

KODEKS POSTĘPOWANIA
W SPRAWIE PRZETWARZANIA DANYCH OSOBOWYCH
DLA CELÓW BADAŃ NAUKOWYCH
PRZEZ BIOBANKI W POLSCE
(PROJEKT)

Przygotowany
przez zespół ds. etycznych prawnych i społecznych aspektów biobankowania (ELSI)
działający w ramach konsorcjum BBMRI.pl

Red. dr hab. Jakub Pawlikowski (UML), dr Dorota Krekora-Zajac (UW)

Skierowano do konsultacji zewnętrznych dnia 20 czerwca 2018 r.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wzrostego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

Spis treści

WPROWADZENIE	3
1. CEL KODEKSU	4
2. DEFINICJE	4
3. DOPUSZCZALNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH I INNYCH DANYCH WRAŻLIWYCH DLA CELÓW BADAŃ NAUKOWYCH	7
4. ZASADY PRZETWARZANIA DANYCH DLA CELÓW NAUKOWYCH PRZEZ BIOBANKI NA PODSTAWIE ZGODY OSOBY, KTÓREJ DANE DOTYCZA	8
5. WTÓRNE PRZETWARZANIE DANYCH NAUKOWYCH BEZ KONIECZNOŚCI UZYSKIWANIA PONOWNEJ ZGODY	11
5.2. PRZETWARZANIE DANYCH POCHODZĄCYCH Z DOKUMENTACJI MEDYCZNEJ	13
6. PRZETWARZANIE DANYCH NIE PODLEGAJĄCYCH REGULACJI ROZPORZĄDZENIA	13
6.1 DANE OSÓB ZMARŁYCH (MOTYW 27 PREAMBULY RODO)	13
6.2 DANE ANONIMOWE I ZANONIMIZOWANE	15
7. ZASADY OCHRONY DANYCH PRZETWARZANYCH DLA CELÓW NAUKOWYCH	15
7.1 MINIMALIZACJA DANYCH	16
7.2 PSEUDONIMIZACJA	16
7.3 ZALECENIA TECHNICZNE SŁUŻĄCE ZAPEWNIENIU BEZPIECZEŃSTWA DANYCH PRZETWARZANYCH PRZEZ BIOBANKI	17
8. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE DLA CELÓW BADAŃ NAUKOWYCH PRZEZ BIOBANKI	19
8.1 PRAWO DO WYCOFANIA ZGODY I ZAPRZESTANIA PRZETWARZANIA DANYCH	19
8.2 PRAWO DO SPROSTOWANIA DANYCH	19
8.3 PRAWO DO INFORMACJI O PRZETWARZANYCH DANYCH, W TYM DO DO INFORMACJI O PRZYPADKOWO WYKRYTYCH ISTOTNYCH INFORMACJACH DOTYCZĄCYCH ZDROWIA	19
8.4 PRAWO DO INFORMACJI O SKUTKACH ANONIMIZACJI DANYCH	20
8.5 PRAWA OSÓB NIEZDOLNYCH DO WYRAŻENIA ZGODY	21
9. ADMINISTRATOR DANYCH I INSPEKTOR DANYCH	21
10. OBOWIĄZEK ZGLASZANIA NARUSZEŃ	22
11. TRANSGRANICZNA WYMIANA DANYCH	23
12. PRZYJĘCIE KODEKSU	24



BBMRI.pl

BioBanking and
BioMolecular resources
Research Infrastructure
Poland

Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

WPROWADZENIE

Od 25 maja 2018 r. Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (nazywane dalej „RODO” lub „Rozporządzeniem”) będzie stosowane wprost do każdego przetwarzania danych osobowych we wszystkich krajach Unii Europejskiej w tym również w Polsce. W przypadku sprzeczności pomiędzy polską ustawą o ochronie danych osobowych a Rozporządzeniem stosowane będzie Rozporządzenie (wyjątkiem jest sytuacja, w której ustawa będzie zawierała szerszy zakres gwarancji praw osoby, której dane dotyczą).

Poniżej prezentujemy kodeks postępowania w sprawie przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce opracowany przez konsorcjum BBMRI.pl na podstawie art. 40 Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 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.

Dostrzegając szczególną rolę bezpieczeństwa danych dawców i pacjentów w biobankach oraz uznając, że podstawą funkcjonowania biobanków jest szczególne zaufanie jakim są one darzone przez pacjentów/dawców/uczestników badań, a dane zebrane przez biobanki mogą być przetwarzane przez trudny do określenia czas, proponujemy standardy postępowania zarówno w odniesieniu do przetwarzania danych osobowych od osób żyjących (których Rozporządzenie dotyczy bezpośrednio), jak i danych pochodzących od osób zmarłych (w zakresie tych danych Rozporządzenie pozostawia państwom członkowskim swobodę regulacji).

Uwzględniając również specyfikę pozyskiwania danych osobowych przez biobanki oraz szczególną sytuację prawną tych podmiotów w Polsce proponujemy również standardy dotyczące wtórnego wykorzystania danych pacjentów/dawców/uczestników badań dla celów badań naukowych przez biobanki funkcjonujące w naszym kraju. Postanowienia kodeksu uwzględniają przepisy krajowe zawarte w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2017 r. poz. 1318), ustawie z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2018 r. poz. 617), ustawie z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej (t.j. Dz.U. z 2016 r. poz. 2245), ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (t.j. Dz.U. z 2018 r. poz. 87) oraz innych aktów prawnych, także normy i zalecenia etyczne zawarte w Deklaracji z Tajpej Światowego Stowarzyszenia Lekarzy (WMA) w sprawie etycznych aspektów medycznych baz danych i biobanków (2016), Wytycznych Organizacji Współpracy



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wzrostu

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

Gospodarczej i Rozwoju (OECD) w zakresie biobankowania materiału ludzkiego i tworzenia baz danych genetycznych dla celów badań naukowych (2009) oraz innych dokumentów regulujących prowadzenie badań naukowych z wykorzystaniem ludzkiego materiału biologicznego.

1. CEL KODEKSU

Nadrzędnym celem Kodeksu jest stworzenie właściwego poziomu ochrony pacjentów/dawców/uczestników badań, których dane przetwarzane są przez biobanki polskie dla celów naukowych. Kodeks doprecyzowuje regulacje wynikające z Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 uwzględniając specyfikę przetwarzania danych osobowych przez biobanki, a żadne z postanowień Kodeksu nie powinno być interpretowane sprzecznie z Rozporządzeniem.

Konsekwencją stosowania się do niniejszego Kodeksu jest stworzenie domniemania wywiązywania się przez administratorów danych z obowiązków wynikających z Rozporządzenia, a w szczególności z zasady rozliczalności.

2. DEFINICJE

Użyte w kodeksie określenia oznaczają:

- 1) biobank - jednostka organizacyjnie posiadająca lub nieposiadająca osobowości prawnej przetwarzająca dane osobowe dla celów badań naukowych oraz zbierająca, przechowująca i przekazująca dla celów naukowych ludzkie próbki biologiczne oraz dane osobowe z nimi powiązane;
- 2) pacjent - osobę zwracającą się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny;
- 3) dawca - osoba przekazująca swoje dane osobowe wraz z materiałem biologicznym w celu wykorzystania dla celów naukowych przez biobank;
- 4) uczestnik badania - osoba przekazująca swoje dane osobowe wraz z materiałem biologicznym w celu wykorzystania dla celu określonego projektu naukowego;
- 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

4



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

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 w rozumieniu art. 4 pkt 1 RODO;

- 6) dane osobowe szczególnie chronione (wrażliwe) - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby w rozumieniu art. 9 ust. 1 RODO;
- 7) dane anonimowe - informacje, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, w rozumieniu motywu (26) RODO;
- 8) dane zanonimizowane - dane osobowych przekształcone w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować w rozumieniu motywu (26) RODO;
- 9) dane pseudonimizowane - dane osobowe przetworzone w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
- 10) dane osób zmarłych - dane dotyczące osoby zmarłej pobrane za jej życia jako dane osobowe lub po jej śmierci z dokumentacji medycznej w rozumieniu art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta ;
- 11) przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak 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 w rozumieniu art. 4 pkt 2 RODO;
- 12) badania naukowe - badania podstawowe, badania stosowane oraz badania finansowane ze środków zarówno publicznych i prywatnych, w szczególności badania prowadzone w interesie publicznym w



dziedzinie zdrowia publicznego oraz działania badawczo-rozwojowe w rozumieniu art. 2 ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (t.j. Dz.U. z 2018 r. poz. 87);

- 13) opinia komisji bioetycznej - uchwała w przedmiocie wyrażenie opinii o projekcie eksperymentu medycznego podejmowana przez właściwą komisję bioetyczną w rozumieniu Rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 11 maja 1999 r. w sprawie szczegółowych zasad powoływania i finansowania oraz trybu działania komisji bioetycznych (Dz.U. 1999 Nr 47, poz. 480);
- 14) administrator danych - administratorem danych osobowych przetwarzanych przez biobank dla celów badań naukowych jest biobank posiadający osobowość prawną lub podmiot, którego jest on jednostką organizacyjną. Biobank udostępniający dane osobowe podmiotowi prowadzącemu badania naukowe dokonuje tego albo na podstawie umowy o powierzenia przetwarzania danych (wtedy gdy samodzielnie określa cele przetwarzania) albo poprzez udostępnienie ich współadministratorowi (wówczas gdy wraz z podmiotem prowadzącym badania naukowe określa cele przetwarzania oraz oba podmioty przetwarzają dane osobowe na tej samej podstawie prawnej).

Wyjaśnienie:

W rozumieniu RODO każda osoba fizyczna i prawna przechowująca, zbierająca lub udostępniająca dane osobowe dla celów badań podstawowych lub stosowanych będzie podmiotem zobowiązanym do stosowania Rozporządzenia. Brak podmiotowości prawnej niektórych biobanków oznacza, że podmiotem przetwarzającym dane będą uczelnie, uniwersytety, szpitale, spółki i inne osoby prawne, których są one częściami, a tym samym podmioty te winny uwzględnić w polityce ochrony danych w obrębie swoich jednostek specyfikę przetwarzania danych w ramach biobankowania ludzkiego materiału biologicznego;

Rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób fizycznych a zatem nie będzie stosowane do przetwarzania danych osób zmarłych (nie posiadają one już osobowości prawnej) oraz danych anonimowych i zanonimizowanych (nie są one już danymi osobowymi).

Osoba, który przekazał swój materiał biologiczny bez danych identyfikujących nie jest dawcą w rozumieniu kodeksu o ile prowadzone badania nie mają na celu identyfikacji tej osoby,



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wzrostego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Białolekularnych
BBMRI-ERIC

3. DOPUSZCZALNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH I INNYCH DANYCH WRAŻLIWYCH DLA CELÓW BADAŃ NAUKOWYCH

Zasada:

Dane genetyczne i inne dane szczególnie wrażliwe, zgodnie z art. 89 ust. 1 RODO, mogą być przetwarzane przez biobanki dla celów badań naukowych tylko na podstawie wyjątków przewidzianych w przepisach prawa Unii Europejskiej lub prawa państwa członkowskiego. Takie przetwarzanie jest legalne, jeśli jest konieczne dla realizacji wyznaczonego celu naukowego, nie narusza istoty prawa do ochrony danych i przewiduje odpowiednie, konkretne środki ochrony podstawowych praw i interesów osoby, której dane dotyczą. W prawie polskim zasady ochrony praw pacjentów/dawców/uczestników badań wynikają wprost z Konstytucji Rzeczypospolitej Polskiej, RODO, z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, kodeksu cywilnego oraz kodeksu karnego.

Wyjaśnienie:

W sytuacji kiedy biobank jest podmiotem prowadzącym działalność leczniczą lub jednostką organizacyjną takiego podmiotu, a pozyskiwania materiału biologicznego do badań i danych osobowych następuje w związku ze świadczeniami zdrowotnymi (np. pochodzących z dokumentacji medycznej) zastosowanie do ochrony danych dawcy będą miały regulacje ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. W sytuacji zaś gdy biobank nie jest podmiotem prowadzącym działalność leczniczą, a pobranie danych osobowych nie następuje w związku z świadczeniem zdrowotnym wówczas podstawą prawną chroniącą osobę której dane dotyczą będzie bezpośrednio RODO.

Zalecenie:

Wszystkie biobanki przetwarzające dane szczególnie chronione dla celów naukowych powinny:

- 3.1) Zapewniać wysoki poziom ochrony bezpieczeństwa danych, w szczególności uniemożliwiającego dostęp do danych identyfikujących osobom postronnym.
- 3.2) Przetwarzać dane w sposób gwarantujący zachowanie prawa do prywatności wyrażone w art. 51 Konstytucji RP, art. 267 § 1 k.k., art. 24 § 1 k.c.
- 3.3) Gwarantować pacjentom/dawcom/ uczestnikom badań ich prawa określone w pkt. 7 niniejszego Kodeksu.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasadów Biomolekularnych
BBMRI-ERIC

3.4) Opisać w polityce bezpieczeństwa danych lub regulaminie ochrony danych zasady przetwarzania danych osobowych przez biobank powinny.

3.4.1) Wówczas, gdy zasady polityki bezpieczeństwa przetwarzania danych osobowych nie są tworzone na potrzeby biobanku, ale jednostki organizacyjnej, której jest on częścią, np. na poziomie uniwersytetu lub szpitala klinicznego, w pracach tych uczestniczyć powinien przedstawiciel biobanku, znający specyfikę przetwarzania danych osobowych w ramach biobankowania ludzkiego materiału biologicznego.

3.4.2) Administrator danych powinien sprawdzić procedury przetwarzania danych przez biobank oraz przeprowadzać ocenę ryzyka oraz skutków wszystkich projektowanych zmian w zakresie przetwarzania danych osobowych w obrębie biobanku (np. zmian w polityce ochrony danych, zmian oprogramowania itd.).

3.4.3) Administrator danych może je powierzyć innemu podmiotowi na podstawie umowy o powierzenie przetwarzania danych. Wówczas podmiot przetwarzający może wykorzystywać je jedynie zgodnie z treścią umowy, a po jej zakończeniu zobowiązany jest do zniszczenia danych lub ich zwrotu Administratorowi. O możliwości przekazania danych powinni być zawiadomione osoby, których dane osobowe są przetwarzane.

3.4.4) W sytuacji kiedy administrator prowadzi wspólne badania naukowe na danych osobowych z innym podmiotem, wówczas współadministrują oni dane osobowe.

4. ZASADY PRZETWARZANIA DANYCH DLA CELÓW NAUKOWYCH PRZEZ BIOBANKI NA PODSTAWIE ZGODY OSOBY, KTÓREJ DANE DOTYCZĄ

Zasada:

Podstawą dla przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą. Zgodnie z Rozporządzeniem zgodą może być oświadczenie osoby, której dane dotyczą, jej przedstawiciela lub wyraźnym działaniem potwierdzającym, iż przyzwala ona na przetwarzanie swoich danych osobowych (art. 4 pkt 11 RODO). Rozporządzenie nie określa formy zgody, wskazuje jedynie, że powinna być ona wyrażona dobrowolnie, świadomie i jednoznacznie.

8



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biotanków i Zasobów Biomolekularnych
BBMRI-ERIC

Jeżeli dawca/uczestnik badania/pacjent wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, to zgodnie z art. 7 ust 2 RODO „zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem”.

Wyrażenie zgody powinno zostać poprzedzone poinformowaniem osoby, której dane dotyczą o:

- 1) tożsamości i danych kontaktowych administratora oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych jego przedstawiciela;
- 2) danych kontaktowych inspektora ochrony danych;

Wyjaśnienie:

Inspektor ochrony danych osobowych może być powołany na poziomie jednostki, której biobank jest komórką organizacyjną. Dane kontaktowe powinny być tak ukształtowane, aby przekazywanie zgłoszeń o naruszeniach było możliwe i łatwe (np. podanie adresu e-mail inspektora ochrony danych).

- 3) tym, że dane są przetwarzane dla celów naukowych realizowanych przez dany biobank lub dla określonych badań naukowych, oraz że przetwarzanie takich danych następuje na podstawie zgody pacjenta/dawcy/uczestnika badań lub przepisów prawa;
- 4) przewidywanych odbiorcach danych osobowych lub o kategoriach odbiorców;
- 5) możliwości przekazania danych osobowych do państwa trzeciego (poza Unię Europejską) lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
- 6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

Wyjaśnienie:

Administrator powinien poinformować pacjenta/dawcę/uczestnika badania o okresie w jakim jego dane będą przetwarzane. Dopuszczalna jest sytuacja kiedy biobank określi, że dane będą przetwarzane przez czas trwania określonego projektu badawczego lub przez czas funkcjonowania biobanku.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

- 7) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- 8) prawie do cofnięcia zgody w dowolnym momencie, jednak bez możliwości wpływu na przetwarzanie, którego dokonano na podstawie zgody przed jej cofnięciem, oraz o niemożności usunięcia danych, jeśli zostały one już wykorzystane w badaniach naukowych;
- 9) prawie wniesienia skargi do organu nadzorczego wraz z podaniem danych kontaktowych do organu;
- 10) tym, że podanie danych osobowych nie jest wymogiem prawnym oraz, że osoba, której dane dotyczą, jest niezobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- 11) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacjach o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 1 i ust 2 RODO).

Wyjaśnienie:

Zgoda na przetwarzanie danych osobowych winna być wyraźna i odrębna od zgody na inne czynności, np. pobranie, przechowywanie i udostępnianie materiału biologicznego.

Badania naukowe, na które osoby wyrażają zgodę winny być zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Ponadto zgodnie z motywem 33 preambuły RODO „Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwi to zamierzony cel.”

Zalecenia:

4.1) Z uwagi na fakt, że biobanki przetwarzają dane szczególnie (dane wrażliwe), których przetwarzanie jest z zasady zabronione, za wyjątkiem przypadków wskazanych w art. 9 ust. 2, podstawą prawną takiego przetwarzania powinna być zgoda (art. 4 pkt 11 RODO) na przetwarzanie danych dla celu naukowego. Zgoda taka powinna spełniać warunki określone w pkt 4 niniejszego Kodeksu.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

4.2) Zaleca się zachowanie przy pobieraniu zgody formy pisemnej (zawierającej własnoręczny podpis osoby, której dane są przetwarzane), elektronicznej (zawierającej kwalifikowany podpis elektroniczny) lub dokumentowej (tj. utrwalonej w taki sposób, że możliwa jest identyfikacja osoby, która wyraziła zgodę np. nagranie głosu, email, wypełnienie formularza online) z uwagi na fakt, że na administratorze danych będzie ciążył obowiązek wykazania, że osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych.

4.3) Zgoda na przetwarzanie danych powinna być uzyskiwana niezależnie od zgody na czynności związane z materiałem biologicznym.

4.4) Od braku zgody na przetwarzanie danych nie można uzależniać współpracy z pacjentem/ dawcą/uczestnikiem badań jeśli zgoda na przetwarzanie danych nie jest niezbędna do pobrania, przechowywania i udostępniania materiału.

4.5) Zaleca się wypracowanie przez biobanki możliwości udzielenia zgody poziomowanej lub dynamicznej, która umożliwiałaby wyrażenie lub cofnięcie zgody na różne rodzaje badań naukowych.

4.6) Biobank powinien określić zakres i sposoby udostępniania danych pacjentów/dawców/uczestników badań oraz określić główne kategorie odbiorców, w tym wskazać wyraźnie czy dane będą przetwarzane przez podmioty komercyjne oraz w badaniach prowadzonych poza Polską.

4.7) Biobank powinien poinformować, że będzie udostępniał dane tylko do krajów, które mają odpowiedni poziom zabezpieczeń określony w prawie krajowym i prawie Unii Europejskiej, zgodnie z zasadami wyrażonymi w pkt 10 niniejszego kodeksu.

5. WTÓRNE PRZETWARZANIE DANYCH NAUKOWYCH BEZ KONIECZNOŚCI UZYSKIWANIA PONOWNEJ ZGODY

Zasada:

Zgodnie z motywem 50 preambuły RODO przetwarzanie dla celów badań naukowych uznaje się za zgodne z prawem i z pierwotnymi celami, jeśli zgoda na pierwotny cel była udzielona prawidłowo.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

Wyjaśnienie:

Jeżeli dane zostały zebrane np. dla celów medycznych za zgodą osoby, której dotyczą, lub na podstawie ustawy, mogą być one wtórnie przetwarzane dla celów naukowych. Jeżeli zaś nie było podstawy prawnej do przetwarzania danych w pierwotnym celu, przetwarzanie dla celów naukowych również nie będzie legalne.

Podobnie, jeśli uzyskano zgodę na przetwarzanie danych na potrzeby określonych badań naukowych, to wykorzystanie ich na potrzeby innych badań również będzie możliwe z zastrzeżeniem pkt 5.1.1) oraz pkt 5.1.1) niniejszego kodeksu.

Obowiązek informacyjny administratora danych w przypadku zmiany celu może być wyłączony (art. 14 RODO), jeśli udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. W takich przypadkach administrator ma obowiązek podjęcia środków mających na celu ochronę praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą.

Wyjaśnienie:

Może to dotyczyć sytuacji, w której biobank przetwarza dane osobowe dawców materiału biologicznego pobrane przed rozpoczęciem stosowania Rozporządzenia i ponowny kontakt z dawcami w celu uzupełnienia obowiązku informacyjnego byłby niemożliwy lub wymagałby niewspółmiernie dużego wysiłku (np. przy braku jakiegokolwiek aktualnej formy kontaktu, jak: adres korespondencyjny, numer telefonu, adres poczty elektronicznej).

Zalecenie:

5.1.1) Na wtórne wykorzystanie danych osobowych dla celów naukowych należy uzyskać zgodę dawcy, jeśli nie była ona w tym zakresie udzielona wcześniej z zastrzeżeniem p. 5.1.2.

5.1.2) Od wymogu uzyskania zgody na wtórne wykorzystanie danych osobowych dla celów naukowych można odstąpić tylko w sytuacji, kiedy uzyskanie zgody byłoby niemożliwe lub wymagałoby nadzwyczajnych środków. W takim przypadku zaleca się uzyskanie opinii właściwej komisji bioetycznej.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obszarze Infrastruktury Białkowej
Biobanków i Zasobów Białkowych
BBMRI-ERIC

5.2. Przetwarzanie danych pochodzących z dokumentacji medycznej

Zasady przechowywania dokumentacji medycznej wynikają z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Obowiązek przechowywania dokumentacji medycznej wynika z ustawy, zatem pacjentowi, nie przysługuje prawo do zniszczenia dokumentacji medycznej.

Wyjaśnienie:

Dane pochodzące z dokumentacji medycznej mogą być przez biobank przetwarzane dla celów naukowych, jeśli zostanie spełniony jeden z trzech warunków:

- 1) po uzyskaniu zgody osoby, której dane dotyczą;
- 2) w sytuacji, gdy uzyskanie zgody jest niemożliwe lub wiązałoby się z niewspółmiernie dużym wysiłkiem możliwe jest przekazanie danych niezbędnych do prowadzenia badań naukowych na podstawie umowy z podmiotem dysponującym dokumentacją medyczną; zgodnie z art. 24 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, możliwe jest zawarcie umowy o powierzenie przetwarzania danych w rozumieniu art. 28 RODO;
- 3) jeśli dokumentacja medyczna była prowadzona przez podmiot prowadzący działalność leczniczą, której jednostką organizacyjną jest biobank; w takiej sytuacji nie jest wymagana ponowna zgoda ani umowa. Dopuszczalne jest zatem przetwarzanie danych w ramach jednego administratora.

6. PRZETWARZANIE DANYCH NIE PODLEGAJĄCYCH REGULACJI ROZPORZĄDZENIA

6.1 Dane osób zmarłych (motyw 27 preambuły RODO).

Zgodnie z Rozporządzeniem ustawodawstwa krajowe mogą przewidywać system ochrony danych osobowych osób zmarłych. Taka częściowa regulacja związana z przetwarzaniem danych znajdujących się w dokumentacji medycznej znajduje się w art. 14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. W przypadku wykorzystywania danych osoby zmarłej, jej osobom bliskim może przysługiwać ochrona z tytułu naruszenia ich dobra osobistego w postaci kultu pamięci o osobie zmarłej (art. 24 kodeksu cywilnego) poprzez powództwo do sądu cywilnego.

Wyjaśnienie:

Na naruszenie art. 24 k.c. mógłby powoływać się np. bliski osoby, której dane osobowe zostały upublicznione w związku z badaniami nad chorobami niosącymi ryzyko stygmatyzacji społecznej, np. niektóre choroby dziedziczne.



BBMRI.pl
Biobanking and
BioMolecular resources
Research Infrastructure
Poland

Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

Zalecenie:

6.1.1) Dane osób zmarłych mogą być przekazane tylko do projektu naukowo-badawczego, który respektuje wysokie wymagania etyczne, w szczególności uzyskał pozytywną opinię komisji bioetycznej w sytuacjach wymaganych prawem. W sytuacjach wątpliwych zaleca się zawsze uzyskać opinię komisji bioetycznej.

6.1.2) Dane zmarłych pacjentów pochodzących z dokumentacji medycznej mogą być udostępniane dla celów naukowych biobankowi na podstawie umowy zawartej pomiędzy podmiotem prowadzącym działalność leczniczą a biobankiem. Przekazanie takich danych w drodze umowy możliwe jest w sytuacji udzielenia za życia zgody pacjenta lub jego pełnomocnika, albo wyrażonej po śmierci pacjenta zgody osoby bliskiej w rozumieniu art. 3 ust 1 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

6.1.3) Niedopuszczalne jest przekazanie dokumentacji medycznej do biobanków po wyrażeniu sprzeciwu lub odmowie udzielenia zgody przez pacjenta lub jego pełnomocnika. Po śmierci pacjenta niedopuszczalne przekazania dokumentacji medycznej do biobanku po wyrażeniu sprzeciwu, odmowie udzielenia osoby bliskiej pacjenta.

6.1.4) W sytuacji gdy nie zostaną spełnione wymagania z pkt 4.1.1. biobank może pobierać dane osób zmarłych o ile zostały one zanonimizowane.

6.1.5) Dane osób zmarłych powinny być przetwarzane z zachowaniem zasady minimalizacji danych oraz w sposób uniemożliwiający nieuprawnionym osobom dostęp do nich.

6.1.6) Dane osób zmarłych winny być przetwarzane w postaci pseudonimizowanej lub zanonimizowanej. Wyjątki od tej reguły wynikać mogą jedynie z ważnego interesu społecznego lub ważnego interesu osób bliskich (np. badanie przyczyny zgonu, który mógł mieć podłoże dziedziczne).

6.1.7) Publikacje wyników badań prowadzonych na danych osób zmarłych mogą podlegać publikacji w sposób uniemożliwiający identyfikację zmarłego. Publikacja danych zmarłego, która umożliwiałaby jego identyfikację powinna nastąpić jedynie w wyjątkowych sytuacjach na podstawie uprzedniej zgody wyrażonej za życia lub po uzyskaniu zgody osoby upoważnionej do



dostępu do dokumentacji medycznej, a w przypadku braku takiej osoby, po uzyskaniu zgody osoby bliskiej zmarłemu, uwzględniając zawsze ryzyko obciążenia emocjonalnego osób bliskich faktem upublicznienia informacji o zmarłym.

6.2 Dane anonimowe i zanonimizowane

Zasada:

Zgodnie z art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta dokumentacja medyczna zanonimizowana może być udostępniana uniwersytetom i instytutom badawczym. W takim zatem przypadku nie jest potrzebna zgoda pacjenta.

Wyjaśnienie:

Jeśli udostępniany ludzki materiał biologiczny pozwala na identyfikację osoby, to może być uznany za materiał zawierający dane osobowe, pomimo „pozornego” zakodowania danych zawierających np. imię i nazwisko.

W sytuacji kiedy podmiot biobankujący otrzymuje od innego podmiotu dane zakodowane w ten sposób, że są one dla niego nieidentyfikowalne, może być uznany za przetwarzający dane osobowe w rozumieniu RODO, jeśli w umowie o przekazanie danych nie został wyraźnie określony brak możliwości odkodowania danych na żądanie podmiotu biobankującego.

Zalecenie:

6.2.1) W przypadku, gdy planuje się poddać dane pacjenta/dawcy/uczestnika badania naukowego anonimizacji, to należy go poinformować o braku możliwości dochodzenia praw określonych w pkt. 7 niniejszego Kodeksu.

7.

8. ZASADY OCHRONY DANYCH PRZETWARZANYCH DLA CELÓW NAUKOWYCH

Zasada:

Rozporządzenie nakłada na podmioty przetwarzające dane obowiązek oceny ryzyka naruszenia ochrony danych osobowych oraz wdrożenia odpowiednich zasad i środków technicznych i organizacyjnych chroniących przed naruszeniem ochrony danych. Rodzaje zabezpieczeń pozostawione są decyzji i doświadczeniu osób zarządzających podmiotami, ale ogólne zasady i niektóre techniczne

15



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

reguły ochrony danych przechowywanych w biobankach winny być wspólne dla wszystkich podmiotów biobankujących.

7.1 Minimalizacja danych

Zasada:

Zgodnie z art. 89 ust. 1 RODO minimalizacja danych jest jedną z podstawowych zasad mających na celu zabezpieczenie praw osób, których dane są przetwarzane dla celów badań naukowych. Zasada minimalizacji zakłada, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne dla realizacji celów, w których są przetwarzane.

Wyjaśnienie:

Każdy biobank działający dla celów naukowych ma obowiązek wykazania, że dane, które przetwarza, powiązane są z zakresem jego działalności, a zatem z celami naukowymi.

7.2 Pseudonimizacja

Zasada:

Drugim podstawowym sposobem ochrony praw osób, których dane są przetwarzane dla celów badań naukowych, jest pseudonimizacja. Oznacza ona 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 i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Wyjaśnienie:

Dane pseudonimizowane to dane zakodowane w ten sposób, że możliwe jest ich ponowne powiązanie z danymi osobowymi identyfikującymi. Wszystkie zasady Rozporządzenia dotyczące przetwarzania danych osobowych dotyczą również przetwarzania danych pseudonimizowanych. Nie mają natomiast zastosowania do ochrony danych anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, nie można zidentyfikować.



7.3 Zalecenia techniczne służące zapewnieniu bezpieczeństwa danych przetwarzanych przez biobanki

Zalecenia:

7.3.1) biobank powinien przechowywać informacje dotyczące:

- daty pierwszego wprowadzenia danych do systemu,
- źródła danych, jeśli zbierane są dane, nie od osoby, której one dotyczą,
- wycofaniu zgody na przetwarzanie danych,
- prośby o anonimizację danych,

7.3.2) biobank powinien umożliwiać:

- jednoznaczną identyfikację osoby uzyskującej dostęp do systemu IT oraz przechowywanie tej informacji w logach,
- zapisywać czas modyfikacji oraz login użytkownika wprowadzającego dane do systemu,
- użytkownikowi na dostęp wynikający z uprawnień użytkownika tylko do przypisanych zasobów systemu IT.

7.3.3) W celu zapewnienia skuteczności stosowanych zabezpieczeń, zaleca się, aby hasło składało się ze znaków zawierających przynajmniej 3 z 4 grup znaków (duże/małe litery, cyfry, znaki specjalne);

7.3.4) Zasoby informatyczne biobanku (systemy, serwery, stacje robocze i urządzenia przenośne) powinny pracować w wydzielonej sieci;

7.3.5) Sieć biobanku powinna być odseparowana od sieci Internet poprzez zastosowanie urządzenia brzegowego typu Firewall;

7.3.6) W sieci biobanku powinien znajdować się aktywnie działający system typu IDS/IPS;

7.3.7) Systemy informatyczne oraz aktywne urządzenia infrastruktury informatycznej biobanki powinny być skonfigurowane tak, aby zapisywać logi (systemowe/dostępowe/dotyczące ruchu sieciowego),

7.3.8) Logi biobanku powinny być na bieżąco monitorowane,



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

7.3.9) Biobank powinien dokumentować przetwarzanie danych poprzez:

- instrukcje stanowiskowe dla pracownika na stanowisku, gdzie przetwarzane są dane osobowe,
- wykaz programów/systemów służących do przetwarzania danych wraz z opisem przepływu danych pomiędzy systemami,
- sporządzić wykaz pomieszczeń, w których przetwarzane są dane wraz z opisem zastosowanych środków technicznych i organizacyjnych celem należytego zabezpieczenia tych pomieszczeń,
- sporządzić procedury nadawania dostępu do zasobów informatycznych służących przetwarzaniu danych, w szczególności: zasady tworzenia kont użytkowników (siła hasła, czas ważności itp.), zasady uwierzytelniania i autoryzacji użytkowników, sposoby zarządzania kontami użytkowników,
- sporządzić procedury zarządzania, wykonywania, przechowywania i testowania kopii bezpieczeństwa,
- sporządzić procedury zarządzania hasłami kont administracyjnych,
- zabezpieczyć infrastruktury i zasoby informatyczne przed:
 - działaniem złośliwego oprogramowania,
 - nieautoryzowanym/nieuprawnionym dostępem,
 - podsłuchaniem transmisji,
 - kradzieżą danych.

7.3.10) Osoby odpowiedzialne powinny przeanalizować oprogramowanie służące do przetwarzania danych osobowych biobanku, następnie dokonać analizy ryzyka w zakresie istniejących i nowych zagrożeń oraz dobrać odpowiednie metody zabezpieczeń.



8. Prawa osób, których dane są przetwarzane dla celów badań naukowych przez biobanki

8.1 Prawo do wycofania zgody i zaprzestania przetwarzania danych

Zasada:

Zgodnie z art. 7 ust 1 RODO zgoda wyrażona przez osobę, której dane dotyczą może być wycofana w dowolnym czasie i bez żadnych negatywnych konsekwencji. Jednak zgodnie z art. 17 ust. 3 pkt d RODO prawo do żądania usunięcia danych może być wyłączone w przypadku przetwarzania danych osobowych dla celów naukowych, o ile jest prawdopodobne, że prawo to uniemożliwi lub poważnie utrudni realizację celów przetwarzania.

Wyjaśnienie:

Nie będzie możliwości żądania usunięcia danych, jeśli dane przetwarzane przez biobank zostały już przekazane do konkretnych badań naukowych i gdy badania z ich wykorzystaniem zostały zakończone, nawet wówczas kiedy osoba, która wyraziła zgodę, cofnie ją. W procesie uzyskiwania zgody należy o tym wyraźnie poinformować dawcę.

8.2 Prawo do sprostowania danych

Zgodnie z motywem 65 do RODO każda osoba fizyczna ma prawo do sprostowania swoich danych.

Wyjaśnienie:

Prawo do sprostowania danych przysługuje pacjentowi/dawcy/uczestnikowi badań, a zatem tylko on może tego żądać. Nie istnieje natomiast możliwość żądania aktualizacji danych przez biobank.

8.3 Prawo do informacji o przetwarzanych danych, w tym do do informacji o przypadkowo wykrytych istotnych informacjach dotyczących zdrowia

Zasada:

Zgodnie z art. 13 RODO pacjenci/dawcy/uczestnicy badań mają prawo domagać się i otrzymywać informacje o swoich danych oraz ich wykorzystaniu.

Zgodnie z art. art. 9 ust 1 ustawy o prawach pacjenta, pacjent ma prawo do uzyskania wszystkich informacji o swoim stanie zdrowia.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

Wyjaśnienie:

Prawo do informacji odnosi się zatem do wszystkich informacji dotyczących przetwarzania danych. Obejmuje ono również prawo do wiedzy o przypadkowo wykrytych istotnych informacjach mających znaczenie dla zdrowia pacjenta/dawcy/uczestnika badań.

Zalecenia:

8.3.1) Pacjent/dawca/uczestnik badań powinien być poinformowany o zasadach przekazywania przez biobank informacji o przypadkowo wykrytych znaleziskach, istotnych dla zdrowia osoby, której dane dotyczą

8.3.2) Każdy badacz, który uzyska informację istotną dla zdrowia pacjenta/dawcy/uczestnika badań, nawet przypadkowo wykrytą, powinien poinformować o tym pacjenta/dawcę/uczestnika badań lub podmiot upoważniony do kontaktu z pacjentem. Dotyczy to szczególnie lekarza, który przekazując informację winien również przestrzegać reguł zachowania tajemnicy lekarskiej.

8.3.3) Zalecenia 8.1 i 8.2 nie dotyczą sytuacji, w których pacjent/dawca/uczestnik badań złożył oświadczenie o skorzystaniu z prawa do niewiedzy.

8.3.4) Biobank powinien zobowiązać podmiot, któremu udostępni dane osobowe pacjentów/dawców/uczestników badań do przekazania do biobanku informacji przypadkowo wykrytych istotnych dla zdrowia.

8.3.5) Ocena istotności dla zdrowia pozyskanych informacji określana jest przez podmiot dokonujący odkryć z uwzględnieniem ciężaru choroby, możliwości prewencji, leczenia lub modyfikacji przebiegu choroby.

8.4 Prawo do informacji o skutkach anonimizacji danych

Zasada:

Dane osobowe przekształcone w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować, czyli zaninimizowane w rozumiane pkt 2 pdpkt 8 niniejszego Kodeksu i motywu (26) preambuły RODO, nie podlegają reżimowi prawnemu Rozporządzenia.

Zalecenie:



8.4.1) Każdy pacjent/dawca/uczestnik badań powinien być poinformowany, że w przypadku anonimizacji danych niemożliwe będzie: przekazanie mu informacji o przetwarzanych danych, wycofanie zgody na przetwarzanie danych, sprostowanie i uzupełnienie danych.

8.5 Prawa osób niezdolnych do wyrażenia zgody

Zalecenie:

8.5.1) W przypadku osób niezdolnych do wyrażania zgody, w sytuacji gdy osoby te uzyskają lub odzyskują zdolność do wyrażenia zgody, należy podjąć próbę uzyskania od tych osób zgody na dalsze przetwarzanie ich danych osobowych.

9. Administrator danych i inspektor danych

Zasada:

Za przestrzeganie zasad przetwarzania danych osobowych zgodnie z art. 5 ust 2 RODO odpowiada administrator. To on ma obowiązek wykazania, że przetwarzanie danych jest prowadzone w sposób prawnie dozwolony. Jest on zobowiązany do oceny skutków w zakresie ochrony danych, uwzględnienie ochrony danych osobowych w fazie projektowania, notyfikacji naruszeń oraz rejestracji czynności przetwarzania.

Obowiązek rejestracji czynności przetwarzania wyłączony jest wobec przedsiębiorców zatrudniających mniej niż 250 pracowników, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych.

Wyjaśnienie:

W przypadku biobanków należy wskazać, że jeśli nie mają one odrębnej osobowości prawnej, a są częścią organizacyjną uczelni, szpitala czy spółki, limit 250 osób będzie odnosił się do wszystkich pracowników tego pomiotu, a nie tylko do pracowników biobanku.

Obowiązek powołania inspektora ochrony danych następuje m. in. wtedy, gdy podmiotem przetwarzającym jest organ lub podmiot publiczny, a także gdy główna działalność gospodarcza podmiotu polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych. W rozumieniu prawa polskiego będą to uczelnie państwowe, szpitale i instytuty badawcze (podmioty wymienione w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych). Do obowiązków



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

inspektora danych należą m.in.: informowanie o obowiązkach wynikających z rozporządzenia, monitorowanie przestrzegania prawa związanego z przetwarzaniem danych osobowych oraz szkoleń w tym zakresie, współpracy z organem nadzorczym.

Inspektor nawet wówczas kiedy jest członkiem personelu administratora lub podmiotu przetwarzającego ma pozycję niezależną i nie podlega administratorowi danych.

Wyjaśnienie:

Biobanki lub podmioty, które są częścią organizacyjną większych podmiotów (np. uczelni, szpitala), będą miały obowiązek powołania inspektora ochrony danych.

Zalecenie:

9.1) Administrator danych w jednostce posiadającej w swoich strukturach organizacyjnych biobank działający dla celów naukowych, powinien na inspektora ochrony danych powołać osobę posiadającą fachową wiedzę również w zakresie przetwarzania danych osobowych przez biobanki.

10. OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

Zasada:

Zgodnie z art. 4 pkt 12 RODO, naruszenie ochrony danych osobowych oznacza 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.

Co do zasady, Grupa Robocza art. 29 wyróżnia trzy najszerzej znane kategorie naruszenia danych osobowych:

- 1) naruszenie poufności danych osobowych – polegające na nieuprawnionym lub przypadkowym ujawnieniu danych osobowych lub umożliwieniu dostępu do nich;
- 2) naruszenie dostępności danych osobowych – polegające na wystąpieniu nieuprawnionej lub przypadkowej utraty dostępu do danych osobowych lub ich zniszczenia;



3) naruszenie integralności danych osobowych – polegające na nieuprawnionym lub przypadkowej modyfikacji danych osobowych.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zalecenia:

10.1) Inspektor ochrony danych biobanku zgłasza naruszenia ochrony danych osobowych do administratora danych, który ma obowiązek prowadzenia rejestru naruszeń.

10.2) Administrator powinien określić sposób zgłoszenia naruszeń ochrony danych osobowych przez swoich pracowników, w tym szczególnie pracowników biobanku.

10.3) Administrator ma obowiązek zgłoszenia naruszeń w ciągu 72h od powzięcia informacji o naruszeniu, jeśli skutkowało ono ryzykiem naruszenia praw lub wolności osób, których dane są przetwarzane.

10.4) Administrator powinien niezwłocznie powiadomić osoby, których dane są przetwarzane, w sytuacji gdy nastąpiło naruszenie ochrony danych osobowych.

10.5) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

11. TRANSGRANICZNA WYMIANA DANYCH

Zasada:

Transgraniczna wymiana danych osobowych oparta jest na dwóch odrębnych reżimach prawnych. Pierwszy znajduje zastosowanie do wymiany danych osobowych pomiędzy państwami należącymi do Europejskiego Obszaru Gospodarczego/Unii Europejskiej, a drugi pomiędzy państwami należącym do EOG/UE a państwem nienależącym do EOG/UE (państwo trzecie) lub organizacją międzynarodową.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Biomolekularnych
BBMRI-ERIC

W pierwszym reżimie przepływ danych osobowych odbywa się swobodnie pomiędzy państwami członkowskimi, na ogólnych zasadach określonych w Rozporządzeniu.

Natomiast drugi reżim, zgodnie z art. 44 RODO wymaga aby przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następować tylko, gdy administrator i podmiot przetwarzający spełnią warunki określone w Rozdziale V RODO.

Na mocy art. 45 ust. 3 RODO przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, a takie przekazanie nie wymaga specjalnego zezwolenia.

W razie braku decyzji wydanej zgodnie z art. 45 ust. 3, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

Zalecenia:

11.1) Biobank może przekazać zgromadzone dane osobowe tylko do takiego kraju trzeciego lub organizacji międzynarodowej, które zapewniają należyty stopień ochrony danych stwierdzony przez Komisję Europejską.

11.2) Przekazanie danych możliwe jest jedynie przez umowę zawartą pomiędzy biobankiem a podmiotem otrzymującym próbki, z której wynikają obowiązki stron w zakresie ochrony danych osobowych.

11.3) Umowa przekazania danych powinna zawsze określać poziom ochrony danych (np. pseudonimizowane, anonimizowane).

12. Przyjęcie Kodeksu

Każdy podmiot prowadzący biobanki dla celów naukowych mających siedzibę w Rzeczypospolitej Polskiej może przystąpić do Kodeksu dobrowolnie.



Projekt finansowany ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego

Utworzenie sieci biobanków w Polsce
w obrębie Infrastruktury Badawczej
Biobanków i Zasobów Białolekularnych
BBMRI-ERIC