Zarządzenie nr 17/2024
z dnia 5 września 2024 r.

Dyrektora Instytutu Biologii Medycznej Polskiej Akademii Nauk w sprawie wprowadzenia w życie „Polityki Ochrony Danych Osobowych" w Instytucie Biologii Medycznej Polskiej Akademii Nauk

§1

Wprowadzam do realizacji dokument „Polityka ochrony danych osobowych" w Instytucie Biologii Medycznej Polskiej Akademii Nauk - dotyczący zasad przetwarzania danych osobowych w Instytucie Biologii Medycznej PAN, stanowiący załącznik do niniejszego zarządzenia.

§2

Przestrzeganie przepisów wprowadzonej Polityki oraz dokumentów towarzyszących obowiązuje wszystkich pracowników i stypendystów Instytutu oraz współpracowników wykonujących zadania na jego rzecz na podstawie umów cywilnoprawnych lub w inny sposób, a w szczególności osoby przetwarzające dane osobowe w zbiorach, których administratorem jest Instytut Biologii Medycznej PAN.

§3

Zobowiązuję Kierowników pracowni i laboratoriów oraz pozostałych działów organizacyjnych Instytutu do realizacji i nadzorowania wykonywania postanowień zawartych w Polityce.

§4

Nadzór nad realizacją zarządzenia powierzam Inspektorowi Ochrony Danych w Instytucie Biologii Medycznej PAN, na którego wskazana została Pani Natalia Jaros.

§5

Traci moc Zarządzenie nr 17/2016 z dnia 06 grudnia 2016 roku Dyrektora Instytutu Biologii Medycznej PAN w sprawie wprowadzenia w życie „Polityki Bezpieczeństwa w Zakresie Ochrony Danych Osobowych Instytutu Biologii Medycznej PAN wraz z Instrukcją Zarządzania Systemem Informatycznym".

§6

Zarządzenie wchodzi w życie z dniem podpisania.

Do wiadomości:
- wszystkie komórki organizacyjne IBM PAN

DYREKTOR
Instytutu Biologii Medycznej
Polskiej Akademii Nauk

Prof. dr hab. Jarosław Dziadek
(2)

Załącznik nr 1 do Zarządzenia Nr 17/2024 z dnia 5.09.2024
Dyrektora Instytutu Biologii Medycznej PAN

INSTYTUT

BiolMed

INSTYTUT BIOLOGII MEDYCZNEJ
POLSKIEJ AKADEMII NAUK
93-232 Łódź, ul. Lodowa 106

POLITYKA OCHRONY DANYCH OSOBOWYCH INSTYTUTU BIOLOGII MEDYCZNEJ POLSKIEJ AKADEMII NAUK

§ 1
Cel i zakres Polityki

1. Niniejsza Polityka i dokumenty jej towarzyszące opisują reguły i procedury zapewnienia bezpieczeństwa danych osobowych w Instytucie
2. Zakres obowiązywania Polityki obejmuje:
   a) wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne (papierowe) dokumenty, w których przetwarzane są lub będą dane osobowe;
   b) dane podmiotów danych lub informacje będące własnością Instytutu, partnerów, konsorcjantów lub osób korzystających z usług Instytutu;
   c) wszystkie typy nośników, na których są lub będą znajdować się dane osobowe, zarówno tradycyjnej, jak i elektroniczne;
   d) wszystkie lokalizacje- pomieszczenia i części pomieszczeń, w których są lub będą przetwarzane dane osobowe;
3. Politykę Ochrony Danych Osobowych zobowiązana jest stosować każda osoba wchodząca w skład struktury organizacyjnej Instytutu lub przetwarzająca dane osobowe ze względu na współpracę z Instytutem, niezależnie od rodzaju stosunku prawnego łączącego ją z Instytutem, która przetwarza dane osobowe pochodzące od Instytutu.

§ 2
Pojęcia

Ilekroć w niniejszym dokumencie używane są poniższe pojęcia ich rozumienie zgodne jest z podaną definicją oraz - jeśli dotyczy - zakresem zastosowania wynikającym z RODO:

1. **Instytut (Administrator) -** Instytut Biologii Medycznej Polskiej Akademii Nauk z siedzibą w Łodzi wykonujący zadania administratora danych osobowych w rozumieniu i zgodnie z RODO;

2. **Dane osobowe** - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
3. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
4. **Organ nadzorczy** - organ właściwy w sprawach ochrony danych osobowych;
5. **Inspektor** - wyznaczona przez Administratora osoba odpowiedzialna za koordynowanie przestrzegania obowiązków spoczywających na Administratorze, a wynikających z przepisów dotyczących ochrony danych osobowych i niniejszej Polityki;
6. **Dyrektor** - osoba zatrudniona na stanowisku Dyrektora Instytutu lub pełniąca obowiązki Dyrektora na czas jego zastępstwa lub powołania;
7. **Właściciel danych** - kierownicy działów i zespołów Instytutu, którzy koordynują ich prace oraz samodzielne stanowiska, które odpowiadają za przetwarzanie danych w ramach własnej jednostki organizacyjnej;
8. **Użytkownik** - osoba upoważniona przez Administratora do przetwarzania danych osobowych, w szczególności pracownicy Administratora;
9. **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na Danych osobowych 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;
10. **Podmiot przetwarzający** - osoba fizyczna lub prawna lub inny podmiot, który przetwarza Dane osobowe w imieniu Administratora;
11. **Pracownik** - osoba współpracująca z Instytutem, niezależnie od formy współpracy, w tym stażyści, stypendyści, doktoranci i osoby zaangażowane w innej formie, w tym umów cywilnoprawnych przez cały okres współpracy;
12. **System informatyczny** - sprzęt komputerowy, oprogramowanie i dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w Instytucie, w szczególności w celu przetwarzania danych.

§ 3
Zasady przetwarzania Danych osobowych

1. Dane osobowe w Instytucie przetwarzane są w sposób zapewniający przestrzeganie poniższych zasad:
   a) **zgodność z prawem, przejrzystość, rzetelność** - zgodnie z normami prawa powszechnie obowiązującego i wewnętrznymi regulacjami, rzetelnie, starannie i w sposób zrozumiały i łatwo dostępny dla osoby, której dane dotyczą, w połączeniu z jasną komunikacją;
   b) **ograniczenie celu** - Dane osobowe zbierane są wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach, i przetwarzane wyłącznie w sposób zgodny z tymi celami i do nich ograniczony;
   c) **minimalizacja danych** - Dane osobowe przetwarzane są w zakresie adekwatnym i możliwie najwęższym w stosunku do realizacji celów, dla jakich zostały zebrane;
   d) **prawidłowość** - podczas przyjmowania i przetwarzania danych Użytkownik dba o ich prawidłowość (poprawność) i w razie potrzeby aktualizuje zebrane dane w sposób umożliwiający prawidłowa identyfikację osób, których dane dotyczą;

e) **ograniczenie przechowywania (retencja)** - Dane osobowe przechowywane są przez czas niezbędny i nie dłuższy niż wymaga tego realizacja celu dla jakiego zostały zebrane, a po tym czasie są skutecznie usuwane lub trwale anonimizowane;

f) **bezpieczeństwo, integralność i poufność** - Dane osobowe przetwarzane są w sposób zapewniający ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem lub przypadkową utratą, ujawnieniem, zniszczeniem lub uszkodzeniem w części lub całości;

g) **rozliczalność** - kontrola nad Danymi osobowymi pozwala zidentyfikować kto i w jakim czasie miał do nich dostęp i jakich dokonywał czynności przetwarzania;

h) **uwzględnienie bezpieczeństwa w każdej fazie procesu** - bezpieczeństwo danych osobowych jest naczelną i domyślną zasadą projektowania i realizacji procesów i systemów, w których przetwarzane są Dane osobowe.

2. Do przetwarzania danych mogą przystąpić i być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.

§ 4
Obowiązki i zadania Administratora

1. Administrator danych wyznacza cele przetwarzania i sposoby zabezpieczenia Danych osobowych, w tym środki techniczne i organizacyjne zapewniające ochronę, odpowiednie do zagrożeń oraz kategorii Danych osobowych objętych ochroną.
2. Administrator zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do Instytutu oraz komu są przekazywane.
3. Administrator decyduje o zakresie udzielanych upoważnień do przetwarzania i powierzeniu Danych osobowych podmiotom przetwarzającym.
4. Po zakończeniu okresu upoważnienia do przetwarzania danych Administrator Danych dokonuje adnotacji na upoważnieniu, stosownej zmiany w zakresie dostępu do zasobów tradycyjnych i elektronicznych or9fbv1qwinformuje osobę upoważnioną o obowiązku zaprzestania przetwarzania.

§ 5
Obowiązki i zadania Inspektora

1. Do zadań Inspektora należy:
   a) przygotowanie, audyt, monitorowanie przestrzegania i aktualności dokumentacji bezpieczeństwa Danych osobowych obowiązujących u Administratora oraz przekazywanie rekomendacji;
   b) koordynacja i wsparcie procesów przetwarzania Danych osobowych w Instytucie przez Właścicieli danych i Użytkowników, w tym wsparcie w zakresie prowadzenia rejestrów czynności przetwarzania oraz upoważnień;
   c) prowadzenie rejestru umów powierzenia przetwarzania oraz rejestru kategorii czynności przetwarzania;
   d) podejmowanie działań zwiększających świadomość Użytkowników;
   e) udzielanie informacji, porad i konsultacji, w tym wsparcie w kontakcie z osobami, których dane dotyczą i Organem nadzorczym;
   f) konsultacji odpowiednich działań korekcyjnych w celu właściwego zabezpieczenia danych.
2. Inspektor prowadzi pełną dokumentację zapewniającą zgodność procesu przetwarzania danych z wymogami bezpieczeństwa i przepisami prawa.

3. Inspektor jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych oraz przegląd dokumentacji ochrony danych osobowych, co najmniej raz do roku.

§ 6
Obowiązki Właścicieli danych

1. Właściciel danych zobowiązany jest:
   a) prowadzić wspólnie z Inspektorem rejestr czynności przetwarzania dla procesów na Danych osobowych, których jest właścicielem;
   b) realizować obowiązek informacyjny w imieniu Instytutu podczas pozyskiwania Danych osobowych;
   c) nadzorować proces przetwarzania Danych osobowych oraz przestrzegania wymagań wynikających z Polityki, w szczególności przez podległych pracowników;
   d) w przypadku zlecenia przetwarzania Danych osobowych podmiotom zewnętrznym informować o potrzebie zawarcia umowy powierzenia przetwarzania Danych osobowych Inspektora;
   e) przestrzegać zasad retencji danych, w szczególności usuwać lub anonimizować Dane osobowe, których przetwarzanie przestało być konieczne ze względu na cel i podstawę przetwarzania.
2. W przypadku konieczności zawarcia umowy powierzenia odmiennej od wzoru stanowiącego załącznik do Polityki, Właściciel danych skonsultuje uprzednio zawarcie takiej umowy z Inspektorem.

§ 7
Obowiązki i zadania Użytkownika

1. Wszyscy Użytkownicy zobowiązani są do:
   a) przetwarzania Danych osobowych zgodnie z zasadami, o których mowa w § 3 Polityki;
   b) przetwarzania Danych osobowych wyłącznie w zakresie udzielonego przez Administratora upoważnienia;
   c) przestrzegania Polityki, procedur i wykonywania poleceń Administratora, Inspektora lub Właściciela danych związanych z Danymi osobowymi;
   d) reagowania w przypadku stwierdzenia naruszenia ochrony Danych osobowych lub ryzyka wystąpienia takiego naruszenia oraz zgłaszania naruszeń i wątpliwości do Administratora i Inspektora;
   e) podejmowania działań niezbędnych w celu ograniczenia ryzyka powstania zagrożeń oraz minimalizacja skutków wystąpienia naruszeń;
   f) zgłaszania żądania realizacji praw od osób których dane dotyczą do Inspektora;
   g) zgłaszania Administratorowi niezbędnych potrzeb mających na celu przetwarzanie danych w sposób bezpieczny.
2. Każdy Użytkownik przed dopuszczeniem do pracy z Danymi osobowymi powinna zostać przeszkolony lub zapoznany z zasadami przetwarzania przez Inspektora.
3. Każdy Użytkownik zobowiązany jest podnosić swoją wiedzę w zakresie bezpiecznego przetwarzania Danych osobowych, w szczególności poprzez zapoznanie z komunikatami Inspektora.
4. W razie powzięcia wątpliwości co do zakresu upoważnienia do przetwarzania lub innych zagadnień związanych z ochroną Danych osobowych Użytkownik zobowiązany jest niezwłocznie skonsultować się z Inspektorem.

5. Obowiązki odnoszące się do Użytkownika dotyczą wszystkich Pracowników Instytutu.

§ 8
Zasady codziennej pracy z Danymi osobowymi

1. Codzienne, podstawowe czynności wykonywane przez wszystkich Pracowników wpływają na poziom bezpieczeństwa danych Instytutu i wymagają należytej staranności, zachowania poufności i dbałości o bezpieczeństwo.
2. Praca z Danych osobowych w formie tradycyjnej i elektronicznej oraz przebywanie w obszarach przetwarzania danych powinno być zgodne z zasadami przetwarzania danych określonymi w §3 oraz Regulaminami stanowiącymi załącznik do Polityki i innymi wytycznymi Administratora i Inspektora.
3. Dokumenty, niezależnie od formy, powinny być odpowiednio chronione podczas korzystania z nich i przechowywania. W szczególności należy zapobiegać dostępowi do Danych osobowych osób nieuprawnionych, w tym innych pracowników nieposiadających stosownego upoważnienia.
4. Po zakończeniu pracy z Danymi osobowymi lub współpracy z Instytutem każdy Użytkownik zobowiązany jest do zwrotu powierzonych Danych osobowych i zasobów elektronicznych, w tym sprzętu należącego do Instytutu, nie później niż w dniu zakończenia pracy z Danymi osobowymi lub współpracy z Instytutem.

§ 9
Zasady retencji danych

1. Dla każdego procesu przetwarzania Danych osobowych, Właściciel danych w porozumieniu z Inspektorem określa czas, przez który Dane osobowe, przetwarzane w ramach tego procesu, będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania okresu retencji Danych osobowych.
2. Po zakończeniu przetwarzania, Dane osobowe powinny zostać usunięte w sposób uniemożliwiający ich odtworzenie, zanonimizowane lub przekazane podmiotowi uprawnionemu ustawowo do przejęcia ich od Administratora zgodnie z kategorią Danych osobowych.
3. Kryteria ustalania okresu niezbędności przetwarzania danych osobowych mogą wynikać z następujących przesłanek:
   a) cel, w którym dane są przetwarzane,
   b) podstawa prawna legalizująca przetwarzanie danych w tym celu.

§ 10
Zasady realizacji praw osób, których dane dotyczą

1. Każda osoba, której dane osobowe są przetwarzane przez Instytut, ma prawo do:
   a) otrzymania w zwięzłej, przejrzystej, zrozumiałej formie, wszelkich informacji, o jej Danych osobowych przetwarzanych przez Instytut;
   b) sprostowania Danych osobowych, ich poprawienia i uzupełnienia;
   c) żądania usunięcia lub ograniczenia przetwarzania jej Danych osobowych, o ile spełnia prawnie określone przesłanki;
   d) wniesienia sprzeciwu w przypadku, jeśli jej Dane osobowe miałyby podlegać zautomatyzowanym przetwarzaniu do celu podejmowania decyzji;
   e) przenoszenia danych.

2. Realizacja praw osób, których dane dotyczą poprzedzona jest obligatoryjną weryfikacją tożsamości wnioskodawcy i konsultacją z Inspektorem.
3. Udostępnienie informacji podmiotowi danych jest zasadniczo bezpłatne, jednak, jeżeli Instytut uzna, że żądania są ewidentnie nieuzasadnione lub nadmierne, może pobrać opłatę, uwzględniając koszty administracyjne udzielenia informacji, prowadzenia komunikacji lub podjęcia żądania działań, albo odmówić podjęcia działań w związku z żądaniem.

§ 11
Instrukcja postępowania z incydentami

1. Do typowych zagrożeń bezpieczeństwa Danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyniesienie lub wyciek informacji lub nośników danych, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
2. Naruszeniem bezpieczeństwa Danych osobowych jest każde niezgodne z prawem, w tym przypadkowe zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Każdy pracownik Instytutu, który stwierdzi zaistnienie zagrożenia bezpieczeństwa Danych osobowych lub fakt naruszenia ochrony Danych osobowych zobowiązany jest do podjęcia czynności niezbędnych do powstrzymania skutków naruszenia, zabezpieczenia dowodów umożliwiających ustalenie przyczyn oraz skutków zagrożenia, oraz niezwłocznego powiadomienia Administratora i Inspektora.
4. W przypadku stwierdzenia naruszenia bezpieczeństwa Danych osobowych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia. W przypadku zasobów elektronicznych dodatkowo należy niezwłocznie odłączyć je od sieci.
5. Po ustaleniu wszelkich okoliczności związanych z zaistniałym naruszeniem Inspektor dokumentuje zaistniały przypadek naruszenia oraz wspólnie z Administratorem lub wyznaczoną przez niego osobą decyduje o kwalifikacji poziomu naruszenia i rodzącego ryzyko dla praw i wolności podmiotu danych oraz ustala konieczność dalszego postępowania.

§ 12
Postanowienia końcowe

1. W sprawach nieuregulowanych w Polityce zastosowanie znajdują przepisy prawa powszechnie obowiązującego, przede wszystkim RODO, Kodeksu pracy i ustawy o ochronie danych osobowych.
2. Naruszenie zasad opisanych w Polityce i Regulaminach może stanowić naruszenie obowiązków pracowniczych, w tym prowadzące do zastosowania sankcji dyscyplinujących z rozwiązaniem umowy o pracę z winy pracownika włącznie.
3. Integralną częścią Polityki stanowią jej załącznik:
   d) **Załącznik nr 1**- Upoważnienie do przetwarzania danych osobowych- wzór
   e) **Załącznik nr 2** - Rejestr upoważnień - wzór

f) **Załącznik nr 3**- Umowa powierzenia- wzór
g) **Załącznik nr 4** - Rejestr Umów powierzenia
h) **Załącznik nr 5** - Rejestr czynności przetwarzania - wzór
i) **Załącznik nr 6** - Regulamin bezpieczeństwa przetwarzania danych osobowych w pomieszczeniach Instytutu
j) **Załącznik nr 7** - Regulamin Korzystania z zasobów elektronicznych Instytutu

4. W sprawach nieuregulowanych w załącznikach stosuje się zapisy Polityki.