ZARZĄDZENIE NR 44/2024/2025

Dyrektora Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie

z dnia 25.08.2025 r.

w sprawie: Procedury używania służbowych zewnętrznych nośników danych przez pracowników Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie

§ 1.

Procedury używania służbowych zewnętrznych nośników danych przez pracowników Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie– stanowiące załącznik nr 1, zostają wprowadzone w celu:

1. Zapewnienia zgodności z przepisami RODO - zgodnie z art. 5 RODO;
2. Zminimalizowania ryzyka naruszeń oraz zapewnia, że wszelkie działania są zgodne z prawem.
3. Określa zasady użytkowania służbowych zewnętrznych nośników danych.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

(-) Sylwia Szczygłowska

Dyrektor Szkoły Podstawowej nr 27

im. Z. Łęskiego w Częstochowie

Załącznik nr 1 do Zarządzenia nr 44/2024/2025 z dnia 25.08.2025r.

Procedura używania służbowych zewnętrznych nośników danych przez pracowników Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie

Definicje

Szkoła - nazwa jednostki

Pracownicy – osoba zatrudniona przez Dyrektora Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie na podstawie umowy o pracę

Zewnętrzny nośnik danych – służbowy, szyfrowany nośnik danych będący własnością Szkoły Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie

Cel procedury

Zapewnienie bezpieczeństwa danych osobowych i innych informacji chronionych, przechowywanych na szyfrowanych nośnikach danych używanych przez pracowników szkoły oraz ochrona tych danych przed dostępem osób nieuprawnionych.

1. Zakres procedury

Procedura dotyczy wszystkich pracowników szkoły, którzy wykorzystują zewnętrzne nośniki danych w celu przechowywania, przetwarzania lub drukowania danych związanych z realizacją zadań służbowych pracowników szkoły.

2. Zasady ogólne

1) **Zakup i rejestracja zewnętrznych nośników danych**
   a. Zewnętrzne nośniki danych są zapewniane przez szkołę.
   b. Każdy zewnętrzny nośnik danych musi być oznaczony i zarejestrowany w spisie sprzętu wykorzystywanego do przetwarzania danych osobowych.
   c. Pracownicy nie mogą używać prywatnych nośników danych do celów służbowych.
2) **Procedury weryfikacji dostępu**
   a. Dostęp do danych przechowywanych na zewnętrznych nośnikach danych mają wyłącznie osoby upoważnione przez dyrektora szkoły.

b. Lista osób upoważnionych do korzystania z zewnętrznych nośników danych oraz przypisanych im urządzeń jest prowadzona przez Dyrektora i podlega okresowej weryfikacji.

c. Każdy pracownik jest zobowiązany do nieudostępniania zewnętrznego nośnika danych innym osobom, również wewnątrz szkoły, bez zgody dyrektora.

3) **Korzystanie z zewnętrznych nośników danych**

a. Zewnętrzny nośnik danych może być używany wyłącznie do przechowywania danych służbowych.

b. Wszystkie dane przechowywane na zenętrznych nośnikach danych muszą być zaszyfrowane.

c. Dostęp do danych jest możliwy wyłącznie po podaniu hasła.

d. Pracownik ma zakaz wynoszenia zewnętrznych nośników danych poza teren szkoły.

4) **Bezpieczeństwo użytkowania**

a. Hasła do zewnętrznych nośników danych muszą spełniać wymogi bezpieczeństwa (minimum 12 znaków, duże i małe litery, cyfry, znaki specjalne).

b. Hasło nie może być zapisywane w łatwo dostępnych miejscach ani udostępniane innym osobom.

c. W przypadku zgubienia lub kradzieży zewnętrznego nośnika danych należy natychmiast powiadomić Dyrektora szkoły, który następnie powiadomi Inspektora Ochrony Danych.

5) **Przenoszenie danych**

a. Zewnętrzny nośnik danych może być podłączany wyłącznie do wyznaczonych urządzeń służbowych wyposażonych w aktualne oprogramowanie antywirusowe.

b. Zabrania się podłączania zewnętrznych nośników danych do urządzeń nie będących własnością szkoły.

c. Dane należy usuwać z zewnętrznego nośnika danych natychmiast po ich przeniesieniu na służbowy sprzęt szkolny.

d. Na zewnętrznych nośnikach danych powinny znajdować się tylko kopie dokumentów. Oryginał dokumentu pozostaje na laptopie służbowym.

3. Sposób postępowania w przypadku naruszenia bezpieczeństwa

1) W razie podejrzenia naruszenia bezpieczeństwa danych (np. zgubienie zewnętrznego nośnika danych, wyciek danych, nieautoryzowany dostęp) pracownik ma obowiązek:
   a. Natychmiast powiadomić dyrektora, który powiadomi IOD.
   b. Opisać okoliczności zdarzenia w formie pisemnej.
   c. Współpracować z Dyrektorem oraz Inspektorem Ochrony Danych w celu minimalizacji ryzyka.
   d. W przypadku naruszenia bezpieczeństwa danych należy postępować zgodnie z Instrukcją reagowania na incydenty mające wpływ na bezpieczeństwo danych przetwarzanych w Szkole Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie stanowiącej załącznik nr 8 do Polityki Bezpieczeństwa Informacji.

4. Szkolenia i świadomość

1) Każdy pracownik przed rozpoczęciem użytkowania zewnętrznego nośnika danych musi przejść szkolenie dotyczące bezpieczeństwa danych przetwarzanych na zewnętrznych nośnikach danych przeprowadzone przez Dyrektora.

2) Szkolenie o którym mowa w ustępie 1 odbywa się co najmniej raz w roku.

5. Odpowiedzialność

1) Pracownik ponosi odpowiedzialność za:

   a. Prawidłowe użytkowanie zewnętrznego nośnika danych.
   b. Zachowanie poufności danych.
   c. Zgłoszenie incydentów naruszenia bezpieczeństwa.
   d. Weryfikacje i poprawność danych przechowywanych na zewnętrznych nośnikach danych.

2) Dyrektor szkołya odpowiada za:
   a. Zapewnienie pracownikom dostępu do odpowiedniego sprzętu i szkoleń.
   b. Monitorowanie zgodności z procedurą.

6. Wybór i konfiguracja zewnętrznych nośników danych

1) Zewnętrzne nośniki danych spełniają wymagania bezpieczeństwa, takie jak:
   a. Sprzętowe szyfrowanie danych (AES-256).
   b. Szyfrowanie za pomocą BitLocker .

7. Okresowe kontrole i audyty

1) Przynajmniej raz na kwartał należy przeprowadzać audyt użytkowania zewnętrznych nośników danych, sprawdzając:
   a. Czy wszystkie zewnętrzne nośniki danych są w spisie sprzętu wykorzystywanego do przetwarzania danych osobowych.
   b. Czy pracownicy przestrzegają procedury (np. stosowanie haseł, bezpieczne przechowywanie).
   c. sprawdzenie poprawności działania szyfrowania.
   d. testy odporności haseł na złamanie.
   e. czy zewnętrzne nośniki danych są sprawne i nadają się do dalszego użytku.
2) Wyniki audytu powinny być przedstawiane w formie raportu i omawiane na spotkaniu z pracownikami a wnioski wdrażane w formie usprawnień procedur.

8. Wydawanie i zwrot zewnętrznych nośników danych

1) Każdorazowe pobranie i oddanie przez pracownika zewnętrznego nośnika danych musi być odnotowane w ewidencji wydanych nośników danych.
2) Pracownik, który opuszcza szkołę lub nie potrzebuje już zewnętrznego nośnika danych, zobowiązany jest do jego zwrotu.

9. Zasady przechowywania zewnętrznych nośników danych

1) Zewnętrzne nośniki danych muszą być przechowywane w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych (np. w zamykanej szufladzie lub szafie).
2) Zabrania się pozostawiania zewnętrznych nośników danych podpiętych pod sprzęt jeżeli pracownik aktualnie na nim nie pracuje oraz pozostawiania go w miejscach ogólnodostępnych np. pomieszczenia socjalne, szatnie, przebieralnie, korytarze, toalety itp.

10. Proces niszczenia zewnętrznych nośników danych

1) Zewnętrzne nośniki danych, które nie są już używane lub uległy uszkodzeniu, podlegają procedurze bezpiecznego niszczenia w celu uniemożliwienia odzyskania danych.
2) Proces niszczenia odbywa się poprzez:
   a. fizyczne zniszczenie nośnika w certyfikowanym urządzeniu niszczącym,
   b. trwałe usunięcie danych przy użyciu specjalistycznego oprogramowania (np. metodą nadpisywania wielokrotnego). Niszczenie zewnętrznych nośników danych jest dokumentowane w protokole, który zawiera:
   - numer ewidencyjny nośnika danych,
   - datę i miejsce zniszczenia,
   - podpisy osób odpowiedzialnych za proces.
3) Dokumentacja dotycząca niszczenia jest przechowywana przez okres zgodny z Jednolitym Rzeczowym Wykazem Akt Szkole Podstawowej nr 27 im. Zygmunta Łęskiego w Częstochowie .

11. Postanowienia końcowe

1) Procedura wchodzi w życie z dniem podpisania.
2) Naruszenie zasad określonych w procedurze może skutkować odpowiedzialnością dyscyplinarną lub innymi konsekwencjami przewidzianymi w regulacjach prawnych.