

Zarządzenie nr 8/2018
Dyrektora Zespołu Szkół nr 2 w Rybniku
z dnia 25 maja 2018 roku

w sprawie zmiany systemu zarządzania bezpieczeństwem informacji, „Procedury zarządzania ryzykiem” i „Procedury zarządzania ryzykiem w bezpieczeństwie informacji”

Na podstawie:

- art. 24 ust. 1 i art. 32 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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),
- art. 68 ust. 2 pkt. 7 i art. 69 ust. 1 pkt 3 ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych,
- § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

zarządzam, co następuje:

§ 1.

Tytuł zarządzenia nr 8/2015 z dnia 11 czerwca 2015 roku otrzymuje brzmienie: *w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.*

§ 2.

1. W załączniku do zarządzenia nr 8/2015 z dnia 11 czerwca 2015 roku:

- 1) skreśla się § 13 ust. 4,
- 2) skreśla się § 15 i § 20,
- 3) w § 32 dodaje się ust. 2 w brzmieniu: *Wymagania dotyczące ochrony fizycznej, kontroli dostępu i wykonywania kopii zapasowych przy pracy na odległość określa „Procedura pracy na odległość”, która stanowi załącznik nr 8,*
- 4) skreśla się § 33 ust. 2,
- 5) § 34 otrzymuje brzmienie:
 1. *Dokumentacja zawierająca dane osobowe powinna być przechowywana w zamkniętych na klucz szafach i szufladach mebli biurowych. Niedopuszczalne jest przechowywanie dokumentacji zawierającej dane osobowe bez jakiegokolwiek zabezpieczenia, np. na otwartych regałach.*
 2. *Dokumentacja zawierająca wrażliwe dane osobowe powinna być przechowywana*

w szafach metalowych o podwyższonej klasie odporności na włamanie i ognioodpornych.

3. Dokumentacja zawierająca dane osobowe po ustaniu jej przydatności do bieżącego przetwarzania oraz braku obowiązku prawnego jej dalszego archiwizowania podlega zniszczeniu w przeznaczonych do tego urządzeniach spełniających co najmniej wymagania poziomu P-3 według normy technicznej DIN 66399 lub równoważnej.
 4. Niedopuszczane jest wyrzucanie do kosza na śmieci jakiegokolwiek dokumentacji zawierającej dane osobowe, bez względu na jej zawartość informacyjną czy upływ czasu od jej wytworzenia.
 5. Pracownik przy przetwarzaniu danych osobowych zobowiązany jest do stosowania zasady czystego biurka polegającej na przechowywaniu pod zamknięciem nieużywanych danych osobowych umieszczonych na elektronicznych nośnikach informacji lub w postaci papierowej, szczególnie jeśli pomieszczenie biurowe jest opuszczane.
 6. Pracownik, którego stanowisko pracy wyposażone jest w tablicę korkową, magnetyczną itp., zobowiązany jest do niezamieszczania na tablicy żadnych danych osobowych.
 7. Pracownik przy przetwarzaniu danych osobowych zobowiązany jest do stosowania zasady czystego ekranu polegającej na:
 - 1) ustawieniu ekranu monitora komputera w sposób uniemożliwiający osobie nieupoważnionej dostęp do danych osobowych wyświetlanych na ekranie monitora,
 - 2) zamykaniu aktywnych sesji po zakończeniu pracy, chyba, że są one zabezpieczone przez odpowiedni mechanizm blokujący – wygaszacz ekranu chroniony hasłem dostępu,
 - 3) zablokowaniu komputera lub wylogowaniu się przy każdorazowym opuszczaniu stanowiska komputerowego w trakcie pracy.
 8. Niedopuszczalne jest pozostawienie osoby nieupoważnionej do przetwarzania danych osobowych w pomieszczeniu biurowym, w którym przetwarzane są dane osobowe bez nadzoru, także wtedy, kiedy stanowisko komputerowe jest wyłączone lub wylogowane, a dokumentacja papierowa umieszczona w zamkniętej szafie.
- 6) § 55 otrzymuje brzmienie:
1. Pracownicy oraz, gdy jest to wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią podlegają szkoleniu w zakresie bezpieczeństwa informacji.
 2. Tematyka szkolenia powinna obejmować w szczególności:
 - 1) aktualny system prawny bezpieczeństwa informacji w Polsce i Unii Europejskiej,
 - 2) wewnętrzne regulacje związane z bezpieczeństwem informacji w Zespole,

- 3) *zagrożenia dla bezpieczeństwa przetwarzanych informacji, w odniesieniu do specyfiki działalności Zespołu,*
 - 4) *role i zadania poszczególnych osób odpowiedzialnych za bezpieczeństwo informacji,*
 - 5) *zasady udzielania dostępu do informacji i danych osobowych,*
 - 6) *zasady przetwarzania informacji w systemach teleinformatycznych,*
 - 7) *procedury postępowania w sytuacji naruszenia bezpieczeństwa przetwarzanych informacji,*
 - 8) *odpowiedzialność dyscyplinarna i karna za nieprzestrzeganie zasad bezpieczeństwa informacji.*
3. *Zapoznanie pracownika z aktami prawnymi – powszechnymi i wewnętrznymi obowiązującymi w Zespole – musi przybrać formę udostępnienia tych dokumentów na czas niezbędny do osobistego zapoznania z ich treścią.*
 4. *Szkolenie przeprowadza Dyrektor lub wyznaczony przez Dyrektora pracownik.*
 5. *Szkolenie, w zależności od potrzeb, może zostać przeprowadzone w formie tradycyjnego wykładu lub kursu e-learningowego.*
 6. *Udział w szkoleniu powinien zostać potwierdzony własnoręcznym podpisem uczestnika lub innym niezaprzeczalnym dowodem jego odbycia.*
 7. *Niedopuszczalne jest, aby szkolenie polegało jedynie na zapoznaniu się osoby z aktami prawnymi bez ich objaśnienia i odniesienia do specyfiki przetwarzania informacji w Zespole. W takim przypadku szkolenie zostanie uznane za nieskuteczne.*
 8. *Szkolenie powinno być uzupełnione indywidualnymi szkoleniami stanowiskowymi, przeprowadzanymi przez bezpośrednich przełożonych tak, aby zdobytą ogólną wiedzę przełożyć na szczególną specyfikę zakresu zadań danej osoby.*
- 7) *skreśla się § 67,*
 - 8) *§ 68 ust. 1 otrzymuje brzmienie: Przynajmniej raz w roku zespół ds. zarządzania ryzykiem przeprowadza szacowanie ryzyka w bezpieczeństwie informacji i ryzyka naruszenia praw i wolności osoby, której dane osobowe dotyczą, mając na uwadze utratę integralności, poufności i dostępności informacji, na zasadach określonych w „Procedurze zarządzania ryzykiem w bezpieczeństwie informacji”,*
 - 9) *dodaje się § 77 w brzmieniu: Dokumentacja systemu zarządzania bezpieczeństwem informacji podlega bezwzględnej tajemnicy.*
2. *„Procedura kontroli dostępu” otrzymuje brzmienie jak w załączniku nr 1 do zarządzenia.*
 3. *„Procedura pracy na odległość” otrzymuje brzmienie jak w załączniku nr 2 do zarządzenia.*
 4. *„Procedura korzystania ze środków wymiany informacji” otrzymuje brzmienie jak w załączniku nr 3 do zarządzenia.*
 5. *„Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji” otrzymuje brzmienie jak w załączniku nr 4 do zarządzenia.*

6. Upoważnienia do przetwarzania danych osobowych nadane przed wejściem w życie zarządzenia pozostają w mocy. Z chwilą nadania nowych upoważnień automatycznie tracą ważność – nie mają tu zastosowania zasady odwołania upoważnień określone w „Procedurze kontroli dostępu”.

§ 3.

Poszczególne paragrafy i załączniki, także przywołane w treści załącznika do zarządzenia nr 8/2015 z dnia 11 czerwca 2015 roku, zostają odpowiednio przenieumerowane, aby zachować ciągłość numeracji.

§ 4.

1. W „Procedurze zarządzania ryzykiem” § 1 ust. 3 otrzymuje brzmienie: *„Procedura” nie ma zastosowania dla zarządzania ryzykiem w bezpieczeństwie informacji i ryzykiem naruszenia praw i wolności osoby, której dane osobowe dotyczą.*
2. W „Procedurze zarządzania ryzykiem w bezpieczeństwie informacji”:
 - 1) § 1 ust. 1 otrzymuje brzmienie: *„Procedura zarządzania ryzykiem w bezpieczeństwie informacji”, zwana w dalszej części „Procedurą”, określa zasady przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji i ryzyka naruszenia praw i wolności osoby, której dane osobowe dotyczą oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, w Zespole Szkół nr 2 w Rybniku,*
 - 2) § 1 ust. 2 pkt 2) otrzymuje brzmienie: *ryzyku – należy przez to rozumieć ryzyko w bezpieczeństwie informacji i ryzyko naruszenia praw i wolności osoby, której dane osobowe dotyczą.*

§ 5.

Nadzór nad realizacją zarządzenia sprawuje Dyrektor.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.