

Zarządzenie nr 52/2020
Rektora Uniwersytetu Medycznego w Białymstoku
z dnia 5.06.2020r.

w sprawie wprowadzenia zmian do Zarządzenia nr 22/2019 z dnia 5.03.2019 r. w sprawie zasad przeprowadzania oceny skutków dla ochrony danych osobowych w Uniwersytecie Medycznym w Białymstoku

Na podstawie art. 35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016) zwanego dalej „RODO” w powiązaniu z Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z dnia 17.06.2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony zarządzam, co następuje:

§1

W Zarządzeniu nr 22/2019 Rektora Uniwersytetu Medycznego w Białymstoku z dnia 5.03.2019 r. w sprawie zasad przeprowadzania oceny skutków dla ochrony danych osobowych w Uniwersytecie Medycznym w Białymstoku wprowadza się następujące zmiany:

1. W §3 zmienia się treść ust. 2 nadając mu nowe brzmienie:
„2. Wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony ogłoszony w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17.06.2019 r., stanowi załącznik nr 3 do niniejszego zarządzenia.”
2. Zmienia się treść załącznika nr 2 i załącznika nr 3 nadając im nowe brzmienie jak w załącznikach do niniejszego Zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

prof. dr hab. Adam Krętowski

Wybrane rodzaje operacji przetwarzania, wymagające oceny skutków, które mogą występować w Uczelni

Poniższy wykaz zawiera przykładowe rodzaje operacji wymagających przeprowadzenia oceny skutków, które mogą występować w Uniwersytecie Medycznym w Białymstoku.

- 1) Przetwarzanie danych genetycznych, laboratoria oferujące diagnostykę genetyczną, diagnoza medyczna, testy DNA, Badania medyczne,
- 2) Przetwarzanie szczególnych kategorii danych osobowych, badania kliniczne, podmioty pobierające materiał genetyczny do badań, dane dotyczące zdrowia pacjentów/klientów,
- 3) Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych:
 - a) specjalistyczne porady i konsultacje medyczne, badania kliniczne o zasięgu międzynarodowym, w tym konsultacje telemedyczne z ośrodkami spoza UE, przekazywanie osobowych danych medycznych o zasięgu międzynarodowym,
 - b) aplikacje z funkcjami komunikowania się i oprogramowaniem umożliwiającym wymianę informacji z najbliższym otoczeniem oraz zdalnie poprzez sieć telekomunikacyjną np. stosowanie urządzeń wyposażonych w różnego rodzaju interfejsy (głośnik, mikrofon, kamera) oraz oprogramowanie i system łączności umożliwiające przekazywanie danych poprzez sieci telekomunikacyjne,
 - c) zastosowanie komunikacji między urządzeniami (Internet rzeczy – np. beacons, drony) w przestrzeni publicznej i w miejscach użyteczności publicznej np. systemy stosowane do analizy i przekazywania danych dostawcom usługi przy użyciu aplikacji mobilnych z urządzeń przenośnych typu: smartwatch, inteligentne opaski, beacons itp. analizujące i przekazujące dane dostawcom przy użyciu aplikacji mobilnych
- 4) Systematyczne monitorowanie na dużą skalę:
 - a) monitoring systemów informatycznych poczty elektronicznej, używanego oprogramowania, kart dostępowych, systemy monitorowania czasu pracy pracowników oraz przepływu informacji w wykorzystywanych przez nich narzędziach,
 - b) przetwarzanie informacji pozyskiwanych przez Internet rzeczy (opaski medyczne, smartwatche itp.) oraz ich przesyłanie w sieci przy użyciu urządzeń mobilnych typu smartfon czy tablet, gromadzenie i wykorzystywanie danych przez aplikacje instalowane w urządzeniach mobilnych w tym w urządzeniach połączonych z osobą pozyskującą dane,

Wykaz rodzajów operacji przetwarzania danych osobowych wymagających
oceny skutków przetwarzania dla ich ochrony

I. Rodzaje/kryteria dla operacji przetwarzania, dla których wymagane jest przeprowadzenie oceny	II. Potencjalne obszary wystąpienia/ istniejące obszary zastosowań	III. Przykłady operacji/zakresu danych/okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania
1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych	Media społecznościowe, firmy marketingowe, firmy headhunterskie	Profilowanie użytkowników portali społecznościowych i innych aplikacji w celu wysyłania informacji handlowej
	Banki, inne instytucje finansowe upoważnione do udzielania kredytów, instytucje pożyczkowe w procesie oceny zdolności kredytowej	Ocena zdolności kredytowej, przy użyciu algorytmów sztucznej inteligencji, objęta obowiązkiem zachowania tajemnicy i żądanie ujawnienia danych niemających bezpośredniego związku z oceną zdolności kredytowej
	Firmy ubezpieczeniowe - oferowanie zniżek związanych ze stylem życia (papierosy, alkohol, sporty ekstremalne, styl jazdy samochodem)	Ocena stylu życia, odżywiania się, jazdy, sposobu spędzania czasu itp. osób fizycznych w celu np. podwyższenia im ceny składki ubezpieczeniowej, na podstawie tej oceny, nazywana ogólnie optymalizacją składki ubezpieczeniowej
	Firmy ubezpieczeniowe - np. korzystniejsze oferty ubezpieczeniowe lub kredytowe dla pracowników określonych grup, np. administracji publicznej, nauczycieli	Profilowanie pośrednie (ocena osoby na podstawie przynależności do określonej grupy)
2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki	Drogi objęte odcinkowym pomiarem prędkości (system gromadzi informacje nie tylko o pojazdach naruszających przepisy, ale o wszystkich pojazdach pojawiających się w kontrolowanym obszarze), odcinki dróg wyposażone w system elektronicznego poboru opłat viaTOLL	Systemy monitoringu wykorzystywane do zarządzania ruchem, umożliwiające szczegółowy nadzór nad kierowcą oraz jego zachowaniem na drodze, w szczególności systemy pozwalające na automatyczną identyfikację pojazdów Systemy automatycznego pobierania opłat za wjazd
	Sklepy internetowe oferujące ceny promocyjne dla określonych grup klientów. Firmy obsługujące programy lojalnościowe (wspólnoty zakupowe)	Systemy profilowania klientów pod kątem zidentyfikowania preferencji zakupowych, automatycznego ustalania cen promocyjnych w oparciu o profil
	Programy marketingowe zawierające elementy profilowania osób	Monitorowanie zakupów i preferencji zakupowych (np. alkohol, słodycze)
3. Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie	Środki komunikacji miejskiej, miasta oferujące systemy wypożyczania rowerów, samochodów oraz wyznaczające strefy płatnego parkowania	Monitorowanie osób korzystających z usług w przestrzeni publicznej, przy wykorzystaniu danych wykraczających poza dane niezbędne do świadczenia

<p>wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa</p>	<p>Zakłady pracy (monitoring systemów informatycznych poczty elektronicznej, używanego oprogramowania, kart dostępowych itp.)</p>	<p>tych usług</p> <p>Systemy monitorowania czasu pracy pracowników oraz przepływu informacji w wykorzystywanych przez nich narzędziach (poczty elektronicznej, Internetu)</p> <p>Kryterium: systematyczne monitorowanie (vide WP 249¹) + wrażliwe podmioty danych</p>
	<p>Przetwarzanie informacji pozyskiwanych przez Internet rzeczy (opaski medyczne, smartwatche itp.) oraz ich przesyłanie w sieci przy użyciu urządzeń mobilnych typu smartfon czy tablet</p>	<p>Gromadzenie i wykorzystywanie danych przez aplikacje instalowane w urządzeniach mobilnych, w tym w urządzeniach zintegrowanych z mundurem, kaskiem lub w inny sposób połączonych z osobą pozyskującą dane</p>
	<p>Systemy komunikujące się typu maszyna - maszyna, w których samochód informuje otoczenie o swoim zachowaniu (ruchu) i w przypadku pojawiającego się zagrożenia otrzymuje od tego otoczenia (infrastruktura drogowa, inne samochody) komunikaty ostrzegawcze</p>	<p>Systemy monitoringu pojazdów nawiązujące połączenia z otoczeniem, w tym z innymi pojazdami</p>
	<p>Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie identyfikacji radiowej (RFID) (2007/C 256/13)</p>	<p>Systemy wykorzystujące RFID w przypadku, gdy znaczniki/etykiety są lub mogą być przypisane osobom fizycznym</p>
	<p>Szpitala/Organizacje prowadzące badania kliniczne. Kluby fitness/ podmioty/ organizacje pobierające materiał genetyczny do badań</p>	<p>Dane dotyczące zdrowia pacjentów/klientów</p>
<p>4. Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29)</p>	<p>Partie polityczne, komitety wyborcze, komitety referendalne i inicjatywy ustawodawcze, organizacje społeczne, kampanie wyborcze</p>	<p>Przetwarzanie przez organy państwowe lub podmioty prywatne danych osobowych dotyczących przynależności partyjnej i/lub preferencji wyborczych</p>
	<p>Operatorzy telekomunikacyjni; dostawcy mediów (prąd, gaz, woda) w zakresie inteligentnego opomiarowania - Zalecenie 2012/148/UE Komisji Europejskiej z marca 2012 r. w sprawie przygotowań do rozpowszechniania inteligentnych systemów pomiarowych</p>	<p>Regularne przetwarzanie danych pomiarowych umożliwiające obserwację stylu życia, przemieszczania się w terenie, intensywności korzystania z mediów, energii itp. (np. danych geolokalizacyjnych, danych z inteligentnych liczników pomiarowych o zużywanym energii, danych bilingowych dotyczących komunikacji elektronicznej itp.)</p>
	<p>Usługi poczty elektronicznej; systemy monitoringu osiągnięć sportowych współpracujące z opaskami typu fitness wykorzystujące chmurę obliczeniową; aplikacje dostarczane przez producentów czytników elektronicznych do zakupu</p>	<p>Serwisy internetowe i inne systemy informatyczne oferowane osobom fizycznym do przetwarzania informacji obejmujących działania o charakterze czysto osobistym lub domowym (jak np. usługi przetwarzania w chmurze do</p>

	książek, gazet elektronicznych z funkcjami robienia notatek itp.	zarządzania dokumentami osobistymi, usługi poczty elektronicznej, kalendarze, e-czytniki wyposażone w funkcje robienia notatek oraz różne aplikacje typu "life-logging", które mogą zawierać informacje o bardzo osobistym charakterze), których ujawnienie lub przetwarzanie do celów innych niż czynności o charakterze domowym może być uznane za bardzo ingerujące w prywatność
5. Przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu	Systemy rozpoznawania twarzy, weryfikacja tożsamości w miejscu pracy w celu kontroli dostępu, weryfikacja tożsamości w urządzeniach/aplikacjach (wliczając rozpoznawanie głosu, odcisków palców, twarzy); systemy monitoringu wejść do określonych pomieszczeń; systemy rozliczeniowo-ewidencyjne operacji bankowych, handlowych, ubezpieczeniowych; systemy kontroli wejść do klubów fitness, hoteli itp.	Wejścia do określonych obszarów, pomieszczeń lub uzyskanie dostępu do określonego konta w systemie informatycznym w celu np. wykonania zlecenia transakcji w systemie teleinformatycznym lub wypłaty gotówki przy użyciu bankomatu itp.
6. Przetwarzanie danych genetycznych	Laboratoria/Firmy/Szpitala oferujące diagnostykę genetyczną	Diagnoza medyczna Testy DNA Badania medyczne
7. Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: * liczby osób, których dane są przetwarzane, * zakresu przetwarzania, * okresu przechowywania danych oraz * geograficznego zakresu przetwarzania	Centralny system: - informacji oświatowej; - informacji w szkolnictwie wyższym; - obsługi ubezpieczeń komunikacyjnych; - kwalifikacji zawodowych itp.	Centralne zbiory danych wspomagające zarządzanie określoną grupą osób w celach związanych z realizacją zadań publicznych, z których dane udostępniane są w różnym zakresie w zależności od ich roli i zadań związanych z realizacją tych obowiązków
	Portale społecznościowe, przeglądarki internetowe, dostawcy usług telewizji kablowej, serwisy subskrypcyjne z filmami i programami telewizyjnymi dostępne na urządzeniach z dostępem do Internetu	Zbieranie szerokiego zakresu danych o przeglądanych stronach internetowych, realizowanych zakupach/ historii zakupów, oglądanych programach telewizyjnych lub radiowych itp.
8. Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł	Firmy marketingowe pobierające dane z różnych źródeł, gdzie występują dane osobowe o klientach, w celach przeprowadzania ukierunkowanych na określone grupy klientów akcji marketingowych	Łączenie danych z różnych rejestrów państwowych i/lub publicznych
	Firmy marketingowe w celach doskonalenia i rozszerzania profili potencjalnych klientów oraz doskonalenia usług reklamy ukierunkowanej na określone grupy społeczne; firmy obsługujące programy lojalnościowe (wspólnoty zakupowe)	Tworzenie profili osób ze zbiorów danych pochodzących z różnych źródeł (łączenie zbiorów)

	Portale społecznościowe, sieci handlowe, firmy marketingowe, banki i instytucje finansowe	Zbieranie danych o przeglądanych stronach, wykonywanych operacjach bankowych, zakupach w sklepach internetowych, a następnie ich analiza w celu tworzenia profilu osoby
9. Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi	Serwisy oferujące pracę, które dokonują dopasowania ofert do określonych preferencji pracodawców	Przetwarzanie danych, w których dokonuje się klasyfikacji lub ocen osób, których dane dotyczą, pod względem np. wieku, płci, a następnie klasyfikacje te wykorzystuje się do przedstawienia ofert lub innych działań, które mogą mieć wpływ na prawa lub wolność osób, których dane są przetwarzane
	Systemy służące do zgłaszania nieprawidłowości (whistleblowing)	Systemy służące do zgłaszania nieprawidłowości (związanych np. z korupcją, mobbingiem) - w szczególności gdy przetwarzane są w nim dane pracowników
10. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych	Sprzedawcy i dystrybutorzy mediów (prąd, gaz, woda, usługi telekomunikacyjne) wdrażający inteligentne liczniki	Systemy zdalnego opomiarowania, które, biorąc pod uwagę zakres i częstość zbierania danych, umożliwiają profilowanie osób lub grupy osób
	Serwisy internetowe przetwarzające dane z urządzeń typu Internet rzeczy, np. aparatów fotograficznych wyposażonych w funkcje lokalizacyjne (GPS)	Systemy analizy i przetwarzania danych znajdujących się w metadanych, np. zdjęcia opatrzone danymi geolokalizacyjnymi
	Zastosowanie komunikacji między urządzeniami (Internet rzeczy - np. beacons, drony) w przestrzeni publicznej i w miejscach użyteczności publicznej	Systemy stosowane do analizy i przekazywania danych dostawcom usługi przy użyciu aplikacji mobilnych z urządzeń przenośnych typu: smartwatch, inteligentne opaski, beacons itp. analizujące i przekazujące dane dostawcom przy użyciu aplikacji mobilnych
	Aplikacje z funkcjami komunikowania się i oprogramowaniem umożliwiającym wymianę informacji z najbliższym otoczeniem oraz zdalnie poprzez sieć telekomunikacyjną	Stosowanie urządzeń wyposażonych w różnego rodzaju interfejsy (głośnik, mikrofon, kamera) oraz oprogramowanie i system łączności umożliwiające przekazywanie danych poprzez sieci telekomunikacyjne
	Zabawki interaktywne	Usługi i zabawki dedykowane dzieciom
	Specjalistyczne porady i konsultacje medyczne, badania kliniczne o zasięgu międzynarodowym	Konsultacje telemedyczne z ośrodkami spoza UE, przekazywanie osobowych danych medycznych o zasięgu międzynarodowym
11. Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy	Podmioty udzielające pożyczek i kredytów oraz oferujące sprzedaż ratalną	Podjęcie decyzji kredytowej w stosunku do potencjalnych klientów na podstawie informacji zawartych w bazach zawierających informacje o dłużnikach lub podobnych bazach danych
	Sklepy internetowe oraz dostawcy innych	Uzależnianie możliwości korzystania z

	usług typu gry, muzyka, loterie itp.	usługi od informacji w zakresie dochodów, kwoty wydatków miesięcznych i innych wartości zebranych w wyniku profilowania
12. Przetwarzanie danych lokalizacyjnych	<p>Urządzenia, aplikacje i platformy wykorzystujące Internet rzeczy.</p> <p>Przetwarzanie danych w kontekście pracy w domu i pracy wykonywanej zdalnie.</p> <p>Przetwarzanie danych lokalizacyjnych pracowników</p>	<p>Przetwarzanie wykorzystujące śledzenie lokalizacji osoby fizycznej (wliczając sieci komunikacyjne i usługi komunikacyjne, wskazujące geograficzną pozycję telekomunikacyjnych terminali urządzeń użytkownika publicznie dostępnej usługi telekomunikacyjnej)</p>

