Załącznik nr 2 do Zarządzenia Dyrektora Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy z dnia 25.05.2023 r.

Załącznik nr 14 do Polityki Bezpieczeństwa Informacji Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy

WYCIĄG Z POLITYKI BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE DANYCH OSOBOWYCH

§1

PREAMBUŁA

Administratorem danych osobowych (Administratorem) jest Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy reprezentowana przez Dyrektor, który ustala cele i sposoby przetwarzania danych osobowych.

Administrator danych osobowych mając na uwadze jak ważne jest bezpieczeństwo przetwarzanych danych osobowych ze względu na ochronę podstawowych praw i wolności osób fizycznych, a w szczególności ich prawo do ochrony danych osobowych oraz w celu zapewnienia zgodności z wymaganiami prawa, ustanawia system ochrony danych osobowych.

Ramy ustanowionego systemu ochrony danych osobowych tworzy polityka bezpieczeństwa informacji uwzględniająca ochronę danych osobowych oraz powiązane z nią dokumenty.

Administrator danych osobowych deklaruje pełne zaangażowanie w dążeniu do spełnienia wymagań wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (zwanego dalej RODO), Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000) i wymagań kontraktowych w tym obszarze oraz ciągłe doskonalenie systemu ochrony danych osobowych.

§2

ROLE W SYSTEMIE OCHRONY DANYCH OSOBOWYCH

Administrator danych osobowych (ADO, Administrator), oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi, ustala cele i sposoby przetwarzania danych osobowych.

Inspektor ochrony danych (IOD), osoba spełniająca wymagania określone w art. 37 ust. 5 RODO powołana przez Administratora danych osobowych w celu nadzorowania procesu ochrony danych osobowych

Dane kontaktowe do Inspektora Ochrony Danych:

- Email adres: iodo@bppragapd.pl
- Numer Telefonu: + 48 22 27 76 100
- Adres do korespondencji: ul. Jana Nowaka-Jeziorańskiego 24, 03-982 Warszawa

§3

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z wymogami RODO dane osobowe muszą być:

- Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**„zasada zgodności z prawem, rzetelności i przejrzystości"**);
- Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; w myśl art. 89 ust. 1 RODO dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie uznaje się za niezgodne z pierwotnymi celami (**„zasada ograniczenia celu"**);
- Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane (**„zasada minimalizacji danych"**);
- **Prawidłowe i w razie potrzeby uaktualniane**, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- **Przechowywane w formie umożliwiającej identyfikację osoby**, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy artykułu 89 ust.1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą;
- **Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych**, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych lub organizacyjnych.

§4

ZASADY UDOSTĘPNIENIA I POWIERZANIA DANYCH OSOBOWYCH

Dane osobowe udostępnia się na pisemny, umotywowany wniosek pochodzący od danego podmiotu lub osoby, chyba że szczególne przepisy prawa stanowią inaczej.

Wniosek o udostępnienie informacji, o którym mowa powyżej, powinien zawierać:

- nazwę podmiotu, jego adres oraz podpis osoby upoważnionej do jego reprezentowania;
- podstawę prawną upoważniającą go do otrzymania informacji na mocy przepisów prawa lub zawartej Umowy;
- wskazanie przeznaczenia dla udostępnionych danych;
- zakres żądanych informacji;
- uzasadnienie potrzeby posiadania informacji, jeżeli ich otrzymywanie nie wynika z przepisów prawa lub zawartej umowy.

Każdorazowe udostępnienie danych osobowych musi być zatwierdzone przez ADO.

Powierzenie danych osobowych do przetwarzania odbywa się zgodnie z art. 28 RODO. Zgodnie z tym artykułem powierzenie może nastąpić na podstawie odpowiedniej umowy spełniającej wymogi wynikające z art. 28 ust. 3 RODO. Każda umowa powierzenia przetwarzania danych przed podpisaniem powinna zostać skonsultowana z IOD.

Dodatkowo zgodnie z wymaganiami RODO w odniesieniu do podmiotów przetwarzających (procesorów) tj. zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymogi RODO i chroniło prawa osób, których dane dotyczą, osoba odpowiedzialna za zawarcie umowy z danym procesorem zobowiązana jest przekazać do wypełnienia kwestionariusz bezpieczeństwa. W przypadku wątpliwości co do oceny potencjalnego procesora należy wypełniony kwestionariusz przesłać do analizy IOD, który po dokonaniu weryfikacji zobowiązany jest wydać swoje rekomendacje.

§5

POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych, zgodnie z art. 4 pkt 12 RODO, 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.

Każde naruszenie ochrony danych osobowych, w którym prawdopodobne jest wystąpienie ryzyka naruszenia praw lub wolności osób fizycznych, należy bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłosić do UODO. Zasady zgłoszenia naruszenia ochrony danych osobowych oraz wskazanie elementów, które powinny być zawarte w treści zgłoszenia określa art. 33 RODO.

Każde naruszenie ochrony danych osobowych musi zostać niezwłocznie po jego stwierdzeniu zgłoszone do IOD, który wspiera ADO w procesie identyfikacji i określenia skutków takiego naruszenia.

W uzasadnionych przypadkach należy dokonać zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z regulacjami art. 34 RODO.

Zapisy dotyczące kwestii zgłaszania naruszeń muszą się znajdować w umowach między ADO, a podmiotem przetwarzającym. Wskazane jest, aby rekomendowany czas zgłoszenia przez procesora do ADO naruszenia nie przekroczył 24h.