Załącznik nr 7 do
Polityki Ochrony Danych Osobowych
Starostwa Powiatowego w Żyrardowie

Kwestionariusz pytań dla podmiotu przetwarzającego dane osobowe

LP	*Pozycja*	*Odpowiedź*
1	Nazwa Organizacji	
2	Data wypełnienia formularza	
3	Imię i nazwisko oraz adres email osoby uzupełniającej	
4	Proszę podać, jaki rodzaj usługi jest realizowany na rzecz Administratora Danych	
5	Proszę opisać, jakie inne usługi są realizowane na rzecz Administratora Danych	
6	Proszę podać zakres danych osobowych przetwarzanych niezależnie od sposobu przetwarzania	
7	Proszę opisać główne założenia realizowanej usługi na rzecz Administratora Danych	
8	Czy została podpisana umowa powierzenia przetwarzania danych osobowych między Administratorem Danych a Państwa organizacją ?	
9	Czy został powołany Inspektor Ochrony Danych ?	
10	Czy planowane jest powołanie Inspektora Ochrony Danych ?	
11	Czy Polityka Ochrony Danych Osobowych została ustanowiona ?	
12	Jeśli udzielono odp. na pytanie 11 - TAK, to proszę załączyć kopię strony na której widnieje podpis osoby zatwierdzającej politykę	
13	Czy została ustanowiona i ogłoszona Instrukcja Zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe ?	
14	Czy dla każdej osoby przetwarzającej dane osobowe zostało wydane upoważnienie do przetwarzania danych osobowych ?	
15	Czy została przeprowadzona analiza ryzyka w obszarze przetwarzania danych osobowych dla dostarczanej usługi/produktu ?	
16	Czy został ustanowiony plan postępowania z ryzykiem ?	
17	Czy został wdrożony plan postępowania z ryzykiem zgodnie z przyjętym harmonogramem ?	
18	Czy została ustanowiona procedura nadawania dostępów do aktywów informatycznych ?	
19	Czy została ustanowiona procedura utrzymania ciągłości działania dostarczanej usługi/produktu ?	
20	Czy została ustanowiona procedura reakcji na incydent naruszenia bezpieczeństwa danych osobowych ?	
21	Czy została ustanowiona procedura zgłaszania naruszenia bezpieczeństwa danych osobowych do Urzędu Ochrony Danych Osobowych w ciągu 72 godzin od wykrycia incydentu ?	
22	Czy została ustanowiona zasada "privacy by design" ?	
23	Czy została ustanowiona zasada "privacy by default " ?	
24	Proszę określić, czy organizacja korzysta z podwykonawców, którzy będą mieli pośrednio lub bezpośrednio dostęp do powierzonych danych osobowych (proszę podać nazwy tych podmiotów)	
25	Czy z podwykonawcami została zawarta umowa powierzenia przetwarzania danych osobowych ?	
26	Czy została przeprowadzona analiza ryzyka dla podwykonawców ?	
27	Czy systemy lub inne aktywności związane z przetwarzaniem danych osobowych powodują konieczność wysłania (transferu, przechowywania) do krajów spoza EEA (włączając podwykonawców) ?	
28	Czy została przeprowadzona ocena skutków dla ochrony danych osobowych ?	
29	Proszę podać jakie rejestry dotyczące ochrony danych osobowych są prowadzone w organizacji	
30	Proszę podać, jakie elementy bezpieczeństwa IT zostały wdrożone u Państwa organizacji	
31	Proszę określić, gdzie znajdują się fizycznie serwery Państwa systemów informatycznych wykorzystywanych do przetwarzania przekazanych danych osobowych	
32	Proszę określić, w jaki sposób są przekazywane dane (np. ftp, email, sftp, specjalny portal www, itd.)	
33	Proszę określić jakie mechanizmy zostały wdrożona aby zapewnić bezpieczeństwo przekazanej dokumentacji papierowej zawierającej dane osobowe	
34	Proszę określić główne mechanizmy bezpieczeństwa fizycznego serwerów przetwarzających przekazane dane osobowe	
35	Czy w okresie ostatnich 5 lat Państwa organizacja podlegała kontroli GIODO /UODO ?	
36	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 ?	
37	Czy w okresie ostatnich 5 lat mieliście Państwo sytuacje, które spowodowały uruchomienie Państwa planów ciągłości działania ?	
38	Czy organizacja posiada Certyfikat ISO27001?	
39	Jeśli udzielono odp. na pytanie 38 - TAK, to proszę załączyć kopię certyfikatu	

WICESTAROSTA
Krzysztof Dziwisz