

**ZARZĄDZENIE Nr 19/2021**  
**Dyrektora Powiatowego Centrum Oświatowego**  
**z dnia 12 maja 2021 r.**

**w sprawie wyznaczenia Inspektora Ochrony Danych, zastępcy Inspektora Ochrony Danych oraz  
wyznaczenia Administratora Systemu Informatycznego w Powiatowym Centrum Oświatowym  
w Mogilnie**

*Na podstawie art 37 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 osobowych), oraz art. 8 i art. 11a Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).*

**zarządzam, co następuje:**

§ 1. 1. Wyznacza się Panią Samantę Zwolanowską na Inspektora Ochrony Danych (IOD) w Powiatowym Centrum Oświatowym w Mogilnie.

2. Zakres powierzonych do wykonywania obowiązków IOD określa załącznik nr 1 do niniejszego zarządzenia.

3. W zakresie powierzonych obowiązków IOD podlega bezpośrednio Dyrektorowi.

§ 2. 1. Wyznacza się Panią Edytę Owsieńską na zastępcę Inspektora Ochrony Danych (IOD) w Powiatowym Centrum Oświatowym w Mogilnie.

2. Zakres powierzonych do wykonywania obowiązków zastępcy IOD określa załącznik nr 2 do niniejszego zarządzenia.

3. W zakresie powierzonych obowiązków zastępcy IOD podlega bezpośrednio Dyrektorowi.

§ 3. 1. Wyznacza się Pana Szymona Jankowskiego oraz Marcina Szajdę na Administratorów Systemu Informatycznego (ASI) w Powiatowym Centrum Oświatowym w Mogilnie.

2. Zakres powierzonych do wykonywania obowiązków ASI określa załącznik nr 3 do niniejszego zarządzenia.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor  
Powiatowego Centrum Oświatowego  
w Mogilnie,  
*Mariusz Pisula*  
mgr Mariusz Pisula

Karolina Madzińska  
*K. Madzińska*  
RADCA PRAWNY  
BD-1378

### **Zakres obowiązków powierzonych IOD**

Inspektor Ochrony Danych jest obowiązany do:

1. informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. monitorowania przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4. współpracy z organem nadzorczym;
5. pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

### **Zakres obowiązków powierzonych Zastępcy IOD**

W przypadku nieobecności Inspektora Ochrony Danych Osobowych Zastępca IOD jest obowiązany do:

1. informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. monitorowania przestrzegania 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), innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4. współpracy z organem nadzorczym;
5. pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

## **Zakres obowiązków powierzonych Administratorowi Systemu Informatycznemu**

Administrator Systemu Informatycznego, w zakresie zadań wykonywanych dla zapewnienia systemom bezpieczeństwa zgodnego z celami i metodologią wdrożonej polityki bezpieczeństwa informacji, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji.

Do zadań Administratora Systemu Informatycznego w szczególności należy:

1. formułowanie, w uzgodnieniu z administratorem danych, którym administrator delegował uprawnienia oraz IOD, sposobu określania uprawnień w systemach informatycznych,
2. realizacja decyzji Dyrektora Powiatowego Centrum Oświatowego odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT PCO tj.:
  - a) tworzenie kont użytkowników w systemach informatycznych,
  - b) przypisywanie startowych haseł uwierzytelniających użytkowników kont,
  - c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
  - d) resetowanie utraconych haseł,
  - e) usuwanie kont osób, które zakończyły pracę w PCO,
  - f) dostarczanie IOD informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych;
3. prowadzenie ewidencji uprawnień,
4. planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w PCO,
5. prowadzenie dziennika administratora systemów informatycznych,
6. prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych,
7. planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych zgodnie z harmonogramem,
8. zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
9. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe,
10. monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
11. monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych oraz zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych,
12. systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,

13. zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki,
14. rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych,
15. monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych,
16. podejmowanie odpowiednich działań w przypadku wykrycia lub podejrzenia naruszenia zabezpieczeń,
17. przygotowywanie, we współpracy z IOD, instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji,
18. prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów informatycznych,
19. nadzór nad systemem komunikacji w sieci komputerowej.

