Polityka Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju

Opracował:	Sprawdził:	Zatwierdził:
Zbigniew Zieliński Dyrektor DAG Podpis:	Waldemar Malinowski Kierownik SNO Podpis:	Jerzy Kątcki Z-ca Dyrektora Centrum Podpis:

Dokument jest nadzorowany i opublikowany w formie elektronicznej. Niniejszy dokument jest aktualny w dniu wydruku. Użytkownik egzemplarza jest zobowiązany do śledzenia zmian w dokumencie po terminie wydruku.

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja, usuwanie, dodawanie:

1. Pełnomocnik Dyrektora Centrum ds. Systemu Zarządzania Bezpieczeństwem Informacji – Dyrektor DAG
2. Administrator Bezpieczeństwa Informacji.

Zakres dostępu do dokumentu – odczyt:

3. Kierownicy Komórek Organizacyjnych.
4. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

Spis treści

1 Wstęp

Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających jednostką oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Pracownicy obsługujący systemy przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

Zastosowanie niniejszej Polityki Bezpieczeństwa Danych Osobowych powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do kategorii danych, jednocześnie dopasowane do poziomu zagrożeń występujących dla przetwarzanych i przechowywanych danych osobowych w Narodowym Centrum Badań i Rozwoju (NCBR). Niniejszy dokument został opracowany zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, 1662), zwanej dalej Ustawą. W związku z koniecznością spełnienia wymagań ochrony danych osobowych oraz w zgodności z § 3, § 4 oraz §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej Rozporządzeniem w sprawie dokumentacji, Administrator Danych Osobowych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa.

2 Cel

Celem Polityki Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju jest zapewnienie właściwej ochrony danych osobowych w NCBR. Polityka Bezpieczeństwa Danych Osobowych jest jednocześnie dokumentem określającym zadania osób funkcyjnych i pracowników służące realizacji zapewnieniu poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych.

Przyjęta Polityka Bezpieczeństwa Danych Osobowych powinna być rozwijana w sposób ciągły i zmieniać się wraz ze zmianami w strukturze organizacyjnej, pojawianiem się nowych zagrożeń i rozwojem dostępnych środków zapobiegawczych. Rozwijający się proces informatyzacji Centrum wymaga, by stosowane zasady były sformalizowane, stosowane oraz przyjęte jako obowiązujące reguły postępowania i sposoby zabezpieczeń danych osobowych. Zapewnienie systematycznego (co najmniej 1 raz w roku) porównywania stanu faktycznego z wymaganiami ochrony danych osobowych z zapisanymi w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji jest zadaniem KKO w komórkach organizacyjnych. Porównywanie jest realizowane pod nadzorem ABI w ramach cyklicznych sprawdzeń zgodności systemu ochrony danych osobowych. Dokument niniejszej polityki powinien być okresowo weryfikowany i dostosowywany do bieżących warunków prawnych, technologicznych i organizacyjnych zgodnie z zasadami przeglądu Systemu Zarządzania Bezpieczeństwem Informacji. W wyniku przeprowadzonych symulacji i treningów powinny być (jeśli to konieczne) zmodyfikowane odpowiednie fragmenty regulacji. Wprowadzane powinny być nowe elementy w przypadku pojawienia się niezdefiniowanych dotychczas zagrożeń lub zmiany wynikające z szacowania ryzyka w bezpieczeństwie informacji NCBR.

Dla skutecznej realizacji niniejszej Polityki, Administrator Danych Osobowych zapewnia:

a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

b) szkolenia w zakresie przetwarzania danych osobowych i sposobu ich ochrony,

c) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,

d) kontrolę i nadzór nad przetwarzaniem danych osobowych,

e) monitorowanie zastosowanych środków ochrony.

Zasady i regulacje niniejszej Polityki Bezpieczeństwa Danych Osobowych oraz Polityki Bezpieczeństwa Systemu Informatycznego nie mogą zmieniać ani zastępować obowiązujących przepisów prawnych.

Polityka Bezpieczeństwa Systemu Informatycznego stanowi Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w rozumieniu §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

3 Zakres stosowania

Politykę Bezpieczeństwa Danych Osobowych powinni stosować wszyscy pracownicy/współpracownicy, zewnętrzni wykonawcy oraz inne osoby zrzeszone lub uczące się, niezależnie od formy zatrudnienia lub współpracy, zaangażowani w proces przetwarzania danych osobowych. Zasady zapisane w niniejszym dokumencie oraz dokumentach związanych powinni stosować wszyscy pracownicy/współpracownicy NCBR.

Dokument ma zastosowanie do wszystkich danych osobowych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

Z dokumentem niniejszej Polityki powinni zapoznać się:

1. Administrator Danych Osobowych.
2. Kierownicy Komórek Organizacyjnych.
3. Administratorzy: Bezpieczeństwa Informacji, Bezpieczeństwa Systemów Informatycznych.
4. Pracownicy oraz współpracownicy przetwarzający dane osobowe.

Osoby przetwarzające dane osobowe w Centrum zapoznają się z zasadami ochrony danych osobowych w Regulaminie Użytkownika Systemu Informatycznego.

Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw.

4 Terminologia

Pojęcia używane w Polityce Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju oraz innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji są zdefiniowane w dokumencie ***Wspólny słownik pojęć używanych w Narodowym Centrum Badań i Rozwoju.***

5 Organizacja ochrony danych osobowych

5.1 Obowiązki Administratora Bezpieczeństwa Informacji

Administrator Danych może powołać Administratora Bezpieczeństwa informacji. Administrator Bezpieczeństwa Informacji realizuje obowiązki zgodnie z wymaganiami obowiązującej ustawy o ochronie danych osobowych oraz zgodnie z rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji.

5.1.1 Kryteria powołania Administratora Bezpieczeństwa Informacji/Zastępcy.

Administratorem Bezpieczeństwa Informacji może być osoba która:

a) Ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych

b) Posiada odpowiednią wiedzę w zakresie ochrony danych osobowych

c) Nie była karana za przestępstwo popełnione z winy umyślnej

Administrator Bezpieczeństwa Informacji podlega bezpośrednio Dyrektorowi Centrum, który zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji niezbędne do niezależnego wykonywania przez Administratora Bezpieczeństwa Informacji zadań opisanych w punkcie 5.1.4 niniejszej Polityki.

5.1.2 Rejestracja Administratora Bezpieczeństwa Informacji

Administrator Danych Osobowych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie Administratora Bezpieczeństwa Informacji w terminie 30 dni od dnia jego powołania lub odwołania.

Wzór zgłoszenia powołania Administratora Bezpieczeństwa Informacji zawiera rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania administratora bezpieczeństwa informacji od rejestracji Generalnemu Inspektorowi Danych Osobowych oraz odwołania administratora bezpieczeństwa informacji (Dz.U. 2014.1934).

Administrator Danych Osobowych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem Administratora Bezpieczeństwa Informacji, w terminie 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.

5.1.3 Wykreślenie administratora bezpieczeństwa informacji

Wykreślenie Administratora Bezpieczeństwa Informacji z rejestru administratorów bezpieczeństwa informacji następuje po powiadomieniu o jego odwołaniu, albo w przypadku jego śmierci.

Generalny Inspektor Ochrony Danych Osobowych wydaje Administratorowi Danych Osobowych decyzję o wykreśleniu Administratora Bezpieczeństwa Informacji z rejestru administratorów bezpieczeństwa informacji, jeżeli:

a) Administrator Bezpieczeństwa Informacji nie spełnia warunków określonych w p. 5.1.1

b) Administrator Bezpieczeństwa Informacji nie wykonuje zadań określonych w p. 5.1.4

c) Administrator Danych Osobowych nie powiadomił o odwołaniu administratora bezpieczeństwa informacji

5.1.4 Zadania Administratora Bezpieczeństwa Informacji i Zastępcy Administratora Bezpieczeństwa Informacji

Do zadań Administratora Bezpieczeństwa Informacji należy:

a) zapewnienie przestrzegania przepisów o ochronie danych osobowych,

b) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych Osobowych, w szczególności opracowywanie przez Administratora Bezpieczeństwa Informacji sprawozdań dla Administratora Danych Osobowych, o których mowa w art. 36a ust 2 pkt 1 lit. a ustawy o ochronie danych osobowych. Dostarczanie do Administratora Danych Osobowych sprawozdania odbywa się na formularzu, którego wzór stanowi załącznik nr 7 do niniejszej Polityki,

c) przygotowywanie planu sprawdzeń i przedstawianie administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń jest określeniem harmonogramu weryfikacji systemu ochrony danych osobowych przygotowywanym przez

Administratora Bezpieczeństwa Informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Jeden raz na pięć lat sprawdzeniem objęte są:

a. Zabezpieczenia: organizacyjne i techniczne
b. System informatyczny
c. Zbiory danych osobowych
d. Dokumentacja przetwarzania danych osobowych

d) sprawdzenia zgodności realizuje się w odniesieniu do kryteriów:

a. Art. 23–27 i art. 31–35 uodo
b. Art. 36 oraz art. 37–39 uodo
c. Art. 43 uodo
d. § 4, § 5, § 7 rozporządzenia w sprawie dokumentacji
e. Załącznik do rozporządzenia w sprawie dokumentacji

e) nadzorowanie opracowania i aktualizowania Polityki Bezpieczeństwa Danych Osobowych oraz Polityki Bezpieczeństwa Systemu Informatycznego wraz z dokumentami związanymi w zakresie ochrony danych osobowych,

f) nadzorowania przestrzegania zasad w określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w rozumieniu Rozporządzenia w Sprawie Dokumentacji oraz dokumentach związanych w zakresie ochrony danych osobowych,

g) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

h) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych,

i) prowadzenie wykazu pomieszczeń lub części pomieszczeń, tworzących obszar przetwarzania danych osobowych,

j) nadzór nad procedurami tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania,

k) nadzór nad sposobem, miejscem i okresem przechowywania elektronicznych nośników informacji zawierających dane osobowe, w tym kopii zapasowych,

l) nadzór nad sposobem zabezpieczenia systemów informatycznych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,

m) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których są przetwarzane dane osobowe oraz kontrolą przebywających w nich osób,

n) podejmowanie natychmiastowych działań zabezpieczających stan systemów informatycznych w przypadku otrzymania informacji wskazujących na naruszenie bezpieczeństwa danych,

o) analizowanie sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych osobowych oraz przedstawienie Administratorowi Danych Osobowych odpowiednich wniosków,

p) prowadzenie ewidencji zdarzeń zagrażających bezpieczeństwu informacji i bezpieczeństwu przetwarzania danych osobowych,

q) śledzenie skuteczności zastosowanych zabezpieczeń oraz zgłaszanie Administratorowi Danych Osobowych propozycji ich udoskonalania,

r) analiza i zarządzanie ryzykiem naruszenia bezpieczeństwa przetwarzania danych,

s) nadzorowanie prac komisji do spraw niszczenia kopii bezpieczeństwa i nośników danych,

t) współpraca z audytorem wewnętrznym w zakresie polityki bezpieczeństwa systemów informatycznych,

u) nadzór nad przetwarzaniem danych osobowych w systemach informatycznych, szczególnie z uwzględnieniem, jakie dane, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

5.1.5 Administrator Danych Osobowych może powierzyć Administratorowi Bezpieczeństwa Informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszej PBDO.

5.1.6 Zastępca Administratora Bezpieczeństwa Informacji wykonuje zadania wynikające z PBDO przypadku nieobecności Administratora Bezpieczeństwa Informacji w Centrum.

5.2 Obowiązki pracowników i innych osób zaangażowanych w przetwarzanie danych osobowych

5.2.1 Wszyscy pracownicy NCBR przetwarzający dane osobowe obowiązani są dołożyć szczególnej staranności w celu ochrony interesu osób, których dane dotyczą a w szczególności należy przestrzegać, aby dane te były:

a) przetwarzane zgodnie z prawem,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

5.2.2 Kierownicy Komórek Organizacyjnych oraz pracownicy na stanowiskach samodzielnych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych w obszarze swojej odpowiedzialności, a także do ścisłej współpracy z Administratorem Bezpieczeństwa Informacji. W tym celu zobowiązani są do:

a) pisemnego wnioskowania o rejestrację nowych zbiorów danych osobowych przed rozpoczęciem ich przetwarzania,

b) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,

c) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,

d) wnioskowania o wydanie upoważnień do przetwarzania danych osobowych i nadzór nad aktualnością upoważnień w zakresie podległych im pracowników,

e) zapewnienia systematycznego (co najmniej 1 raz w roku) porównywania stanu faktycznego z wymaganiami ochrony danych osobowych wynikającymi z dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji; porównywanie jest realizowane pod nadzorem lub przez ABI w ramach cyklicznych sprawdzeń zgodności systemu ochrony danych osobowych. Wzór sprawozdania ze sprawdzenia ochrony danych osobowych zawiera Załącznik nr 7 do niniejszej Polityki.

5.2.3 Naruszenie postanowień Polityki Bezpieczeństwa Danych Osobowych może skutkować zablokowaniem dostępu pracownika do danych i Systemu Informatycznego. Ponadto, w przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania umowy. W przypadku poniesienia strat w wyniku naruszenia, Centrum może dochodzić roszczeń odszkodowawczych na drodze sądowej.

6 Identyfikacja i rejestracja zbiorów danych osobowych

Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, nie podlega Administrator Danych Osobowych, który powołał i zgłosił Generalnemu Inspektorowi Ochrony Danych Osobowych Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji prowadzi rejestr zbiorów danych osobowych zgodnie z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych.

Ponadto Generalny Inspektor Danych Osobowych prowadzi rejestr zbiorów danych osobowych, które nie podlegają zwolnieniu z obowiązku rejestracji na podstawie powyżej podanego warunku oraz art. 43 ustawy o ochronie danych osobowych.

6.1 Procedura identyfikacji i sposób postępowania podczas rejestracji zbioru danych osobowych

6.1.1 Zgodnie z Ustawą, zbiór danych osobowych zgłaszany jest wnioskiem, będącym załącznikiem nr 9 do niniejszej Polityki, o wpisanie do rejestru zbiorów danych osobowych prowadzonego przez Administratora Bezpieczeństwa Informacji. Jeżeli zbiór zawiera dane wrażliwe osobowe, należy przeprowadzić procedurę rejestracji zbioru danych osobowych w GIODO.

6.1.2 W przypadku zbioru danych prowadzonego w wersji papierowej poza Systemem Informatycznym oraz zbierania danych osobowych poza Aplikacjami Centralnymi, obowiązkiem KKO jest:

a) Przygotowanie wniosku na zgłoszenie zbioru danych do GIODO, przy czym:

i. wniosek jest wypełniany, parafowany przez KKO, posiada opinię radcy prawnego, jest weryfikowany przez Administratora Bezpieczeństwa Informacji i akceptowany jest przez Administratora Danych Osobowych,

ii. wniosek jest przekazywany do Administratora Bezpieczeństwa Informacji w celu zaewidencjonowania w rejestrze przez niego prowadzonym lub elektronicznego zgłoszenia do platformy E-GIODO.

b) Wdrożenie i nadzór nad zabezpieczeniem przetwarzania danych, w tym:

i. przystosowanie warunków przetwarzania danych w zbiorze do warunków zgodnych z obowiązującymi przepisami,

ii. wnioskowanie o wydanie upoważnień do przetwarzania danych osobowych i nadzór nad aktualnością upoważnień w zakresie podległych im pracowników. Ewidencję osób upoważnionych do przetwarzania danych osobowych z określonego zbioru, zawierającej: imię i nazwisko osoby upoważnionej, datę nadania i datę ustania uprawnień do przetwarzania danych oraz zakres upoważnienia do przetwarzania danych osobowych prowadzi ABI dla wszystkich pracowników/współpracowników.

iii. KKO zobowiązany jest do potwierdzania we wniosku zasadności dostępu do przypisanego mu zbioru danych osobowych przez pracowników / współpracowników Centrum, dla których złożono stosowne wnioski o wydanie upoważnienia do przetwarzania danych osobowych.

iv. W przypadku zmiany na stanowisku Kierownika Komórki Organizacyjnej, nowo mianowany KKO (lub osoba go zastępująca) przejmuje automatycznie jego funkcję z identycznym zakresem uprawnień i obowiązków jak poprzedni KKO.

v. W przypadku zmian w strukturze organizacyjnej Centrum, których efektem jest rozwiązanie Komórki Organizacyjnej lub połączenie z inną, należy ustalić Komórkę Organizacyjną, która przejęła opiekę nad dotychczas przetwarzanymi zbiorami danych i jej KKO automatycznie przejmuje nad nim opiekę.

vi. Ewidencję użytkowników przetwarzających dane z określonego zbioru oraz zakres upoważnienia do przetwarzania danych osobowych prowadzi ABI dla wszystkich pracowników. Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna zawierać:

a) imię i nazwisko osoby upoważnionej,

b) datę nadania,

c) datę ustania uprawnień do przetwarzania danych,

d) zakres upoważnienia do przetwarzania danych osobowych,

e) identyfikator użytkownika zarejestrowany w systemie informatycznym.

2. Jeżeli przetwarzanie danych ze zbioru jest prowadzone z użyciem Systemu Informatycznego, obowiązkiem Administratora Bezpieczeństwa Informacji jest zaewidencjonowanie w rejestrze przez niego prowadzonym lub zgłoszenie zbioru danych do platformy E-GIODO, przy czym:

a) fakt powstania zbioru danych osobowych, podlegającego rejestracji lub aktualizacji, zgłaszany jest pisemnie do Administratora Bezpieczeństwa Informacji przez SNI wraz z wypełnionym wnioskiem,

b) wniosek wypełniany jest przez SNI we współpracy z Administratorem Bezpieczeństwa Informacji,

c) wniosek następnie weryfikuje Administrator Bezpieczeństwa Informacji.

d) za przystosowanie warunków przetwarzania danych w zbiorze do warunków obowiązujących zgodnie z niniejszą Polityką odpowiada SNI oraz Administrator Merytoryczny (AM), a nadzoruje Administrator Bezpieczeństwa Informacji,

e) AM zobowiązany jest do potwierdzania zasadności dostępu do przypisanego mu zbioru danych osobowych przez pracowników lub współpracowników Centrum, dla których złożono stosowne wnioski o wydanie upoważnienia do przetwarzania danych osobowych.

f) W przypadku zmiany na stanowisku Kierownika Komórki Organizacyjnej, nowo mianowany KKO (lub osoba go zastępująca) przejmuje automatycznie funkcję AM przypisana do poprzedniego KKO, z identycznym zakresem uprawnień i obowiązków jak poprzedni KKO.

g) W przypadku zmian w strukturze organizacyjnej Centrum, których efektem jest rozwiązanie Komórki Organizacyjnej lub połączenie z inną, należy ustalić Komórkę Organizacyjną, która przejęła opiekę nad dotychczas przetwarzanymi zbiorami danych i jej KKO automatycznie przejmuje funkcję AM.

h) KKO, w zakresie podległych mu pracowników lub współpracowników Centrum, wnioskuje o wydanie upoważnień do przetwarzania danych osobowych dla konkretnego zbioru danych osobowych i prowadzi nadzór nad aktualnością upoważnień będących w użyciu. Wzór wniosku zawiera Regulamin Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.

i) Ewidencję użytkowników przetwarzających dane z określonego zbioru oraz zakres upoważnienia do przetwarzania danych osobowych prowadzi ABI dla wszystkich pracowników.

j) Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna zawierać:

k) imię i nazwisko osoby upoważnionej,

i. datę nadania,

ii. datę ustania uprawnień do przetwarzania danych,

iii. zakres upoważnienia do przetwarzania danych osobowych,

iv. identyfikator użytkownika zarejestrowany w systemie informatycznym.

3. Każda zmiana informacji podlegających zgłoszeniu do rejestracji, następuje zgodnie z pkt. 1 i 2 z zachowaniem terminu 30 dni na jej dokonanie od dnia dokonania zmiany w zbiorze danych.

4. Zgodnie z art. 46 ustawy o ochronie danych osobowych przetwarzanie danych nie będących danymi, których mowa w art. 27 ust. 1 uodo, może zostać rozpoczęte po zgłoszeniu danego zbioru do Administratora Bezpieczeństwa Informacji.

5. Na wniosek KKO, skierowany do Administratora Bezpieczeństwa Informacji, wydawane są upoważnienia. Wzór upoważnienia stanowi załącznik nr 1 do niniejszej Polityki.

6. Szczegółowe zasady wydawania upoważnień dostępu do przetwarzania danych osobowych określone są w ***Procedurze kontroli dostępu do Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.*** .

7. Zbiór danych osobowych jest rejestrowany w wykazie zbiorów danych osobowych oraz rejestrze zbiorów danych osobowych zgodnie z niniejszą Polityką, przy czym jeżeli jest to zbiór prowadzony elektronicznie informacja o powstaniu zbioru jest zamieszczana w wykazie po otrzymaniu zawiadomienia od KKO.

7 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Wykaz budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe obejmuje obszary przetwarzania danych osobowych, w których wykonuje się operacje na danych osobowych:

- Zbieranie.

- Utrwalanie.
- Przechowywanie.
- Opracowywanie.
- Zmienianie.
- Udostępnianie.
- Usuwanie.

Należą do nich również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (pomieszczenia, w których znajdują się: szafy z dokumentacją pisemną, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco, skrytki bankowe, archiwum). Do obszaru chronionego zalicza się również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami) zawierające dane osobowe.

Wzór wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego stanowi załącznik nr 2 do niniejszej Polityki, a jest prowadzony przez Administratora Bezpieczeństwa Informacji w formie elektronicznej.

Szczególny nacisk położony na bezpieczeństwo strefy przetwarzania danych związany jest z koniecznością zapewnienia optymalnych warunków ochrony dla przetwarzanych informacji. W związku z powyższym przebywanie wewnątrz obszaru określonego, jako obszar przetwarzania danych osobowych, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą Administratora Danych Osobowych. Jednocześnie budynki lub pomieszczenia, w których przetwarzane są dane osobowe, zamykane są na czas nieobecności osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

Obszary danych osobowych są również wskazane na planach poszczególnych pięter budynku.

8 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Zagadnienia bezpieczeństwa wymagają identyfikacji przetwarzanych zasobów informacyjnych, a dokładniej wskazania nazw zbiorów danych oraz programów używanych do ich przetwarzania. W przypadku, gdy program zbudowany jest z wielu modułów i moduły te mogą pracować niezależnie np. mogą być instalowane na różnych stacjach komputerowych, wówczas wskazanie programu obejmuje wszystkie jego moduły. Wykaz ten zawiera informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, określenie KKO, lokalizacji przetwarzania wtórnego), w którym znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.

Każdy taki moduł przeznaczony jest do wykonywania wydzielonych przez zakres merytoryczny zadań na zbiorze danych osobowych. Dla wszystkich użytkowników posiadających dostęp do określonych programów wydawane jest Upoważnienie zezwalające na przetwarzanie danych w nich zawartych. KKO zobowiązani są do występowania o wydanie upoważnień do przetwarzania danych osobowych dla pracowników im podległych określając niezbędny zakres uprawnień.

AM lub KKO będący administratorem danego zbioru danych osobowych, zobowiązany jest do potwierdzenia zasadności dostępu do zbioru dla zgłaszanych pracowników lub osób współpracujących z Centrum, potwierdzając jednocześnie zakres niezbędnych uprawnień do tego zbioru. Powyższe potwierdzenie

następuje po uprzednim przedłożeniu wniosku o wydanie upoważnienia do przetwarzania danych osobowych przez przełożonego pracowników lub współpracowników Centrum, których wniosek dotyczy.

Wykaz zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania powinien zawierać minimum:

- Nazwy zbiorów danych osobowych.
- Nazwy programów przetwarzających dane osobowe.
- Zakres zbioru.
- Cel zbierania danych w zbiorze.
- Sposób zbierania danych osobowych (np. od osób których dane dotyczą).
- Podstawę prawną zbierania danych w zbiorze.

W Narodowym Centrum Badań i Rozwoju za pomocą programów lub w postaci ewidencji pisemnej przetwarzane są zbiory danych osobowych, umieszczone w Wykazie zbiorów danych osobowych prowadzonym w formie elektronicznej przez Administratora Bezpieczeństwa Informacji. Wzór wykazu zbiorów danych osobowych zawarty jest w załączniku nr 3 do niniejszej Polityki.

9 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Zgodnie z § 4 pkt 3 Rozporządzenia, dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych zakresów informacji w strukturze zbioru danych jednoznacznie wskazują kategorie danych, jakie są w nich przechowywane i przetwarzane. Należy przy tym pamiętać, że wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbioru danych, oznacza wymóg wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą. Załącznik nie przedstawia pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól, kluczy, definicji czy procedur itp. tylko ich interpretację pod kątem przetwarzania danych osobowych.

Opis może być prowadzony w formie:

- Graficznej.
- Opisu tekstowego.

Pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze danych osobowych, jest prowadzony przez Administratora Bezpieczeństwa Informacji. Przykładowy opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 4 do niniejszej Polityki.

10 Sposób przepływu danych pomiędzy systemami

Opis sposobu przepływu danych wskazuje, które z systemów są połączone oraz w jakim zakresie. Opis ten może być przedstawiony w postaci graficznej, ukazującej istniejące powiązania pomiędzy obiektami, jak również w postaci opisu tekstowego. Tworząc sposób przepływu danych osobowych należy uwzględnić możliwość wystąpienia przepływów:

1. Automatycznych.
   a) Półautomatycznych (np. import export plików przesyłanych za pomocą sieci).
   b) Manualnych – przy wykorzystaniu zewnętrznych nośników danych (płyty CD, DVD, PenDrive itp.).

Załącznik nr 5 do niniejszej Polityki zawiera wzór sposobu przepływu danych pomiędzy systemami, a połączenia pomiędzy systemami oraz zakres tych połączeń jest prowadzony zgodnie z tym wzorem przez Administratora Bezpieczeństwa Informacji.

11 Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Administrator Danych Osobowych zobowiązany jest upoważnić pracownika do przetwarzania danych osobowych w określonych zbiorach danych.

Administrator Danych Osobowych zobowiązany jest do zastosowania, adekwatnych do stwierdzonego poziomu ryzyka dla poszczególnych systemów, środków technicznych i organizacyjnych dla zapewnienia poufności, integralności, dostępności i rozliczalności przetwarzanych danych.

W zakresie środków organizacyjnych Narodowe Centrum Badań i Rozwoju wdraża:

1. Politykę Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju.
   a) Politykę Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.
   b) Regulamin Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.
   c) Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzoną przez Administratora Bezpieczeństwa Informacji powołanego przez Administratora Danych Osobowych. Wzór ewidencji stanowi załącznik nr 6 do niniejszego dokumentu.
   d) Rejestr zbiorów danych osobowych.
   e) Wykaz zbiorów danych osobowych zgodnie z załącznikiem nr 3.
   f) Wzór umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 8.
   g) Rejestr Podmiotów którym udostępniono do przetwarzania dane osobowe NCBR zgodnie z załącznikiem nr 10.
   h) Wniosek Zgłoszenia Zbioru Danych do rejestracji Administratorowi Danych Informacji zgodnie z załącznikiem nr 9.

W zakresie środków technicznych wdraża się:

1. Kontrolę dostępu do obszarów fizycznych przetwarzania danych osobowych.
   a) Ochronę kryptograficzną przesyłanych danych.
   b) Zabezpieczenia przed utratą danych (np. zapasowe zasilanie, wykonywanie kopii zapasowych itp.).

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych, naprawy, — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

Użytkując komputer przenośny zawierający dane osobowe należy zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem wskazanym w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Należy stosować środki ochrony kryptograficznej w stosunku do danych osobowych przetwarzanych na komputerach przenośnych o ile są używane poza obszarem przetwarzania danych osobowych.

Systemy chroniące dostęp z sieci publicznej do systemów przetwarzających dane osobowe muszą zapewniać:

1. Kontrolę przepływu informacji pomiędzy systemem informatycznym przetwarzającym dane osobowe, a siecią publiczną.
2. Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Szczegółowy opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawierają właściwe dokumenty Systemu Zarządzania Bezpieczeństwem Informacji.

Podpisanie umowy, związanej z powierzeniem przetwarzania danych osobowych, nadzoruje Kierownik Komórki Organizacyjnej przygotowujący umowę główną. Przed podpisaniem umowy związanej z powierzeniem przetwarzania danych osobowych, poprawność zapisów przedmiotowej umowy powinien zweryfikować Administrator Bezpieczeństwa Informacji. Kserokopia podpisanej umowy powierzenia przetwarzania danych przekazywana jest do Administratora Bezpieczeństwa Informacji w terminie 3 dni od dnia jej podpisania.

12 Zasady rozpowszechniania

Z zapisami Polityki Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju, które zostały zawarte w Regulaminie Użytkownika Systemu Informatycznego, powinna zapoznać się kadra kierownicza oraz pracownicy/współpracownicy, a także inne osoby mające dostęp do danych osobowych (stażyści odbywający staż, praktykanci odbywający praktykę).

Pracownicy firm zewnętrznych realizujących prace na podstawie odpowiednich umów zapoznają się z Regulaminem Ochrony Informacji dla Wykonawcy.

Niniejszy dokument może być udostępniony w celu zapoznania się i zgodnego postępowania tylko uprawnionym podmiotom zewnętrznym.

Nadzór nad przestrzeganiem Polityki Bezpieczeństwa Danych Osobowych oraz dokumentów związanych pełni Administrator Bezpieczeństwa Informacji.

Bieżący nadzór nad wypełnianiem zaleceń bezpieczeństwa w zakresie danych osobowych pełni Administrator Bezpieczeństwa Informacji.

Postępowanie niezgodne z niniejszą Polityką Bezpieczeństwa Danych Osobowych wiąże się ze skutkami przewidzianymi w Regulaminie Pracy oraz artykułach od 49 do 54 ustawy o ochronie danych osobowych.

Zmiany w niniejszym dokumencie wprowadzane są zgodnie z ***procedurą PZ3-4 Nadzór nad dokumentacją opisująca procesy.***

13 Odstępstwa od reguł ochrony

Odstąpienie od zasad opisanych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji jest możliwe wyłącznie po spełnieniu poniższych warunków:

a) Zwrócić się z pisemnym wnioskiem do Administratora Danych Osobowych o odstąpienie od reguł ochrony i uzasadnić we wniosku powód odstąpienia od przyjętych zasad bezpieczeństwa

b) Otrzymanie pisemnej decyzji Administratora Danych Osobowych

c) Postępować zgodnie z wymogami obowiązującego prawa

14 Wykaz aktów prawnych

Akty prawne, z których wynikają zasady ochrony informacji stosowane w NCBR, są wymienione w dokumencie ***Wykaz aktów prawnych w bezpieczeństwie informacji Narodowego Centrum Badań i Rozwoju*.**

15 Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju
2. Polityka Bezpieczeństwa Systemu Informatycznego
3. Regulamin Użytkownika Systemu Informatycznego
4. Regulamin Ochrony Informacji dla Wykonawcy
2. Regulamin Użytkownika Systemu Informatycznego
3. Wspólny słownik pojęć używanych w Narodowym Centrum Badań i Rozwoju.

16 Załączniki

Załącznik nr 1 – Wzór upoważnienia do dostępu do przetwarzania danych osobowych

Załącznik nr 2 – Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Narodowym Centrum Badań i Rozwoju

Załącznik nr 3 – Wzór wykazu zbiorów danych osobowych

Załącznik nr 4 – Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Załącznik nr 5 – Wzór sposobu przepływu danych pomiędzy systemami

Załącznik nr 6 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 7 – Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie

Załącznik nr 8 – Wzór umowy powierzenia przetwarzania danych osobowych.

Załącznik nr 9 – Wzór wniosku zgłoszenia zbioru danych do rejestracji Administratorowi Bezpieczeństwa Informacji

Załącznik nr 10 – Wzór rejestr podmiotów którym powierzono do przetwarzania dane osobowe NCBR

16.1 Załącznik nr 1 – wzór upoważnienia do dostępu do przetwarzania danych osobowych

Warszawa, ……

Egz. Nr ……

UPOWAŻNIENIE Nr ……

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135 j.t.)

upoważniam Panią/Pana ……. (identyfikator: ……..)

(imię, nazwisko)

do przetwarzania danych osobowych, w zbiorze prowadzonym z wykorzystaniem Systemu Informatycznego:

……..

……..

w zakresie zgodnym z Wnioskiem o nadanie, zmianę i odebranie uprawnień w celu realizacji powierzonych zadań.

Pani/Pan ……została/ł zapoznana/y z przepisami w zakresie ochrony danych osobowych, w szczególności z „Regulaminem Użytkownika Systemu Informatycznego".

Upoważnienie jest ważne od …… do ……

Jednocześnie nakładam obowiązek zabezpieczania danych osobowych przed ich udostępnieniem osobom nieuprawnionym, zabraniem, uszkodzeniem lub zniszczeniem, a także, do zachowania ich w tajemnicy. Obowiązek ten istnieje również po zakończeniu zatrudnienia/współpracy.

……
(pieczątka, data i podpis)

Oświadczam, że znane są mi przepisy z zakresu ochrony danych osobowych oraz zasady przetwarzanie danych osobowych w Narodowym Centrum Badań i Rozwoju.

Zobowiązuję się do zachowania danych osobowych przetwarzanych w Narodowym Centrum Badań i Rozwoju oraz sposobu zabezpieczenia w czasie trwania zatrudnienia/współpracy, jak również po ustaniu zatrudnienia/współpracy a także do zabezpieczania danych osobowych przed ich udostępnieniem, zabraniem przez osoby nieupoważnione, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

……
(data i podpis osoby upoważnionej)

16.2 Załącznik nr 2 - Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Narodowym Centrum Badań i Rozwoju

Lp.	Sekcja	Budynek, pomieszczenie lub część pomieszczenia tworzących obszar przetwarzania danych	Nazwa zbioru przetwarzanych danych osobowych
I.	**Budynek**		
1.			
2.			
3.			
II.			
1.			
2.			

16.3 Załącznik nr 3 – wzór wykazu zbiorów danych osobowych

Lp.	**Nazwa zbioru danych osobowych**	Nazwy programów przetwarzających dane osobowe	Zakres zbioru	Cel zbierania danych w zbiorze	**Sposób przetwarzania** Sposób zbierania danych osobowych		Podstawę prawną zbierania danych w zbiorze
					Tradycyjny	**w systemie informatycznym (nazwa programu)**	
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							
16.							
17.							
18.							

16.4 Załącznik nr 4 – opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru danych osobowych	Struktura zbioru	Powiązania między polami informacyjnymi
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

16.5 Załącznik nr 5 – wzór sposobu przepływu danych pomiędzy systemami

Lp.	Nazwa zbioru	Sposób przepływu danych pomiędzy poszczególnymi systemami
1.		

16.6 Załącznik nr 6 – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp	Nazwisko	Imię	Stanowisko	Data udzielenia upoważnienia	Data wstrzymania upoważnienia	Komórka/Sekcja	Zakres upoważnienia	Identyfikator użytkownika w systemie informatycznym	Uwagi
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
34									
35									
36									
37									
38									
39									
40									
41									
42									
43									
44									

16.7 Załącznik nr 7 – Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie

Sprawozdanie ze sprawdzenia	planowego nr X/20XX pozaplanowego nr ..... (nr kolejny/ rok)* * niepotrzebne skreślić

1. Osoby uczestniczące w sprawdzeniu

2. Opis przeprowadzonych działań

3. Efekty przeprowadzonych działań po ostatnim sprawdzeniu

4. Zalecenia i wnioski

4.1 Sprawdzenie zabezpieczeń fizycznych i organizacyjnych

4.2 Sprawdzenie zabezpieczeń informatycznych

Dokument sporządził:	Dokument zatwierdził:
(imię, nazwisko, stanowisko, data i podpis)	*(imię, nazwisko, stanowisko, data i podpis)*

5. Wykaz załączników

Podpis:

16.8 Załącznik nr 8 – Wzór umowy powierzenia przetwarzania danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

wzór „Umowa Powierzenia Przetwarzania Danych Osobowych”

W związku z zawarciem przez Narodowe Centrum Badań i Rozwoju (dalej: „Zamawiający”) oraz …….. (dalej: „Wykonawca”) w dniu …… Umowy nr ……. (dalej: „Umowa”), zgodnie z § …… ust. …….. Umowy, Strony zawierają niniejszą umowę powierzenia przetwarzania danych (dalej: „Umowa w Sprawie Danych”):

1. Zamawiający, jako administrator danych w rozumieniu art. 7 pkt. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135 j.t.) (dalej: „ustawa o ochronie danych osobowych”) powierza Wykonawcy do przetwarzania bazy danych: „…” zawierające dane osobowe … . Zakres powierzonych do przetwarzania danych obejmuje:

    a) ….

2. Powierzenie przetwarzania danych osobowych, o którym mowa w ust. 1, następuje wyłącznie w zakresie niezbędnym w celu prawidłowej realizacji Umowy przez Wykonawcę. Wykonawca nie jest uprawniony do jakiegokolwiek dalszego wykorzystania i udostępniania powierzonych danych osobowych ani do przechowywania i sporządzania kopii bezpieczeństwa powierzonych danych w zakresie, który nie jest konieczny do prawidłowej realizacji Umowy.

3. W związku z powierzeniem Wykonawcy przetwarzania danych osobowych, o których mowa w ust. 1, Wykonawca zobowiązuje się do zachowania najwyższej staranności oraz do zastosowania przy ich przetwarzaniu wszelkich środków technicznych i organizacyjnych przewidzianych dla administratora danych w art. 36-39a ustawy o ochronie danych osobowych oraz do przestrzegania wymogów Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100 poz. 1024) (dalej: „Rozporządzenie”) i stosowania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych, o którym mowa w Rozporządzeniu. W zakresie przestrzegania tych przepisów Wykonawca ponosi odpowiedzialność na zasadach przewidzianych dla administratora danych.

4. Wykonawca oświadcza, że miejscem przetwarzania danych osobowych w rozumieniu § 4 ust. 1 Rozporządzenia jest ..... .

5. Wykonawca nie może powierzyć czynności przetwarzania danych osobowych, o których mowa w ust.1, osobom trzecim. W przypadku powierzenia realizacji części Umowy podmiotowi trzeciemu na zasadach określonych w Umowie, Wykonawca odpowiedzialny jest za zawarcie przez ten podmiot z Zamawiającym umowy o powierzenie przetwarzania danych osobowych, zgodnie z postanowieniami § ……. Umowy.

6. Do przetwarzania danych osobowych, o których mowa w ust. 1, mogą być dopuszczeni jedynie pracownicy Wykonawcy posiadający imienne upoważnienie do przetwarzania danych osobowych (dalej: „upoważnieni pracownicy”). Upoważnienie wygasa z chwilą ustania zatrudnienia upoważnionego pracownika bądź odwołania upoważnienia. Upoważnienie nie może przekraczać zakresu czynności określonego w ust. 2.

7. Wykonawca prowadzi ewidencję upoważnionych pracowników wyznaczonych do przetwarzania danych osobowych powierzonych Wykonawcy przez Zamawiającego w związku z wykonywaniem Umowy.

8. Wykaz wyznaczonych upoważnionych pracowników oraz kopie wydanych im upoważnień zostaną dostarczone Zamawiającemu przez Wykonawcę w terminie …… dni roboczych po zawarciu Umowy. Aktualizacje rejestru wyznaczonych upoważnionych pracowników oraz kopie wydanych upoważnień będą dostarczane Zamawiającemu przez Wykonawcę w terminie 5 dni roboczych od ich udzielenia.

9. Wykonawca oświadcza, że upoważnieni pracownicy zostali zapoznani i przeszkoleni z zasad ochrony danych osobowych. Upoważnieni pracownicy nie mogą wykonywać operacji na danych przekraczających zakres wydanych im upoważnień ani posiadać prawa dostępu do danych w zakresie szerszym, niż wynikałoby to z upoważnienia lub też przetwarzać danych w celu innym, niż ten, do którego zostali upoważnieni. Za działania upoważnionych pracowników, Wykonawca ponosi odpowiedzialność jak za działania własne.

10. W celu właściwego zapewnienia bezpieczeństwa wszystkich danych, o których mowa w ust. 1, powierzonych przez administratora danych, Wykonawca zobowiązuje się do zachowania najwyższej staranności, w tym do postępowania zgodnego z przepisami ustawy o ochronie danych osobowych oraz wymogami Rozporządzenia.

11. Wykonawca zobowiązuje się do udzielania Zamawiającemu na każde żądanie informacji na temat przetwarzania powierzonych danych osobowych, a w szczególności do niezwłocznego przekazywania informacji o każdym przypadku naruszenia przez niego i jego pracowników obowiązków dotyczących ochrony danych osobowych.

12. Wykonawca zobowiązuje się do niezwłocznego informowania Zamawiającego o wszelkich przypadkach naruszenia bezpieczeństwa oraz tajemnicy danych osobowych lub ich niewłaściwym użyciu, a także o wszelkich czynnościach związanych z danymi osobowymi objętymi Umową w Sprawie Danych prowadzonych przed Generalnym Inspektorem Ochrony Danych Osobowych, urzędami państwowymi, policją lub sądami.

13. W przypadku wystąpienia okoliczności, o których mowa w ust. 11 i 12 Wykonawca jest zobowiązany do podjęcia wszelkich niezbędnych środków w celu ochrony danych osobowych, o których mowa w ust. 1.

14. Wykonawca zobowiązuje się do:

    a) umożliwienia Zamawiającemu dokonania kontroli w miejscach, w których są przetwarzane powierzone dane osobowe, w zakresie stosowania postanowień Umowy w Sprawie Danych, w terminie ustalonym przez Strony, nie później jednak niż w terminie 7 dni kalendarzowych od dnia powiadomienia Wykonawcy przez Zamawiającego o zamiarze przeprowadzenia kontroli, w celu sprawdzenia prawidłowości przetwarzania oraz zabezpieczania danych osobowych,

    b) zastosowania się do zaleceń pokontrolnych Zamawiającego, dotyczących poprawy jakości zabezpieczania danych osobowych oraz sposobu ich przetwarzania, o ile zalecenia te są zgodne z przepisami prawa.

15. Po zakończeniu realizacji Umowy, lub na pisemną prośbę Zamawiającego, Wykonawca zwróci Zamawiającemu wszystkie nośniki z otrzymanymi danymi osobowymi, a w przypadku sporządzenia dodatkowych kopii, trwale usunie je z wszelkich nośników, które nie zostały zwrócone Zamawiającemu.

16. Wykonawca zobowiąże wszystkich swoich pracowników, którzy na podstawie niniejszej Umowy w Sprawie Danych biorą udział w przetwarzaniu powierzonych mu danych osobowych, do zachowania w poufności wszelkich uzyskanych danych osobowych i informacji. Zobowiązanie, o którym mowa w

zdaniu poprzedzającym, obowiązuje bezterminowo, także po ustaniu zatrudnienia osób, o których mowa w zdaniu poprzedzającym, u Wykonawcy.

16.9 Załącznik nr 9 - Wniosek Zgłoszenia Zbioru Danych do rejestracji Administratorowi Bezpieczeństwa Informacji

Warszawa dnia xx.xx.xxxx

Wnioskujący [Kierownik Komórki Organizacyjnej]

Imię i Nazwisko……

Oznaczenie Komórki Organizacyjnej……

Lp.	Nazwa zbioru danych osobowych	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Forma przetwarzania danych zbiorze	Sposób prowadzenia zbioru danych osobowych		Kategorie danych osobowych przetwarzanych	Sposób udostępniania danych ze zbiorów	Powierzenie przetwarzania danych osobowych	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego
					Centralny	Rozproszony				
1										
2										
3										
4										
5										
6										

Opis pól wniosku:

Nazwa zbioru danych osobowych – KKO dowolnie określa nazwę zbioru. Zaleca się, aby nazwa zbioru była zwięzła i adekwatna do rodzaju danych przetwarzanych w zbiorze.

Podstawa prawna upoważniająca do przetwarzania danych w zbiorze:

– w przypadku gdy przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa KKO powinien precyzyjnie określić przepisy prawa, które zezwalają na przetwarzanie danych osobowych, wskazując tytuł oraz miejsce publikacji aktu prawnego

- w przypadku gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego - należy opisać te zadania

Cel przetwarzania danych w zbiorze - W punkcie tym należy dokładnie opisać cel, dla którego dane są przetwarzane w zbiorze.

Forma przetwarzania danych zbiorze – należy określić, czy dane w zbiorze przetwarzane są wyłącznie w postaci papierowej, czy też z użyciem systemu informatycznego.

Sposób prowadzenia zbioru danych osobowych - należy zaznaczyć jedną z dwóch możliwości przetwarzania danych. Centralne prowadzenie zbioru danych, zarówno w przypadku przetwarzania danych w systemie informatycznym jak i w tzw. systemie tradycyjnym (papierowym), oznacza zlokalizowanie danych w jednym miejscu. Zbiór prowadzony jest centralnie w sytuacji zgromadzenia danych (zarówno w postaci papierowej jak i zamieszczonych na serwerze) w jednym pomieszczeniu lub budynku. Prowadzenie zbioru w architekturze rozproszonej, zarówno w przypadku przetwarzania danych w systemie informatycznym jak i w tzw. systemie tradycyjnym papierowym), oznacza że dane są przetwarzane w sposób zdecentralizowany. Zbiór prowadzony jest w architekturze rozproszonej (w przypadku przetwarzania danych w systemie informatycznym) np. w sytuacji gromadzenia danych na dwóch serwerach zlokalizowanych w odrębnych budynkach.

Kategorie danych osobowych przetwarzanych - W punkcie tym należy wskazać jakich kategorii osób dotyczą dane przetwarzane w zbiorze (np. klienci, darczyńcy).

Sposób udostępniania danych ze zbiorów - W punkcie tym należy zaznaczyć pole wyboru, jeżeli pozyskane dane będą przekazywane podmiotom innym niż uprawnione do ich pozyskania na podstawie obowiązujących przepisów prawa.

Powierzenie przetwarzania danych osobowych - Jeżeli KKO zamierza powierzyć przetwarzanie danych osobowych innemu podmiotowi w punkcie tym należy podać numer umowy, datę podpisania, nazwę i siedzibę podmiotu, któremu powierzono przetwarzanie danych osobowych.

Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego - Jeżeli KKO zamierza przekazywać dane osobowe do państwa trzeciego, tj. państwa nienależącego do Europejskiego Obszaru Gospodarczego, powinien spełnić warunki określone w art. 47 lub art. 48 ustawy o ochronie danych osobowych.

16.10 Załącznik nr 10 - Rejestr Podmiotów, którym powierzono do przetwarzania dane osobowe NCBR

Lp.	Nazwa, adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych	Numer lub oznaczenie umowy powierzenia przetwarzania danych osobowych	Okres przetwarzania		Nazwa udostępnionego zbioru/zasobu danych osobowych	Podstawa prawna upoważniająca do przetwarzania danych w zbiorze	Cel przetwarzania danych w zbiorze	Forma przetwarzania danych zbiorze (papierowa, elektroniczna)	System przetwarzania (w przypadku wykorzystania systemu informatycznego)	Kategoria powierzonych danych osobowych	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego - należy podać nazwę państwa
			Od daty	Do daty							
1											
2											
3											
4											
5											
6											

17 Rejestr zmian

Lp.	Data	Opis	Dotyczy stron(y)	Wprowadzający zmianę