściwej do spraw kadr i płac ABM lub przewodniczącego NKB.
5. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w NKB, której wzór jest określony w **załączniku nr 10** do Polityki.
6. Ewidencja, o której mowa w ust. 5, nie obejmuje osób, dla których, w związku z zawartymi umowami powierzającymi przetwarzanie danych osobowych, obowiązek wydania upoważnień nie spoczywa na administratorze.
7. Każdy osoba, przed rozpoczęciem przetwarzania danych osobowych, w momencie wydania upoważnienia, o którym mowa w ust. 1 powinna zapoznać się z przepisami, procedurami i zasadami dotyczącymi ochrony danych osobowych, w tym, w szczególności z przepisami UODO i RODO, a także z obowiązującą w NKB Polityką Bezpieczeństwa Teleinformatycznego w NKB. Członkowie NKB podpisują w tym zakresie oświadczenie o zapoznaniu się z przepisami i zasadami ochrony danych oraz o zachowaniu w poufności, stanowiące **załącznik nr 1** do Polityki. W odniesieniu do pozostałych osób obowiązki i odpowiedzialność w obszarze ochrony danych osobowych określane są w umowie lub innym dokumencie będącym podstawą nawiązania stosunku prawnego pomiędzy administratorem a użytkownikiem.
8. Upoważnienie, o którym mowa w ust. 1, traci moc w przypadku wygaśnięcia lub rozwiązania umowy lub ustania innego stosunku prawnego łączącego administratora z użytkownikiem. Administrator może w każdym czasie cofnąć lub zmienić upoważnienie, w przypadku zmiany zakresu wykonywanych zadań i zakresu dostępu do danych osobowych.
9. Komórka organizacyjna właściwa do spraw kadr i płac lub przewodniczący NKB niezwłocznie powiadamia IOD o każdym przypadku rozwiązania lub wygaśnięcia umowy lub innego stosunku prawnego, nie później niż w terminie 7 dni od momentu jego zaistnienia.

§ 18.

Użytkownicy są w szczególności zobowiązani do:

1) przetwarzania danych osobowych zgodnie z przepisami UODO i RODO, dokumentami wewnętrznymi, w tym Polityką, oraz zgodnie z celem, dla którego te dane zostały zebrane;

2) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;

3) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem danych osobowych;

4) przetwarzania danych osobowych w odpowiednio zabezpieczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;

5) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych w systemie teleinformatycznym, określonych w Polityce Bezpieczeństwa Teleinformatycznego w NKB lub dokumentach, których mowa w § 17 ust. 8 Polityki;

6) posiadania swojego własnego indywidualnego identyfikatora (loginu) do logowania się. Nie można samodzielnie zmieniać swoich uprawnień, Zabronione jest także umożliwianie pracy na koncie nieupoważnionym osobom;

7) do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**;

8) wylogowania się z systemu informatycznego po zakończeniu pracy, a jeśli to wymagane - następnie wyłączenia sprzętu komputerowego oraz do zabezpieczenia stanowiska pracy, w szczególności wszelkich nośników magnetycznych i optycznych, na których znajdują się dane osobowe;

9) stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy;

10) niepozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych;

11) niewyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np. na terenach publicznych miejskich lub w lesie;

12) zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych, a w szczególności przed kradzieżą, uszkodzeniem i zaginięciem;

13) niszczenia w niszczarkach wszystkich zbędnych dokumentów zawierających dane osobowe lub w inny sposób uniemożliwiający ich odczytanie lub odtworzenie;

14) nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;

15) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez administratora;

16) zachowania szczególnej ostrożności przy wysyłaniu korespondencji tradycyjnej i elektronicznej. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć

metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości";

17) szyfrowania plików zawierających dane osobowe, wysyłanych za pośrednictwem poczty elektronicznej, (np. programem 7 zip, winzipem, winrarem) i zahasłowania plików, gdzie hasło powinno być przesłane do odbiorcy odrębnym kanałem informacji (np. SMS);

18) zachowania szczególnej ostrożności podczas transportu urządzeń przenośnych zawierających dane osobowe (laptopy, nośniki danych USB, dyski zewnętrzne), dane osobowe wynoszone poza NKB muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki), a dokumentacji papierowej należy zapewnić bezpieczne przewożenie w plecakach, teczkach;

19) używania adresu email służbowego wyłącznie do wykonywania obowiązków służbowych;

20) współpracy jedynie przy użyciu dokumentów niezbędnych do wykonania zadań NKB;

21) przechowywania dokumentów w czasie nie dłuższym niż czas niezbędny do zrealizowania zadań, do których wykonania dokumenty są przeznaczone;

22) nietworzenia kopii dokumentów innych niż niezbędne do realizacji powierzonych obowiązków;

23) skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada;

24) niewyłączania systemu antywirusowego podczas pracy systemu teleinformatycznego przetwarzającego dane osobowe.

§ 19.

Użytkownicy obowiązani są stosować środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych w NKB, które zostały określone w Polityce Bezpieczeństwa Teleinformatycznego w NKB.

Rozdział 4
Struktura organizacji ochrony danych osobowych

§ 20.

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, UODO, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w NKB, odpowiadają:

1) przewodniczący NKB;
2) Inspektor Ochrony Danych;
3) członek NKB nie będący przewodniczącym NKB
4) osoby upoważnione.

§ 21.

Przewodniczący NKB jest właściwy w szczególności do:

1) wyznaczenia i odwołania IOD oraz jego zastępcy;
2) poinformowania organu nadzorczego o wyznaczeniu i odwołaniu IOD oraz jego zastępcy oraz

zamieszczenia stosownej informacji na stronie internetowej;

3) wdrożenia odpowiednich procedur ochrony danych osobowych;

4) zagwarantowania odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych;

5) wdrożenia w NKB odpowiednich środków organizacyjnych i technicznych w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu istniejącemu ryzyku naruszenia praw lub wolności osób, których dane osobowe dotyczą;

6) zapewnienia środków umożliwiających prawidłową realizację praw osób, których dane osobowe dotyczą;

7) ustalenia środków i celów przetwarzania danych osobowych w NKB;

8) nadzoru nad przetwarzaniem danych osobowych w NKB;

9) nadzoru nad prowadzeniem w NKB rejestru czynności przetwarzania danych osobowych i rejestru kategorii przetwarzania danych osobowych;

10) nadawania upoważnień do przetwarzania danych osobowych oraz nadzór na ewidencją osób upoważnionych do przetwarzania danych osobowych;

11) wspierania IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, w szczególności:

   a) włączania IOD w kluczowe kwestie i decyzje podejmowane w NKB, które mogą mieć związek z przetwarzaniem danych osobowych,

   b) zapewnienia zasobów niezbędnych do wykonania zadań IOD oraz dostępu do danych osobowych i operacji przetwarzania danych osobowych, a także zasobów niezbędnych do utrzymania fachowej wiedzy IOD,

   c) umożliwienia IOD należytego wykonywania swoich obowiązków bez presji lub instrukcji dotyczących sposobu realizacji zadań i osiągania celów;

12) współpracy z organem nadzorczym w ramach wykonywania swoich zadań;

13) zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki oraz zawiadamiania osób, których dane osobowe dotyczą o naruszeniu tych danych w przypadkach określonych w przepisach;

14) nadzoru nad dokumentowaniem wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;

15) jeśli uzna to za konieczne, stosowania zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako elementów dla stwierdzenia przestrzegania przez NKB ciążących na niej obowiązków;

16) zapewnienia odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki;

17) realizacji innych obowiązków nałożonych na NKB na podstawie przepisów RODO i UODO.

§ 22.

1. Dla zapewnienia przestrzegania przepisów o ochronie danych osobowych w NKB funkcjonuje IOD.

2. IOD oraz jego zastępca jest wyznaczany i odwoływany przez przewodniczącego NKB.

3. Dopuszcza się powołanie wspólnego IOD w przypadkach, w których przewodniczący NKB jest współadministratorem.

4. IOD realizuje zadania samodzielnie lub przy pomocy zastępcy we współpracy z osobami upoważnionymi.

5. Do zadań IOD należy w szczególności:

   1) informowanie administratora, podmiotu przetwarzającego oraz członków NKB, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych powszechnie obowiązujących przepisów prawa o ochronie danych osobowych i doradzanie im w tej sprawie;

   2) monitorowanie przestrzegania RODO, innych powszechnie obowiązujących przepisów prawa o ochronie danych osobowych oraz Polityki administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia członków NKB uczestniczących w operacjach przetwarzania danych osobowych oraz powiązane z tym audyty;

   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

   4) współpraca z PUODO;

   5) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

   6) uczestniczenie w postępowaniu wyjaśniającym w przypadku naruszenia ochrony danych osobowych oraz prowadzenie rejestru naruszeń i podejrzeń naruszeń ochrony danych osobowych, o którym mowa w § 29 Polityki;

   7) przekazywanie informacji o bieżących kwestiach związanych z ochroną danych osobowych, w tym o stanowiskach organu nadzorczego;

   8) rekomendowanie, doradzanie oraz zalecanie osobom upoważnionym określonych działań w zakresie przestrzegania przepisów o ochronie danych osobowych;

   9) przeprowadzanie szkoleń z zakresu ochrony danych osobowych dla członków NKB;

   10) reagowanie na bieżące problemy z zakresu ochrony danych osobowych;

   11) przeprowadzanie sprawdzeń bieżących, doraźnych i planowych w zakresie przestrzegania przepisów RODO, ustawy i wdrożonych procedur ochrony danych osobowych;

   12) uczestnictwo w spotkaniach oraz konsultacjach związanych z zadaniami ADO, które mogą mieć związek z ochroną danych osobowych;

   13) prowadzenie rejestru czynności przetwarzania danych osobowych oraz rejestr kategorii przetwarzania danych osobowych;

   14) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

   15) aktualizowanie Polityki i innych dokumentów związanych z ochroną danych osobowych.

6. IOD współpracuje z ADO we wdrażaniu RODO i utrzymaniu zgodności przetwarzania danych osobowych z RODO, w tym w zakresie zasad przetwarzania danych osobowych, realizacji praw osób, których dane osobowe dotyczą, ochrony danych w fazie projektowania, rejestru czynności przetwarzania danych osobowych, zgłaszania naruszeń związanych z ochroną danych osobowych oraz stosowania zasady domyślnej ochrony danych.

7. IOD dokumentuje podejmowane przez siebie działania w zakresie ochrony danych osobowych w celu wykazania działania z należytą starannością, zgodnie z zasadą rozliczalności, w szczególności

dokumentuje podejmowane działania, opiniuje projekty umów, wydaje pisemne zalecenia i rekomendacje.

§ 23.

1. Za ochronę danych osobowych przetwarzanych w NKB odpowiada także członek NKB nie będący przewodniczącym NKB.
2. Do zadań osób wskazanych w ust. 1 należy w szczególności:
   1) inicjowanie i koordynowanie działań, których celem jest zapewnienie poziomu ochrony danych osobowych, odpowiadającego wymogom prawa, w przydzielonym obszarze;
   2) nadzór nad przestrzeganiem zasad ochrony określonych w Polityce;
   3) zgłaszanie IOD zmian, uzupełnień i aktualizacji do rejestru czynności przetwarzania danych osobowych, o którym mowa w § 9 ust. 1 Polityki oraz rejestru kategorii czynności przetwarzania danych osobowych, o którym mowa w § 9 ust. 4 Polityki.
3. Członek NKB nie będący przewodniczącym NKB , w fazie wdrażania nowego projektu, w przypadku gdy będzie dotyczył on przetwarzania danych osobowych, przeprowadza analizę ryzyka naruszenia praw lub wolności osób fizycznych, w szczególności: kradzieży tożsamości, straty finansowej, naruszenia dobrego imienia, naruszenia poufności danych chronionych tajemnicą zawodową, nieuprawnionego odwrócenia pseudonimizacji, utraty przysługujących osobom praw i wolności lub sprawowania kontroli nad swoimi danymi osobowymi, ujawnienia danych osobowych szczególnej kategorii.
4. W przypadku, gdy dany rodzaj przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele, może powodować wysokie ryzyko naruszenia praw lub wolności osób, członek NKB nie będący przewodniczącym NKB w oparciu o zalecenia i we współpracy z IOD, dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych (analiza DPIA).
5. Członek NKB nie będący przewodniczącym NKB , uwzględniając wynik analizy, o której mowa ust. 3 oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych wdraża odpowiednie środki techniczne i organizacyjne.
6. Członek NKB nie będący przewodniczącym NKB , zapewnia przestrzeganie ochrony danych zgodnie z przyjętymi zasadami, w szczególności:
   1) odpowiada za przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa;
   2) podejmuje działania zmierzające do wyeliminowania ewentualnych zagrożeń bezpieczeństwa danych osobowych i minimalizacji ryzyka oraz konsultuje się w tym zakresie z IOD;
   3) dba o zaplecze techniczne niezbędne do prawidłowego przetwarzania danych osobowych;
   4) włącza (od jak najwcześniejszego etapu prac) IOD w spotkania i konsultacje mające lub mogące mieć związek z przetwarzaniem danych osobowych;
   5) odpowiada za prawidłowe poszanowanie praw i wolności osób, których dane dotyczą w zakresie zadań realizowanych, w tym zatwierdza klauzule informacyjne w porozumieniu z IOD;
   6) aktualizuje rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych, zgłaszając informacje do IOD;
   7) zgłasza IOD potrzeby w zakresie dodatkowego przeszkolenia użytkowników z zakresu bezpieczeństwa przetwarzania i ochrony danych osobowych;
   8) niezwłocznie informuje IOD o zdarzeniu, w którym nastąpiło naruszenie lub z dużym stopniem prawdopodobieństwa mogło nastąpić naruszenie ochrony danych osobowych;

9) współpracuje z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych.

Rozdział 5

Postępowanie w przypadku podejrzenia naruszenia albo stwierdzenia naruszenia ochrony danych osobowych

§ 24.

1. Za naruszenie ochrony danych osobowych uznaje się, w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
   2) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmianę zawartości danych osobowych, utratę całości lub części danych osobowych);
   3) udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
   4) niezamierzoną zmianę lub utratę danych osobowych zapisanych na kopiach zapasowych;
   5) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu teleinformatycznego);
   6) nieuprawnione modyfikacje, kopiowanie lub uszkodzenie informacji przetwarzanej w systemie teleinformatycznym;
   7) nieuprawnione naruszenie lub próby naruszenia integralności systemu teleinformatycznego;
   8) zanotowanie, w krótkim czasie, dużej liczby nieudanych prób rozpoczęcia pracy w systemie teleinformatycznym;
   9) ujawnienie wirusów komputerowych lub innych programów godzących w poufność, integralność lub dostępność przetwarzanych danych osobowych w systemie teleinformatycznym;
   10) wydarzenia losowe obniżające poziom bezpieczeństwa systemu teleinformatycznego (np. brak zasilania lub pożar);
   11) kradzież urządzeń przenośnych i nośników informatycznych, na których przetwarzane są dane osobowe (np. laptopów, płyt CD, DVD, dysków twardych, nośników danych USB, dysków zewnętrznych);
   12) nieuprawnione zmiany konfiguracji systemu teleinformatycznego.
2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń NKB lub próby takich działań.
3. Sposób postępowania użytkowników w zakresie podstaw rozpoznawania naruszeń ochrony danych osobowych określa Poradnik rozpoznawania naruszeń ochrony danych osobowych, który stanowi **załącznik nr 11** do Polityki.

§ 25.

1. Każdy użytkownik w przypadku zaobserwowania sytuacji, która może stanowić naruszenie lub uzasadnione podejrzenie naruszenia ochrony danych osobowych jest obowiązany zgłosić niezwłocznie ten fakt do IOD.
2. Każdy użytkownik, , bezzwłocznie od momentu stwierdzenia przez niego okoliczności wystąpienia niepożądanego zdarzenia/incydentu dotyczącego danych osobowych przekazuje za

pośrednictwem poczty elektronicznej na adres: iod.@nkb.gov.pl. informację zawierającą: datę i godzinę wystąpienia naruszenia (jeśli jest znana), miejsce naruszenia, charakter naruszenia, informacje o nośnikach danych, których dotyczy naruszenie, kategorie i ilość osób których dotyczy naruszenie, skutki naruszenia, w tym możliwe konsekwencje naruszenia dla osób fizycznych, jeśli zgłoszenia naruszenia dokonano po upływie 24 godzin od momentu powzięcia informacji o naruszeniu – wyjaśnienie przyczyn opóźnienia.

§ 26.

IOD niezwłocznie podejmuje i prowadzi postępowanie wyjaśniające w każdej zgłoszonej sytuacji, w której naruszenia ochrony danych osobowych nie można wykluczyć, przy czym ocena dokonywana jest na podstawie informacji uzyskanych od zgłaszającego użytkownika. O każdej sytuacji mogącej stanowić naruszenie ochrony danych osobowych IOD zawiadamia ADO.

§ 27.

Postępowanie wyjaśniające jest prowadzone w celu ustalenia, czy zgłoszony przypadek stanowi naruszenie ochrony danych osobowych,

§ 28.

W toku postępowania wyjaśniającego wszczętego w związku z podejrzeniem naruszenia ochrony danych osobowych IOD:

1) może komunikować się z użytkownikami, osobami trzecimi, uzyskiwać dostęp do pomieszczeń, urządzeń i schowków, z zastrzeżeniem zachowania prywatności;
2) dokumentuje podjęte działania.

§ 29.

Stwierdzenie naruszenia ochrony danych osobowych następuje w chwili, gdy na podstawie zebranych informacji można racjonalnie przyjąć, że do naruszenia doszło lub mogło dojść z dużym stopniem prawdopodobieństwa.

§ 30.

W przypadku stwierdzenia naruszenia ochrony danych (niezależnie od jego ostatecznej kwalifikacji) należy odnotować datę i godzinę, w której doszło do stwierdzenia naruszenia. Na podstawie informacji zebranych w toku postępowania wyjaśniającego IOD ocenia stopień ryzyka możliwego naruszenia praw lub wolności osób fizycznych.

§ 31.

1. Dokonując oceny, IOD uwzględnia okoliczności naruszenia, w tym jego ciężar, skalę, możliwy wpływ na sytuację osób fizycznych, lub prawdopodobieństwo wystąpienia wpływu, a w szczególności bierze pod uwagę:
   1) rodzaj naruszenia, tj. czy doszło do nieuprawnionego ujawnienia, utraty, zniszczenia, zmodyfikowania danych osobowych, czy nieuprawnionego uzyskania dostępu do danych osobowych;
   2) rodzaj, poziom wrażliwości i skalę danych osobowych, których dotyczy naruszenie, zwłaszcza

czy naruszenie dotyczy danych osobowych szczególnych kategorii;

3) czy dane można łatwo powiązać z osobą fizyczną;

4) wagę potencjalnych konsekwencji dla osób fizycznych;

5) specjalne cechy osób, których dane dotyczą, np. młody wiek lub uzależnienia;

6) liczbę osób fizycznych, których dotyczy naruszenie.

2. Prawdopodobieństwo wpływu potencjalnego naruszenia na prawa lub wolności osób, następuje na podstawie obiektywnej oceny wagi naruszenia. Wynik oceny wagi naruszenia stanowi podstawę do podjęcia decyzji o zgłoszeniu naruszenia organowi nadzorczemu.

3. Szczegółowy sposób przeprowadzenia oceny wagi naruszenia został przedstawiony w **załączniku nr 12** do Polityki.

§ 32.

W przypadku ustalenia, że jest mało prawdopodobne, iż naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, IOD podejmuje postępowanie wyjaśniające, o którym mowa w § 28 - 30 oraz powiadamia ADO o zaistniałym incydencie.

§ 33.

1. W przypadku ustalenia, że jest prawdopodobne, iż stwierdzone okoliczności skutkują ryzykiem naruszenia praw lub wolności osób fizycznych, w szczególności kradzieży tożsamości, straty finansowej, naruszenia dobrego imienia, naruszenia poufności danych chronionych tajemnicą zawodową, nieuprawnionego odwrócenia pseudonimizacji, utraty przysługujących osobom praw i wolności lub sprawowania kontroli nad swoimi danymi osobowymi, ujawnienia danych osobowych szczególnej kategorii, IOD w porozumieniu z ADO i w jego imieniu:

   1) dokonuje zgłoszenia w sposób określony przez PUODO, nie później niż w czasie 72 godzin od momentu stwierdzenia naruszenia;

   2) jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, informuje o naruszeniu osoby fizyczne, których dotyczy naruszenie bez zbędnej zwłoki, w najkrótszym możliwym czasie, zgodnie ze wzorem zawiadomienia, określonym w **załączniku nr 13** do Polityki.

2. Jeśli wyczerpujące określenie podmiotów danych osobowych, których dotyczy naruszenie, nie jest możliwe, IOD w porozumieniu z ADO zamieszcza informację na stronie podmiotowej lub przekazuje ją w inny sposób, który maksymalizuje szansę dotarcia informacji do odpowiednich podmiotów danych osobowych.

3. Jeśli przekazanie kompletu informacji PUODO nie jest możliwe w terminie 72 godzin, należy przesłać część informacji, wskazując jednocześnie rodzaj informacji, które zostaną uzupełnione oraz termin tego uzupełnienia, a w przypadku uchybienia terminowi należy dokonać zgłoszenia, wyjaśniając powody niedotrzymania terminu.

§ 34.

IOD w imieniu ADO prowadzi rejestr wszystkich naruszeń i podejrzeń naruszeń ochrony danych osobowych, którego wzór stanowi **załącznik nr 14** do Polityki.

§ 35.

W każdym przypadku naruszenia, w którym ADO nie dokonuje zgłoszenia, lub nie informuje podmiotów, których dane osobowe dotyczą, należy w rejestrze opisać powody takiej decyzji.

§ 36.

1. IOD analizuje wpisy w rejestrze naruszeń i podejrzeń naruszeń ochrony danych osobowych, (jeżeli wystąpiły) nie rzadziej niż raz w roku w celu:
   1) oceny skuteczności środków technicznych i organizacyjnych zabezpieczenia danych osobowych;
   2) zidentyfikowania powtarzających się naruszeń;
   3) zaplanowania, w zależności od wyników oceny, działań zmierzających do poprawy środków organizacyjnych i technicznych zabezpieczenia danych osobowych.
2. IOD przedstawia ADO wnioski analizy wpisów w rejestrze naruszeń i podejrzeń naruszeń danych osobowych.

Rozdział 6
Kontrola i nadzór nad przetwarzaniem danych osobowych

§ 37.

1. Bieżący nadzór nad przetwarzaniem danych osobowych w NKB sprawuje przewodniczący NKB.
2. W ramach nadzoru, o którym mowa w ust. 1, przewodniczący NKB jest zobowiązany do zapewnienia przestrzegania postanowień Polityki przez użytkowników przetwarzających dane osobowe oraz do informowania IOD o stwierdzonych nieprawidłowościach.

§ 38.

1. Czynności kontrolne w podmiotach, którym zostało powierzone przetwarzanie danych osobowych przeprowadza merytorycznie przewodniczący NKB w porozumieniu z IOD.
2. Z przeprowadzonych czynności kontrolnych sporządzana jest informacja pokontrolna wraz z zaleceniami, do której podmiot kontrolowany może zgłosić swoje uwagi.
3. Kopia informacji pokontrolnej przekazywana jest do wiadomości IOD, w przypadku, gdy nie jest on jej autorem, oraz ADO.

Rozdział 7
Sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

§ 39.

1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych są dokonywane przez IOD w trybie:
   1) bieżącym - prowadzonym z własnej inicjatywy oraz na podstawie zgłoszenia;
   2) doraźnym - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia

informacji o tym, że doszło do naruszenia lub mogło dojść do naruszenia z dużym stopniem prawdopodobieństwa;

3) planowym - według planu sprawdzeń, który określa przedmiot, zakres oraz planowany termin przeprowadzenia poszczególnych sprawdzeń.

2. Plan sprawdzeń jest przedstawiany ADO, nie później niż dwa tygodnie przed dniem rozpoczęcia okresu objętego tym planem.

3. IOD zawiadamia użytkownika o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem planowanego przeprowadzenia czynności.

4. IOD dokumentuje czynności przeprowadzone podczas sprawdzenia przez:

1) utrwalanie danych z systemu teleinformatycznego służącego do przetwarzania danych osobowych lub zabezpieczenia danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych;

2) sporządzanie notatki służbowej z przeprowadzonych czynności, w szczególności z zebranych wyjaśnień, dokonanych oględzin oraz czynności związanych z dostępem do urządzeń, nośników oraz systemów teleinformatycznych służących do przetwarzania danych osobowych;

3) odbieranie ustnych wyjaśnień osoby, której czynności objęto sprawdzeniem;

4) sporządzanie kopii otrzymanego dokumentu lub obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu teleinformatycznego służącego do przetwarzania danych osobowych lub zabezpieczania danych osobowych;

5) sporządzanie kopii zapisów rejestrów systemu teleinformatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

5. Materiały dokumentujące czynności przeprowadzane podczas sprawdzenia są sporządzane w postaci papierowej lub elektronicznej oraz w postaci fotografii cyfrowej.

6. Z przeprowadzonych sprawdzeń jest sporządzane sprawozdanie w postaci papierowej lub elektronicznej, którego wzór stanowi **załącznik nr 15** do Polityki. Sprawozdanie jest przedkładane ADO, niezwłocznie po zakończeniu sprawdzenia.

Rozdział 8
Szkolenia
§ 40.

1. ADO zapewnia szkolenia dla użytkowników w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych.

2. ADO dokłada należytej staranności, aby użytkownicy mieli wiedzę niezbędną do prawidłowego rozpoznawania sytuacji mogących stanowić naruszenie ochrony danych osobowych.

3. Każdy użytkownik przed rozpoczęciem przetwarzania danych osobowych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych.

4. Szkolenia prowadzi IOD, osoba zastępująca IOD lub wyznaczona przez przewodniczącego NKB osoba posiadająca wiedzę z zakresu ochrony danych osobowych.

5. IOD może wydawać dokumenty związane z prowadzoną działalnością szkoleniową, z wyłączeniem upoważnień, o których mowa § 17 ust. 1 Polityki.

6. IOD może w celu podniesienia bieżącej wiedzy użytkowników z zakresu ochrony danych wysyłać

cyklicznie za pośrednictwem poczty e-mail biuletyn związany z tematyką ochrony danych osobowych.

7. Dopuszcza się możliwość prowadzenia szkoleń przez podmiot zewnętrzny posiadający udokumentowaną wiedzę z zakresu ochrony danych osobowych.

Rozdział 9
Postanowienia końcowe

§ 41.

1. Polityka podlega okresowemu przeglądowi pod kątem jej aktualności i adekwatności, nie rzadziej niż raz do roku.
2. Polityka podlega także przeglądom w przypadku:
   1) wystąpienia poważnego naruszenia ochrony danych;
   2) pojawienia się nowych i istotnych rodzajów ryzyka;
   3) zmian regulacji prawnych dotyczących ochrony danych osobowych lub wydania zaleceń i stanowisk Grupy Roboczej art. 29, Europejskiej Rady Ochrony Danych Osobowych i organu nadzorczego;
   4) istotnych zmian organizacyjnych w NKB;
   5) zgłaszanych potrzeb w zakresie ujętym w Polityce.
3. Przeglądu Polityki dokonuje IOD.
4. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   1) procesów funkcjonujących w strukturze NKB;
   2) obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega ADO;
   3) uwag zgłaszanych przez uczestników procesu przetwarzania danych osobowych w imieniu ADO.
5. Polityka może zostać zaktualizowana również w celu zwiększenia zgodności przetwarzania i ochrony danych osobowych z przepisami RODO, ustawy oraz zaleceń i stanowisk Grupy Roboczej art. 29, Europejskiej Rady Ochrony Danych Osobowych i organu nadzorczego.
6. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej przepisów IOD przygotowuje projekt aktualizacji Polityki w wymaganym zakresie.

§ 42.

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację administratora, jest wiążąca dla wszystkich członków NKB i obowiązuje wszystkich użytkowników. Każdy użytkownik ma obowiązek zapoznania się z Polityką.
2. Udostępnienie dokumentacji przetwarzania danych osobowych możliwe jest w przypadkach, w których przewodniczący NKB występuje np. jako współadministrator i pod warunkiem zawarcia porozumienia w sprawie współadministrowania danymi osobowymi, które stanowi **załącznik nr 16** do Polityki. Wzór ten zawiera minimalny zakres postanowień, które powinny być zawarte w porozumieniu i wymaga każdorazowo ewentualnego dostosowania lub rozbudowania jego treści do konkretnych okoliczności faktycznych.

§ 43.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia systemu teleinformatycznego NKB.

Spis załączników do „Polityki Ochrony Danych Osobowych w NKB"

1. Wzór oświadczenia o zapoznaniu się z treścią Polityki ochrony danych osobowych i o zachowaniu poufności.
2. Klauzula informacyjna przy pobieraniu danych osobowych bezpośrednio od osoby.
3. Klauzula informacyjna przy pobieraniu danych osobowych niebezpośrednio od osoby.
4. Wzór umowy (porozumienia) powierzenia przetwarzania danych osobowych.
5. Arkusz oceny podmiotu przetwarzającego dane osobowe.
6. Rejestr umów (porozumień) powierzenia przetwarzania danych osobowych.
7. Rejestr czynności przetwarzania danych osobowych.
8. Rejestr kategorii czynności przetwarzania danych osobowych.
9. Upoważnienie do przetwarzania danych osobowych.
10. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
11. Poradnik rozpoznawania naruszeń ochrony danych osobowych.
12. Kryteria oceny wagi naruszenia.
13. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.
14. Rejestr naruszeń ochrony danych osobowych.
15. Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie.
16. Wzór porozumienia w sprawie współadministrowania danymi osobowymi.

Załącznik nr 1

Oświadczenie o zapoznaniu się
z przepisami i zasadami ochrony danych osobowych oraz o zachowaniu poufności

. . . . . .
(Imię i Nazwisko)

. . . . . .
(miejscowość i data)

Niniejszym oświadczam, że w związku ze współpracą z Naczelną Komisją Bioetyczną do spraw Badań Klinicznych zostałem (-am) zapoznany (-a) z treścią Polityki Ochrony Danych Osobowych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych, Polityką Bezpieczeństwa Teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych oraz przepisami i zasadami ochrony danych osobowych wynikającymi z obowiązujących przepisów prawa m. in. z 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 (ogólne rozporządzenie o ochronie danych- RODO, Dz. U. UE. L. z 2016 r. Nr 119).

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem
- niezwłocznego zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. i ogólnego rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

. . . . . .
(podpis)

Załącznik nr 2

Klauzula informacyjna przy pobieraniu danych osobowych bezpośrednio od osoby

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), zwanego dalej „RODO", informujemy że:

1) administratorem Państwa danych osobowych jest przewodniczący Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych, ul. Stanisława Moniuszki 1A, 00-014 Warszawa;

2) z Inspektorem Ochrony Danych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych mogą Państwa skontaktować się za pośrednictwem poczty elektronicznej przez adres e-mail: iod@nkb.gov.pl;

3) Państwa dane osobowe przetwarzane będą w celu *(Cel przetwarzania danych osobowych)* na podstawie *(Należy podać podstawę prawną przetwarzania, np. art. 6 ust 1 lit. a/b/c/d/e/f);*

4) odbiorcą Państwa danych osobowych będą *(Należy wymienić kategorię odbiorców, o ile istnieją);*

5) Państwa dane osobowe będą przechowywane przez okres *(Jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu, np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji,);*

6) posiadają Państwo prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania), którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie zgody)*(należy wskazać odpowiednio właściwe prawa w zależności od zastosowanych przesłanek przetwarzania danych osobowych określonych w ust. 3);*

7) posiadają Państwa prawo do wniesienia sprzeciwu;

8) mają Państwa prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Państwa danych osobowych dotyczących narusza przepisy RODO;

9) podanie przez Państwa danych osobowych jest *(Należy podać – np. wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy).* Są Państwo zobowiązana/y do ich podania, a konsekwencją niepodania danych osobowych będzie *(Należy podać, jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania; należy też wskazać ewentualne konsekwencje niepodania danych)*;

10) Państwa dane nie będą poddawane zautomatyzowanym decyzjom, w tym nie będą profilowane/Państwa dane będą poddawane zautomatyzowanym decyzjom, w tym będą profilowane/Państwa dane będą poddawane zautomatyzowanym decyzjom, w tym nie będą profilowane/Państwa dane będą profilowane/Państwa dane nie będą profilowane. *(Jeżeli zachodzi).* Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach *(Należy podać zasady profilowania)*, konsekwencją takiego przetwarzania będzie *(Należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą – na przykład, w jaki sposób będą oceniane czynniki osobowe osoby fizycznej. Przykładową konsekwencją takiego przetwarzania może być (...)*

11) Państwa dane osobowe nie będą przekazywane do państwa trzeciego/ organizacji międzynarodowej, o i ile nie będą tego wymagały prawne obowiązki Administratora.

(Jeżeli mamy pewność co do transferu danych do państwa trzeciego to dodajemy poniższy zapis.)
Administrator przekazuje Państwa dane osobowe do państwa trzeciego/ organizacja międzynarodowej tylko wtedy, gdy jest to konieczne, i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez: współpracę z podmiotami przetwarzającymi Dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych, stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską; stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy.

W przypadku przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej, które nie zostały uznane decyzją Komisji Europejskiej za zapewniające odpowiedni stopień ochrony, wystąpimy do Państwa o wyrażenie wyraźnej zgody na takie przekazanie, informując o uprzednim ryzyku wiążącym się z takim przekazaniem na podstawie art. 49 ust. 1 lit. a RODO.

Załącznik nr 3

Klauzula informacyjna przy pobieraniu danych osobowych niebezpośrednio od osoby

Zgodnie z art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), zwanego dalej „RODO", informujemy że:

1) administratorem Państwa danych osobowych jest przewodniczący Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych, ul. Stanisława Moniuszki 1A, 00-014 Warszawa;
2) z Inspektorem Ochrony Danych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych mogą Państwo skontaktować się za pośrednictwem poczty elektronicznej przez adres e-mail: iod@nkb.gov.pl;
3) Państwa dane osobowe przetwarzane będą w celu *(Cel przetwarzania danych osobowych)* na podstawie *(Należy podać podstawę prawną przetwarzania, np. art. 6 ust 1 lit. a/b/c/d/e/f.);*
4) będziemy przetwarzać następujące kategorie Państwa danych osobowych. *(należy wymienić kategorie Danych osobowych, np.: imię i nazwisko, email itd.);*
5) odbiorcą Państwa danych osobowych będą *(Należy wymienić kategorię odbiorców, o ile istnieją);*
6) Państwa dane osobowe będą przechowywane przez okres *(Jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu, np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji,);*
7) posiadają Państwo prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania), którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie zgody) *(należy wskazać odpowiednio właściwe prawa w zależności od zastosowanych przesłanek przetwarzania danych osobowych określonych w ust. 3);*
8) posiadają Państwa prawo do wniesienia sprzeciwu;
9) mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Państwa danych osobowych dotyczących narusza przepisy RODO;
10) Państwa dane osobowe zostały pobrane z *(Należy podać źródło danych, również gdy dane zostały podane z publicznie dostępnego źródła);*
11) Państwa dane nie będą poddawane zautomatyzowanym decyzjom, w tym nie będą profilowane/Państwa dane będą poddawane zautomatyzowanym decyzjom, w tym będą profilowane/Państwa dane będą poddawane zautomatyzowanym decyzjom, w tym nie będą profilowane/Państwa dane będą profilowane/Państwa dane nie będą profilowane. *(Jeżeli zachodzi).* Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach *(Należy podać zasady profilowania)*, konsekwencją takiego przetwarzania będzie *(Należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą – na przykład, w jaki sposób będą oceniane czynniki osobowe osoby fizycznej. Przykładową konsekwencją takiego przetwarzania może być (...).*
12) Państwa dane osobowe nie będą przekazywane do państwa trzeciego/ organizacji międzynarodowej, o i ile nie będą tego wymagały prawne obowiązki Administratora.

(Jeżeli mamy pewność co do transferu danych do państwa trzeciego to dodajemy poniższy zapis.)
Administrator przekazuje Państwa dane osobowe do państwa trzeciego/ organizacji międzynarodowej tylko wtedy, gdy jest to konieczne, i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez: współpracę z podmiotami przetwarzającymi Dane osobowe w państwach, w odniesieniu do

których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych, stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską; stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy,

W przypadku przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej, które nie zostały uznane decyzją Komisji Europejskiej za zapewniające odpowiedni stopień ochrony, wystąpimy do Państwa o wyrażenie wyraźnej zgody na takie przekazanie, informując o uprzednim ryzyku wiążącym się z takim przekazaniem na podstawie art. 49 ust. 1 lit. a RODO.

Załącznik nr 4

Wzór

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu _____ pomiędzy:

_____ *(*dane podmiotu który umowę zawiera),*

zwanym w dalszej części umowy **„Administratorem"**, reprezentowanym przez:

_____, na podstawie/zgodnie z _____, którego kopia stanowi **załącznik nr 1** do umowy

oraz

_____ *(*dane podmiotu który umowę zawiera),*

zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**, reprezentowanym przez:

_____, na podstawie/zgodnie z _____, którego kopia stanowi **załącznik nr 2** do umowy.

§ 1.

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), zwanego w dalej „Rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
4. Podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na podstawie udokumentowanych poleceń Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia niniejszej umowy oraz ewentualnie inne polecenia przekazywane przez Administratora drogą elektroniczną na adres ....lub na piśmie.

§ 2.

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane osobowe (**należy podać rodzaj danych*) ..... *np. dane zwykłe oraz dane szczególnych kategorii* ..... *(*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora danych, osób składających wnioski itd. w zakresie* ..... *np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający, wyłącznie w celu ..... (**należy podać cel przetwarzania danych osobowych przez przetwarzającego dane*), wynikającego z realizacji umowy z dnia ..... nr ..... w zakresie.....*(*np. umowa o świadczenie usług).*

§ 3.

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający, zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych,

zapewniających adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2. 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 przetwarzanych danych w poufności, (zgodnie z przepisem art. 28 ust. 3 lit. b Rozporządzenia) oraz zobowiązać do tego również osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia (okresie współpracy) 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 (*należy wybrać czy przetwarzający dane ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie niezwłocznie, nie później jednak niż w terminie 7 dni *od dnia zakończenia świadczenia usług (postanowienia tego punktu nie stosuje się jeżeli prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.).* Przy czym Podmiot przetwarzający nie usunie danych osobowych bez wyraźnego polecenia Administratora.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32 -36 Rozporządzenia.

§ 4.
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli lub przeprowadzenia audytu czy środki zastosowane przez Pomiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator realizować będzie prawo kontroli i audytu w godzinach pracy Podmiotu przetwarzającego, informując o zamiarze ich przeprowadzenia z przynajmniej .... – dniowym . (**należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora, nie dłuższym niż 7 dni od dnia otrzymania zastrzeżeń na piśmie(**administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5.
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy i po uzyskaniu uprzedniej, pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku, przed rozpoczęciem przetwarzania, Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1 winien spełniać te same gwarancje i obowiązki, które zostały nałożone na Podmiotu przetwarzającego w umowie.

Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6.
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
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 umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez pracowników upoważnionych przez organ właściwy w sprawie ochrony danych osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
3. Podmiot przetwarzający odpowiada za szkody spowodowane własnymi działaniami i zaniechaniami, skutkującymi przetwarzaniem Danych osobowych w sposób naruszający przepisy RODO, inne powszechnie obowiązujące przepisy lub postanowienia Umowy, jeśli nie dopełnił obowiązków nałożonych na niego przez przepisy RODO, inne powszechnie obowiązujące przepisy lub postanowienia Umowy lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.
4. Podmiot przetwarzający ma obowiązek współdziałać z Administratorem na jego żądanie w zakresie ustalenia przyczyn szkody wyrządzonej osobie, której dane dotyczą.
5. W przypadku, gdy Administrator zapłacił odszkodowanie za całą wyrządzoną szkodę spowodowaną przetwarzaniem, ma prawo żądania od Podmiotu przetwarzającego zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi on odpowiedzialność zgodnie z ust. 3 powyżej.

§ 7.
Zgłaszanie incydentów

1. Podmiot przetwarzający zobowiązany jest po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Administratorowi bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin od stwierdzenia naruszenia.
2. Informacja przekazana Administratorowi powinna zawierać co najmniej:
   a) opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy,
   b) opis możliwych konsekwencji naruszenia,
   c) opis zastosowanych lub proponowanych do zastosowania przez Podmiot przetwarzający środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§ 8.
Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony** *od ..... do .....* .jednakże nie dłużej niż do dnia obowiązywania umowy, o której mowa § 2 ust. 2.
2. Każda ze Stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia, przy czym wypowiedzenie niniejszej umowy może skutkować brakiem możliwości realizacji umowy, o której mowa § 2 ust. 2.

§ 9.
Rozwiązanie i wygaśniecie umowy

1. Administrator może rozwiązać umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli i audytu nie usunie ich w wyznaczonym terminie;
   2) przetwarza dane osobowe w sposób niezgodny z umową lub poleceniami administratora;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora;
2. Umowa wygasa w przypadku rozwiązania wygaśnięcia umowy, o której mowa w § 2 ust 2.

§ 10.
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, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej (dalej zwanymi „danymi poufnymi").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych 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 prawa lub o której mowa w § 2 ust. 2.

§ 11.
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. W sprawach nieuregulowanych umową zastosowanie będą miały przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2019 r. poz. 1145), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).
3. Sądem właściwym dla rozpatrzenia sporów mogących wyniknąć z realizacji umowy będzie sąd właściwy dla Administratora (**lub Podmiotu przetwarzającego dane w zależności od postanowień stron*).

_____	_____
Administrator	*Podmiot przetwarzający*

Załączniki:

1. Dokument potwierdzający umocowanie przedstawiciela Administratora do działania w jego imieniu i na jej rzecz (*pełnomocnictwo/inne*).
2. Dokumenty potwierdzające umocowanie przedstawiciela Podmiotu przetwarzającego do działania w jego imieniu i na jego rzecz (*pełnomocnictwo/odpis z KRS/inne*).

Przed skorzystaniem przeczytaj poniższy komentarz, a następnie usuń go ze wzoru.
Jest to wzór podstawowej umowy powierzenia danych osobowych.

W przypadku powierzania danych na większą skalę lub danych wrażliwych, należy umowę rozbudować i dodatkowo zabezpieczyć NKB jako administratora (większe prawo kontroli, potwierdzenie spełnienia wymagań bezpieczeństwa).
Umowa może być wykorzystywana również w sytuacji, gdy NKB będzie podmiotem przetwarzającym wówczas można z kolei ograniczyć prawo kontroli – np. bez audytu pomieszczeń.

W przypadku dalszego powierzenia można wprowadzić w umowie zgodę na określone podmioty – znane w chwili zawarcia umowy. Jeżeli powierzamy dane osobowe firmie IT, która będzie je powierzać dalej podwykonawcy (np. usług hostingowych) – wówczas możemy z góry w umowie na to zezwolić

Załącznik nr 5

ARKUSZ OCENY PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE			
Data przeprowadzenia oceny		*(dd.mm.rrrr)*	
Dane oceniającego		*(imię, nazwisko, stanowisko/ funkcja)*	
Dane podmiotu ocenianego		*(nazwa, adres, dane kontaktowe)*	
Cel przetwarzania danych osobowych przez podmiot przetwarzający		*(przedmiot i data zawarcia umowy głównej)*	
KRYTERIA OCENY WYKONAWCY/PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE		**OCENA CZĄSTKOWA***	
		TAK	NIE
1.	Gwarancja zgodnego z prawem przetwarzania danych osobowych *(rekomendacje, dokumentacja ochrony danych itp.)*		
2.	Środki techniczne i organizacyjne dostosowane do stopnia zagrożenia bezpieczeństwa danych osobowych *(oświadczenie, analiza ryzyka)*		
3.	Personel daje rękojmię przetwarzania zgodnie z prawem *(upoważnienia, przeszkolenie, zachowanie tajemnicy przetwarzanych danych osobowych, itp.)*		
4.	Doświadczenie w zakresie ochrony danych osobowych *(w latach)***		
5.	Liczba incydentów bezpieczeństwa ochrony danych osobowych***		
6.	Liczba zwartych dotychczas umów powierzenia****		
7.	Certyfikaty/kodeksy postępowania, o których mowa w RODO/UODO		
OCENA			

		OCENA	
*	*należy zaznaczyć "X"*		
**	*gdy więcej niż 2 należy zaznaczyć "TAK"*	**POZYTYWNA*** *(gdy większe lub równe 4)*	**NEGATYWNA*** *(gdy większe lub równe 4)*
***	*gdy równe 0 należy zaznaczyć "TAK"*		
****	*gdy większe lub równe 1 należy zaznaczyć "TAK"*		

REJESTR UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH								Załącznik nr 6
Lp.	Nazwa podmiotu *(z którym zawarto umowę, adres siedziby)*	Data zawarcia umowy	Data wygaśnięcia umowy	Komórka organizacyjna zawierająca umowę powierzenia	Kategoria osób których dane dotyczą	Zakres czynności przetwarzania	Uwagi	
1.								
2.								
3.								

Rejestr czynności przetwarzania Załącznik nr 7

Rejestr ten powinien zawierać wszystkie informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

LP	1 Nazwa czynności przetwarzania	2 Jednostka organizacyjna (departament, dział itp.)	3 Cel przetwarzania Art. 30 ust. 1 pkt b	4 Kategorie osób Art. 30 ust. 1 pkt c	5 Kategorie danych Art. 30 ust. 1 pkt c	6 Podstawa prawna	7 Zbiór/-y danych	8 Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe) Art. 30 ust. 1 pkt f	9 Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy) Art. 30 ust. 1 pkt a	10 Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy) Art. 30 ust. 1 pkt d	11 Kategorie odbiorców (w tym podmiot przetwarzający) Art. 30 ust. 1 pkt d	12 Nazwa systemu lub oprogramowania	13 Ogólny opis (techniczny i organizacyjny) środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe) Art. 30 ust. 1 pkt g	14 Ocena skutków przetwarzania danych osobowych dla ochrony danych (DPIA) - Przeprowadzamy, jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (tak/nie)	15 Transfer do krajów trzecich lub organizacji międzynarodowych Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) Art. 30 ust. 1 pkt e	16 Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń Art. 30 ust. 1 pkt e
1.																
2.																

Rejestr kategorii czynności przetwarzania

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 2 RODO	Załącznik nr 8

	1	2	3	4	5	6	7	8	9	10	11
LP	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

Załącznik nr 9

Warszawa, ...

NKB-sek-00/2022/.....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), zwanego dalej „RODO",
z dniem: ..... (dd-mm-rr)

upoważniam Panią/Pana*: ..... (imię i nazwisko osoby upoważnionej), współpracującej z Naczelną Komisją Bioetyczną do spraw Badań Klinicznych w ramach ..... do przetwarzania danych osobowych zwykłych/ szczególnych* zgodnie z charakterem obowiązków wynikających z .....
**, na podstawie, której realizowane są polecenia administratora w rozumieniu art. 29 RODO.
Upoważnienie obejmuje przetwarzanie w systemach informatycznych i w dokumentacji papierowej.

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w zakresie: *zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie**

Niniejsze upoważnienie może być w każdym czasie odwołane.

Niniejsze upoważnienie wygasa z chwilą jego odwołania lub ustania stosunku prawnego na podstawie, którego przetwarzane są dane osobowe w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych.

Niniejsze upoważnienie wygasa z dniem ..... (dd-mm-rr) *

.....
pieczęć i podpis administratora danych

.....
data i podpis osoby upoważnionej

* – Niepotrzebne skreślić.
** Wpisać rodzaj umowy lub innego stosunku prawnego łączącego użytkownika z administratorem

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH								Załącznik nr 10
Lp.	Nazwisko i imię	Komórka organizacyjna	Stanowisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia- nazwę czynności przetwarzania lub procesu przetwarzania	Uwagi	
1.								
2.								
3.								
4.								

Załącznik nr 11

Poradnik dla użytkowników w zakresie podstaw rozpoznawania naruszeń ochrony danych osobowych

1. Pamiętaj, że naruszeniem ochrony danych osobowych jest nie tylko duży wyciek danych, atak hakerski czy włamanie do biura. Z naruszeniem ochrony danych osobowych możesz się zetknąć przy wykonywaniu standardowych czynności w ramach swojej pracy. Takie sytuacje często są wynikiem błędu ludzkiego (np. błędne zaadresowanie korespondencji), nieprawidłowego działania urządzenia (np. automatyczne, przedwczesne wykasowanie części bazy danych), zdarzenia losowego (takiego jak pożar), a tylko w skrajnych przypadkach - rażącego niedbalstwa lub umyślnego działania (np. kradzież bazy danych).

2. Zwróć uwagę, że sytuacje naruszenia ochrony danych osobowych generalnie mogą polegać na:
   1) nieuprawnionym zniszczeniu danych osobowych (np. skasowaniu);
   2) utracie danych osobowych (np. kradzieży laptopa służbowego lub zgubienia dysku przenośnego);
   3) nieuprawnionym zmodyfikowaniu danych osobowych (np. nadpisaniu, pomieszaniu);
   4) nieuprawnionym ujawnieniu danych osobowych (np. przesłaniu na błędny adres);
   5) nieuprawnionym uzyskaniu dostępu do danych osobowych (np. kradzieży bazy danych).

3. Twoją czujność powinny wzbudzić:
   1) uszkodzenia fizyczne stacji roboczych, drzwi, zamków, skrytek;
   2) niestandardowe komunikaty wyświetlane na ekranie urządzeń;
   3) znaczne spowolnienie działania systemu informatycznego;
   4) błędy w funkcjonowaniu systemu informatycznego (brak możliwości logowania, niedostępność funkcji, modułów lub aplikacji systemowych);
   5) przedłużający się brak możliwości odnalezienia określonych dokumentów, nośników danych lub urządzeń służących do przetwarzania danych osobowych (np. komputera, telefonu).

   Powyższe sytuacje nie zawsze świadczą o wystąpieniu naruszenia, ale należy je wyjaśnić.

4. Pamiętaj, że mamy obowiązek podjęcia określonych prawem działań w sytuacji stwierdzenia naruszenia ochrony danych osobowych, dlatego Twoja współpraca, szczególnie wykonywanie obowiązków opisanych poniżej, ma kluczowe znaczenie.

5. Pamiętaj, że Twoim obowiązkiem jest poinformowanie Inspektora Ochrony Danych o sytuacji, która w Twojej ocenie może stanowić naruszenie lub podejrzenie naruszenia ochrony danych osobowych. Powinieneś to zrobić natychmiast po zaobserwowaniu lub uzyskaniu wiedzy o takiej sytuacji. Powinieneś także podjąć rozsądne działania zmierzające do ograniczenia skutków naruszenia, a w następnej kolejności - odpowiednio do okoliczności - zabezpieczyć ślady mogące wskazywać na naruszenie (np. zrobić zrzut ekranu, zabezpieczyć pomieszczenie).

6. Pamiętaj, że jeśli naruszenie jest wynikiem Twojego błędu lub niedopatrzenia, to zgłaszając nam tę sytuację, działasz wyłącznie na swoją korzyść.
7. Pamiętaj, że informując o możliwym naruszeniu ochrony danych osobowych, dajesz nam szansę na odpowiednią reakcję i zapobiegnięcie negatywnym konsekwencjom naruszenia.
8. Za naruszenie lub podejrzenie naruszenia ochrony danych osobowych uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
   2) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmianę zawartości danych osobowych, utratę całości lub części danych osobowych);
   3) udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
   4) niezamierzoną zmianę lub utratę danych osobowych zapisanych na kopiach zapasowych;
   5) naruszenie lub próby naruszenia poufności, integralności i rozliczalności;

6) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu informatycznego);
7) nieuprawnione modyfikacje, kopiowanie lub uszkodzenie informacji przetwarzanej w systemie informatycznym;
8) nieuprawnione naruszenie lub próby naruszenia integralności systemu informatycznego,
9) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy;
10) zanotowanie, w krótkim czasie, dużej liczby nieudanych prób rozpoczęcia pracy w systemie informatycznym;
11) ujawnienie wirusów komputerowych lub innych programów godzących w poufność, integralność lub dostępność przetwarzanych danych osobowych w systemie informatycznym;
12) wydarzenia losowe obniżające poziom bezpieczeństwa systemu informatycznego (np. przerwa w zasilaniu lub pożar);
13) kradzież nośników przetwarzanych danych osobowych w systemie informatycznym (np. płyt CD, DVD, dysków twardych, pendrive'ach, dyskach zewnętrznych,);
14) nieuprawnione zmiany konfiguracji systemu informatycznego.

9. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których są przetwarzane dane osobowe lub próby takich działań.

Załącznik nr 12

Kryteria oceny wagi naruszenia

Głównymi kryteriami oceny wagi naruszenia (WN) są:

Kontekst przetwarzania danych osobowych **(KPD)** – główny czynnik określający poziom krytyczności zestawu naruszonych danych osobowych, w określonym kontekście przetwarzania.

Prawdopodobieństwo Identyfikacji (PI) – czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych osobowych dla osób, które uzyskały dostęp do nich.

Okoliczności Naruszenia (ON) – czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.

Każdy z czynników podlega wycenie:

WN = KPD * PI + ON

Kontekst przetwarzania danych osobowych – KPD

1. Rodzaj i poziom wrażliwości danych osobowych:
   1) dane podstawowe = 1
   2) dane dotyczące zachowań osoby = 2
   3) dane finansowe = 3
   4) dane szczególne = 4

2. Kontekst przetwarzania danych osobowych, który może podwyższyć lub obniżyć wycenę:
   1) szeroki zakres danych/wolumen danych (+)
   2) charakter danych (+/-)
   3) specyfika podmiotu danych lub administratora (+/-)
   4) możliwe negatywne skutki dla podmiotu danych (+)
   5) publiczna dostępność danych przed naruszeniem (-)
   6) nieważność danych (-)

Prawdopodobieństwo identyfikacji – PI

1. Prawdopodobieństwo identyfikacji
   1) znikome = 0,25
   2) ograniczone = 0,5
   3) wysokie = 0,75
   4) maksymalne = 1

Okoliczności Naruszenia – ON

1. Naruszenie poufności – dane osobowe ujawnione:
   1) znanym odbiorcom danych (+0,25)
   2) nieznanej liczbie odbiorców danych (+0,5)

2. Naruszenie integralności - dane osobowe zmienione i:
    1) możliwe jest ich odzyskanie (+0,25)
    2) brak jest możliwości ich odzyskania (+0,5)
3. Naruszenie dostępności – niedostępność danych osobowych:
    1) czasowa (+0,25)
    2) pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)
    3) intencjonalne działanie sprawcy (+0,5).

Wynik	**Waga naruszenia**	**Opis**	**Podejmowane działanie**
WN < 2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności.	Odnotowanie incydentu w rejestrze naruszeń odo i wpis do ewidencji naruszeń odo (nie podlega zgłoszeniu do organu nadzorczego).
2 ≤ WN <3	Średnia	Osoby mogą napotkać niedogodności, możliwe do pokonania.	Odnotowanie incydentu w rejestrze naruszeń odo i wpis do ewidencji naruszeń odo oraz zgłoszenie do organu nadzorczego.
3 ≤ WN < 4	Wysoka	Mogą wystąpić konsekwencje, możliwe do pokonania, ale z poważnymi skutkami.	Odnotowanie incydentu w rejestrze naruszeń odo i wpis do ewidencji naruszeń odo, zgłoszenie do organu nadzorczego.
4 ≤ WN	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje.	Odnotowanie incydentu w rejestrze naruszeń odo i wpis do ewidencji naruszeń odo, zgłoszenie do organu nadzorczego oraz powiadomienie osób, których naruszenie ochrony danych dotyczy.

Załącznik nr 13

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

(Miejsce sporządzenia), (DD/MM/RRRR)

(Oznaczenie Administratora)

(Adres Administratora)

Szanowny Panie/Szanowna Pani,

Informujemy, że wykryliśmy naruszenie ochrony danych osobowych, które dotyczy Pani/Pana danych osobowych obejmujących (*rodzaj lub kategorie danych objętych naruszeniem).*

Naruszenie polega na *(krótki i szczegółowy opis naruszenia).*

Skutkiem naruszenia dla Pani/Pana może być *(wskazanie możliwych ryzyk wynikających z naruszenia dla podmiotów danych).*

Przepraszamy za zaistniałą sytuację. Zapewniamy, że podejmujemy wszelkie możliwe działania w celu zminimalizowania ryzyka i ewentualnych negatywnych konsekwencji *naruszenia dla Pani/Pana sytuacji. W szczególności (*ogólny opis podjętych lub zaplanowanych działań naprawczych*).* Zdarzenie miało charakter incydentalny i wyniknęło z błędu ludzkiego, które było działaniem nieumyślnym.

W zaistniałej sytuacji rekomendujemy (*opis rekomendowanych działań*).

Jednocześnie uprzejmie informujemy, że Naczelna Komisja Bioetyczna do spraw Badań Klinicznych dokłada wszelkiej staranności, żeby Pani/Pana dane osobowe były przetwarzane w sposób gwarantujący ich bezpieczeństwo.

Dodatkowe informacje może Pani/Pan uzyskać, kontaktując się z nami *(dane kontaktowe, w tym numer telefonu lub adres e-mail IOD lub osoby wyznaczonej jako osoba kontaktowa w związku z naruszeniem).*

Z poważaniem

.....
(podpis)

Załącznik nr 14

Rejestr naruszeń i podejrzeń naruszeń ochrony danych osobowych																								
Dane dot. zgłoszenia						Dane dot. naruszenia/ podejrzenia naruszenia ochrony danych osobowych, jego skutków							Zgłoszenie / zawiadomienie o wystąpieniu naruszenia								Podjęte działania		
				Zgłaszający									Organu Nadzorczego (UODO)				Osób, których danych dot. naruszenie				Naprawcze	Zaradcze	
Lp	Naruszenie (stypizowany opis naruszenia)	Data i godzina zaistnienia naruszenia (dd-mm-rrrr) (00:00)	Data i godzina zakończenia naruszenia (dd-mm-rrrr) (00:00)	Imię i nazwisko	Dane kontaktowe	Nazwa procesu związanego z naruszeniem	Właściciel procesu biznesowego związanego z naruszeniem (wskazanie komórki organizacyjnej)	Opis naruszenia/ podejrzenia naruszenia (opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazać okoliczności takie jak przyczyna zdarzenia)	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych lub kategorie danych, których dotyczy naruszenie	Możliwe konsekwencje naruszenia/ podejrzenia naruszenia ochrony danych osobowych	Dot. podejrzeń Czy miało miejsce naruszenie ODO? (wybrać z listy rozwijanej)	Podjęte działania (wybrać z listy rozwijanej)	Data zgłoszenia (dd-mm-rrrr)	Godzina zgłoszenia (00:00)	Treść zgłoszenia	Podjęte działania (wybrać z listy rozwijanej)	Data zawiadomienia (dd-mm-rrrr)	Treść zawiadomienia	Powód braku zawiadomienia Art. 34 ust.3 RODO (wybrać z listy rozwijanej) 1 - ADO wdrożył odpowiednie środki techniczne i organizacyjne, 2 - Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub	Bieżące działania naprawcze (opisać środki zastosowane w celu złagodzenia ew. niekorzystnych skutków naruszeń ODO)	Odpowiedzialny komórki org.	Data zakończenia postępowania (dd-mm-rrrr)
	2	3	4	5	6	7	8	9			10	11	12	13	14	15	16	17	18	19	20	22	23

Załącznik nr 15

Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie w

.....
(nazwa procesu/ów objętego sprawdzeniem/)

Po przeprowadzeniu czynności sprawdzających u w: .....
.....
(imię i nazwisko osoby upoważnionej/osób upoważnionych objętej/tych sprawdzaniem)

w okresie od.....do....., przedstawiam sprawozdanie z dokonanych czynności sprawdzających.

1. Przedmiot i zakres sprawdzenia

Sprawdzeniem objęte było przetwarzanie danych osobowych w ramach realizowanego/nych procesu/ów określonego/ych w rejestrze czynności przetwarzania danych osobowych
.....
.....
.....
.....
(nazwa procesu/ów - z rejestru czynności przetwarzania danych osobowych)

Sprawdzenie dotyczyło danych osobowych w zakresie ich:

1) gromadzenia,
2) udostępniania,
3) zabezpieczenia,
4) usuwania.

(należy wybrać aspekty przetwarzania danych osobowych, które były objęte sprawdzeniem)

2. Wykaz czynności podjętych przez Inspektora Ochrony Danych

W toku sprawdzenia:

1) odebrano pisemne wyjaśnienia od.....
(imię i nazwisko osoby objętej czynnością)

2) przeprowadzono oględziny miejsca przetwarzania danych osobowych.....
.....
(oznaczenie obszaru)

3) zabezpieczono dokumentację opisującą przetwarzanie danych osobowych.

3. Opis stanu faktycznego stwierdzonego w toku sprawdzenia

W toku sprawdzenia ustalono co następuje:

Dane osobowe przetwarzane są w związku z realizacją procesu .....
.....w
celu/ach.....na podstawie.....
.....

.....
(przesłanka legalizująca przetwarzanie danych osobowych)

Przetwarzanie dotyczy.....w zakresie obejmującym następujące
(kategoria osób fizycznych)
dane zwykłe:.....
i szczególne kategorie danych:.....
.....

Dane te udostępniane są:.....
.....
(określenie podmiotów)
na podstawie
.....
(określenie podstawy prawnej)

Dane te są zabezpieczone w następujący sposób: .....
.....
.....
.....

Zalecenia i wnioski:.....
.....
.....
.....
.....
.....

.....
(data i podpis)

Załącznik nr 16

Porozumienie w sprawie współadministrowania danymi osobowymi

z dnia _____ zawarte pomiędzy:

Przewodniczący Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych,

zwaną dalej "**Administratorem 1**", reprezentowanąs przez: _____, na podstawie/zgodnie z _____, którego kopia stanowi **załącznik nr 1** do porozumienia

a

_____

zwanym dalej: "**Administratorem 2**",

reprezentowanym przez: _____,

na podstawie/zgodnie z _____, którego kopia stanowi **załącznik nr 2** do porozumienia,
zwanymi dalej łącznie "**Współadministratorami**" lub "**Stronami**", bądź każda z osobna "**Współadministratorem**" lub "**Stroną**".

§ 1.

1. Niniejsze porozumienie reguluje wzajemne stosunki pomiędzy Stronami w zakresie współadministrowania danymi osobowymi, a w szczególności ustala zakresy odpowiedzialności dotyczące wypełniania obowiązków wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), zwanego dalej „RODO", i innych przepisów prawa powszechnie obowiązującego, jak również określa sposób reprezentacji, w stosunku do podmiotów, których dane osobowe dotyczą oraz ich relacje z tymi podmiotami.
2. Dla potrzeb prawidłowej realizacji porozumienia Współadministratorzy zobowiązują się:

   1) współpracować przy realizacji obowiązków dotyczących ochrony danych osobowych;

   2) przetwarzać powierzone dane osobowe zgodnie z przepisami RODO oraz innymi przepisami prawa powszechnie obowiązującego;
   3) powstrzymywać się od działań faktycznych i prawnych, które mogłyby w jakikolwiek sposób naruszyć bezpieczeństwo danych osobowych albo narazić drugiego Współadministratora na odpowiedzialność cywilną, administracyjną lub karną.

3. W celu uniknięcia wątpliwości, z tytułu realizacji obowiązków wynikających z niniejszej Umowy, żadnemu ze Współadministratorów nie przysługuje wynagrodzenie ani prawo do żądania podwyższenia wynagrodzenia należnego Współadministratorowi, wynikającego z umowy podstawowej albo z innego stosunku prawnego.
4. Każdy Współadministrator pokrywa własne koszty i wydatki związane z prawidłowym wykonaniem niniejszej Umowy.

§ 2.

Niniejsze porozumienie zostało zawarte na czas .....

§ 3.

1. Współadministratorzy zobowiązani są zapewnić bezpieczeństwo przetwarzania danych osobowych przez stosowanie odpowiednich środków technicznych i organizacyjnych, adekwatnych do rodzaju danych osobowych oraz ryzyka naruszenia praw osób, których te dane dotyczą.
2. Współadministratorzy ustalają, że każdy ze Współadministratorów jest zobowiązany we własnym zakresie wywiązywać się z obowiązków informacyjnych, o których mowa w art. 13, art. 14 oraz art. 26 ust. 2 RODO.
3. Współadministratorzy ustalają, że w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, w szczególności realizacji żądań w zakresie prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych osobowych, sprzeciwu wobec przetwarzania danych osobowych właściwy będzie każdy Współadministrator.
4. Współadministratorzy są zobowiązani współpracować między sobą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą. W tym celu Współadministrator zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o każdym żądaniu osoby uprawnionej w ramach wykonywania przez tę osobę praw wynikających z RODO oraz udzielać drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.
5. Współadministratorzy ustalają, że w zakresie realizacji z obowiązków zarządzania naruszeniami ochrony danych osobowych oraz ich zgłaszania do organu nadzoru oraz osoby, której dane dotyczą, właściwy będzie Współadministrator, który stwierdził naruszenie. W przypadku, gdy naruszenie zostanie stwierdzone przez obydwu Współadministratorów, to właściwy do wykonania obowiązków określonych w art. 33 - 34 RODO będzie ten Współadministrator, z którego działania bądź zaniechania naruszenie wynikło.
6. Współadministratorzy są zobowiązani współpracować między sobą w zakresie spełniania obowiązków określonych w art. 33 i 34 RODO. W tym celu Współadministrator zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o każdym stwierdzonym naruszeniu ochrony danych osobowych, podjętych w związku z naruszeniem krokach, treści zgłoszenia przekazanego organowi nadzorczemu w związku z naruszeniem oraz udzielić drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.
7. W przypadku, gdy dany rodzaj przetwarzania danych osobowych, stosowany przez Współadministratora - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Współadministrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych i jest zobowiązany do spełnienia obowiązków określonych w art. 35 i 36 RODO. Współadministrator, o którym mowa w zdaniu poprzedzającym, zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o stwierdzeniu konieczności dokonania oceny skutków dla ochrony danych osobowych oraz przeprowadzenia konsultacji z organem nadzoru oraz udzielać drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.
8. Każdy Współadministrator jest zobowiązany we własnym zakresie prowadzić rejestr czynności przetwarzania, o którym mowa w art. 30 RODO, w przypadku, gdy obowiązek prowadzenia rejestru wynika z przepisów RODO.

§ 4.

1. Dostęp do danych osobowych mogą mieć jedynie pracownicy Współadministratora, którzy otrzymali upoważnienie do przetwarzania tych danych, poprzedzone złożeniem przez te osoby oświadczenia o zachowaniu tych danych oraz sposobie ich zabezpieczenia w poufności.
2. Dopuszcza się udostępnienie Administratorowi 2 w zakresie realizowanych zadań wewnętrznej dokumentacji, a także rozwiązań technicznych i organizacyjnych stosowanych przez Administratora 1 dotyczących ochrony danych osobowych.
3. Dopuszcza się powołanie przez Współadministratorów wspólnego inspektora ochrony danych.
4. Współpraca pomiędzy Wpóładministratorami, o której mowa w ust. 2 i 3, wymaga odrębnych ustaleń.

§ 5.

1. Współadministratorzy mogą powierzać przetwarzanie danych osobowych wyłącznie w celu realizacji czynności, w odniesieniu, do których zostały one przekazane. Powierzenie przetwarzania danych osobowych wymaga zgody Współadministratorów i ustalenia, który z Współadministratorów zawrze stosowną umowę powierzenia przetwarzania danych osobowych.
2. W przypadku niewykonania przez podmiot przetwarzający ciążących na nim obowiązków w zakresie ochrony danych osobowych, Współadministratorzy ponoszą odpowiedzialność solidarną za wykonanie zobowiązań ciążących na podmiocie przetwarzającym.
3. Zabronione jest umożliwienie dostępu do danych osobowych podmiotom, z którymi nie została zawarta umowa powierzenia przetwarzania danych osobowych, z wyłączeniem podmiotów przetwarzających dane osobowe z upoważnienia Administratora.

§ 6.

1. Współadministratorzy zobowiązani są udzielać sobie nawzajem wszelkich informacji niezbędnych dla wykazania wywiązywania się ze wszystkich obowiązków określonych w RODO.
2. Każdy Współadministrator zobowiązany jest, bez zbędnej zwłoki, powiadomić drugiego Współadministratora o wszelkich skargach, pismach, kontrolach organu nadzoru, postępowaniach sądowych i administracyjnych pozostających w związku z danymi osobowymi współadministrowanymi przez Strony oraz udostępniać Współadministratorowi wszelką dokumentację z tym związaną.

§ 7.

1. Każdy Współadministrator odpowiada za działania i zaniechania osób, które upoważnił do przetwarzania danych osobowych lub powierzył przetwarzanie danych osobowych, jak za działania lub zaniechania własne.
2. Każdy Współadministrator odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Administratora.
3. Każdy Współadministrator odpowiada za szkody spowodowane niezastosowaniem właściwych środków bezpieczeństwa.
4. Współadministrator dopuszczający się naruszenia przepisów RODO lub innych przepisów prawa powszechnie obowiązującego jest zobowiązany, w ramach swojej odpowiedzialności za przetwarzanie danych osobowych, do współpracy z drugim Współadministratorem w przypadku postępowania przed organem nadzorczym lub sporu sądowego z podmiotem danych osobowych.

§ 8.

1. Niniejsze porozumienie stanowi uzgodnienia pomiędzy Współadministratorami, o których mowa w art. 26 ust. 1 RODO.
2. Postanowienia porozumienia zastępują wszelkie inne ustalenia dokonane pomiędzy Stronami dotyczące przetwarzania danych osobowych osób uprawnionych, w stosunku do których Strony pozostają współadministratorami.
3. Wszelkie zmiany porozumienia wymagają zachowania formy pisemnej pod rygorem nieważności oraz muszą zostać podpisane przez osoby upoważnione do reprezentacji.
4. Porozumienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator 1 **Administrator 2**

_____ _____

Załączniki:

1. Dokument potwierdzający umocowanie przedstawiciela Administratora 1 do działania w jego imieniu i na jej rzecz (*pełnomocnictwo/inne*).
2. Dokumenty potwierdzające umocowanie przedstawiciela Administratora 2 do działania

w jego imieniu i na jego rzecz (*pełnomocnictwo/odpis z KRS/inne*).