ZARZĄDZENIE NR 1/2026
STAROSTY OSTROWSKIEGO

z dnia 7 stycznia 2026 r.

zmieniające zarządzenie w sprawie aktualizacji Polityki Ochrony Danych Osobowych w Starostwie Powiatowym w Ostrowi Mazowieckiej

Na podstawie art. 24 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady Europy (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 Nr 119, str. 1), w związku z art. 35 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tj. Dz. U. 2025, poz. 1684) zarządza się, co następuje:

§ 1. W Zarządzeniu Nr 7/2021 Starosty Ostrowskiego z dnia 29 stycznia 2021 r. w sprawie aktualizacji Polityki Ochrony Danych Osobowych w Starostwie Powiatowym, zmienionym Zarządzeniem Nr 5/2024 Starosty Ostrowskiego z dnia 16 stycznia 2024 r. oraz Zarządzeniem Nr 25/2025 Starosty Ostrowskiego z dnia 2 lipca 2025 r. załącznik nr 10 stanowiący załącznik do Polityki Ochrony Danych Osobowych w Starostwie Powiatowym w Ostrowi Mazowieckiej otrzymuje brzmienie zgodnie z załącznikiem do niniejszego Zarządzenia.

§ 2. Wykonanie Zarządzenia powierza się kierownikom komórek organizacyjnych oraz osobom zajmującym samodzielne stanowiska pracy w Starostwie Powiatowym.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Ostrowski

Jerzy Bauer

Załącznik do zarządzenia Nr 1/2026
Starosty Ostrowskiego
z dnia 7 stycznia 2026 r.

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.	Proszę określić, czy organizacja korzysta z podwykonawców, którzy będą mieli pośrednio lub bezpośrednio dostęp do powierzonych danych osobowych (proszę podać nazwy tych podmiotów).	
10.	Czy został powołany Administratora Bezpieczeństwa Informacji (od 25.05.2018 Inspektor Ochrony Danych) ?	
11.	Czy planowane jest powołanie Inspektora Ochrony Danych od 25.05.2018 ?	
12.	Czy Polityka Ochrony Danych Osobowych została ustanowiona ?	
13.	Proszę załączyć kopię strony na której widnieje podpis osoby zatwierdzającej politykę.	
14.	Czy została ustanowiona i ogłoszona Instrukcja Zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe ?	
15.	Czy dla każdej osoby przetwarzającej dane osobowe zostało wydane upoważnienie do przetwarzania danych osobowych ?	
16.	Czy została przeprowadzona analiza ryzyka w obszarze przetwarzania danych osobowych dla dostarczanej uługi/produktu ?	
17.	Czy został ustanowiony plan postępowania z ryzykiem ?	
18.	Czy został wdrożony plan postępowania z ryzykiem zgodnie z przyjętym harmonogramem ?	
19.	Czy została ustanowiona procedura nadawania dostępów do aktywów informatycznych ?	

20.	Czy została ustanowiona procedura utrzymania ciągłości działania dostarczanej usługi/produktu ?	
21.	Czy została ustanowiona procedura reakcji na incydent naruszenia bezpieczeństwa danych osobowych ?	
22.	Czy została ustanowiona procedura zgłaszania naruszenia bezpieczeństwa danych osobowych w ciągu 72 godzin od wykrycia incydentu ?	
23.	Czy została ustanowiona zasada "privacy by design" ?	
24.	Czy została ustanowiona zasada "privacy by default " ?	
25.	Czy organizacja wykorzystuje inne podmioty do dostarczenia danej usługi/produktu ?	
26.	Czy z podwykonawcami została zawarta umowa powierzenia przetwarzania danych osobowych ?	
27.	Czy została przeprowadzona analiza ryzyka dla podwykonawców ?	
28.	Czy systemy lub inne aktywności związane z przetwarzaniem danych osobowych powodują konieczność wysłania (transferu, przechowywania) do krajów spoza EEA (włączając podwykonawców) ?	
29.	Czy została przeprowadzona ocena skutków dla ochrony danych osobowych ?	
30.	Proszę podać jakie rejestry dotyczące ochrony danych osobowych są prowadzone w organizacji	
31.	Proszę podać, jakie elementy bezpieczeństwa IT zostały wdrożone u Państwa organizacji.	
32.	Proszę określić, gdzie znajdują się fizycznie serwery Państwa systemów informatycznych wykorzystywanych do przetwarzania przekazanych danych osobowych.	
33.	Proszę określić, w jaki sposób są przekazywane dane (np.. ftp, email, sftp, specjalny portal www, itd…)	
34.	Proszę określić jakie mechanizmy zostały wdrożone aby zapewnić bezpieczeństwo przekazanej dokumentacji papierowej zawierającej dane osobowe.	
35.	Proszę określić główne mechanizmy bezpieczeństwa fizycznego serwerów przetwarzających przekazane dane osobowe.	
36.	Czy w okresie ostatnich 5 lat Państwa organizacja podlegała kontroli UODO ?	
37.	Czy w okresie ostatnich 5 lat w Państwa organizacji zostało stwierdzone naruszenie ochrony danych osobowych, które było potwierdzone decyzją UODO lub/i prawomocnym wyrokiem sądu ?	
38.	Czy w okresie ostatnich 5 lat mieliście Państwo sytuacje, które spowodowały uruchomienie Państwa planów ciągłości działania ?	
39.	Czy organizacja posiada Certyfikat ISO27001?	

40.	Proszę załączyć kopię certyfikatu.	