Załącznik nr 3 do Zarządzenia Dyrektora Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy z dnia 25.05.2023 r.
Załącznik nr 15 do Polityki Bezpieczeństwa Informacji Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy

Kwestionariusz pytań dla Procesora

LP	*Pozycja*	*Odpowiedź*
1	Nazwa Organizacji:	
2	Data wypełnienia formularza:	
3	Imię i nazwisko oraz adres e-mail osoby uzupełniającej:	
4	Proszę podać, jaki rodzaj usługi jest realizowany na rzecz Administratora:	
5	Proszę opisać, jakie inne usługi są realizowane na rzecz Administratora:	
6	Proszę podać zakres danych osobowych przetwarzanych w ramach usługi, niezależnie od sposobu przetwarzania:	
7	Proszę opisać główne założenia realizowanej usługi na rzecz Administratora:	
8	Czy została podpisana umowa powierzenia przetwarzania danych osobowych między Administratorem a Państwa organizacją?	
9	Proszę określić, czy Państwa organizacja korzysta z podwykonawców, którzy będą mieli pośrednio lub bezpośrednio dostęp do powierzonych danych osobowych (proszę podać nazwy tych podmiotów):	
10	Czy został powołany Inspektor Ochrony Danych?	
11	Czy Polityka ochrony danych osobowych została ustanowiona? Jeśli tak, proszę załączyć kopię strony na której widnieje podpis osoby zatwierdzającej politykę.	
12	Czy została ustanowiona i ogłoszona Polityka / Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe? Proszę podać nazwę dokumentu i zakres dokumentu:	
13	Czy dla każdej osoby przetwarzającej dane osobowe zostało wydane upoważnienie do przetwarzania danych osobowych?	
14	Czy została przeprowadzona analiza ryzyka w obszarze przetwarzania danych osobowych dla dostarczanej uługi/produktu?	
15	Czy został ustanowiony plan postępowania z ryzykiem?	
16	Czy został wdrożony plan postępowania z ryzykiem zgodnie z przyjętym harmonogramem?	
17	Czy została ustanowiona procedura nadawania dostępów do aktywów informatycznych?	
18	Czy została ustanowiona procedura utrzymania ciągłości działania dostarczanej usługi/produktu?	
19	Czy została ustanowiona procedura reakcji na incydent naruszenia bezpieczeństwa danych osobowych?	
20	Czy została ustanowiona procedura zgłaszania naruszenia bezpieczeństwa danych osobowych do UODO w ciągu 72 godzin od wykrycia incydentu?	

21	Czy została ustanowiona zasada "privacy by design"?	
22	Czy została ustanowiona zasada "privacy by default "?	
23	Czy z podwykonawcami zaangażowanymi w realizację usługi/produktu została zawarta umowa powierzenia przetwarzania danych osobowych?	
24	Czy została przeprowadzona analiza ryzyka dla podwykonawców?	
25	Czy systemy lub inne aktywności związane z przetwarzaniem danych osobowych powodują konieczność wysłania (transferu, przechowywania) danych osobowych do krajów spoza EOG (włączając podwykonawców)?	
26	Czy została przeprowadzona ocena skutków dla ochrony danych osobowych?	
27	Proszę podać jakie rejestry dotyczące ochrony danych osobowych są prowadzone w organizacji:	
28	Proszę podać, jakie elementy bezpieczeństwa IT zostały wdrożone u Państwa organizacji:	
29	Proszę określić, gdzie znajdują się fizycznie serwery Państwa systemów informatycznych wykorzystywanych do przetwarzania przekazanych danych osobowych w ramach realizowanej usługi:	
30	Proszę określić, w jaki sposób (za pomocą jakich narzędzi) są przekazywane dane (np.ftp, email, sftp, specjalny portal www, itd.) w ramach realizowanej usługi:	
31	Proszę określić jakie mechanizmy zostały wdrożone aby zapewnić bezpieczeństwo przekazanej dokumentacji papierowej zawierającej dane osobowe:	
32	Proszę określić główne mechanizmy bezpieczeństwa fizycznego serwerów przetwarzających przekazane dane osobowe:	
33	Czy w okresie ostatnich 5 lat Państwa organizacja podlegała kontroli GIODO/UODO?	
34	Czy w okresie ostatnich 5 lat w Państwa organizacji zostało stwierdzone naruszenie ochrony danych osobowych, które było potwierdzone decyzją GIODO/UODO lub/i prawomocnym wyrokiem sądu?	
35	Czy w okresie ostatnich 5 lat mieliście Państwo sytuacje, które spowodowały uruchomienie Państwa planów ciągłości działania?	
36	Czy organizacja posiada certyfikowany system zarządzania bezpieczeństwem informacji - ISO27001? Jeśli tak, proszę załączyć kopię certyfikatu.	