

RK. 1710. 8. 2024

RADA POWIATU BYDGOSKIEGO

ul. Juliusza Słowackiego 3

85-008 Bydgoszcz

Bydgoszcz, dnia 2024 -09- 19

OR-III.1711. 6. 2024

**Przewodniczący
Rady Powiatu Bydgoskiego**

Zarząd Powiatu Bydgoskiego

**Kierownik jednostki kontrolowanej:
Starosta Bydgoski**

Na podstawie § 16 ust. 2 Regulaminu Komisji Rewizyjnej Rady Powiatu Bydgoskiego stanowiącego załącznik do Statutu Powiatu Bydgoskiego (Dz. Urz. Woj. Kuj.-Pom. z 2024 r. poz. 2442) przekazuję w załączeniu odpis protokołu z „Kontroli systemu i procedur ochrony danych osobowych w Starostwie Powiatowym w Bydgoszczy w okresie 2021 – 2023”.

Jednocześnie informuję, że zgodnie z § 16 ust. 3 ww. Regulaminu Komisji Rewizyjnej „Zarząd/kierownik jednostki kontrolowanej ma prawo zgłaszania uwag i wyjaśnień do protokołu w terminie 7 dni od daty jego otrzymania”.

Przewodniczący Komisji Rewizyjnej
Rady Powiatu Bydgoskiego

Zenon Rydelski

schowane.
24 września 2024
STAROSTA BYDGOSKI
Piotr Kozłowski

RK
B. KALIŃSKA
25.09.2024

Starosta Powiatu

Karol Czerkawski

Otrzymują:

- 1) Adresat
- 2) a/a

Protokół został omówiony na posiedzeniu
Zarządu Powiatu w dniu 8.10.2024r.

**KIEROWNIK
Referatu Kadr**

Barbara Kalińska

PROTOKÓŁ POKONTROLNY NR 1/2024

1) Podstawa prawna.

Plan pracy Komisji Rewizyjnej Rady Powiatu Bydgoskiego na 2024 r. stanowiący załącznik nr 1 do uchwały Nr 26/II/24 Rady Powiatu Bydgoskiego z dnia 24 czerwca 2024 r. w sprawie zatwierdzenia planów Komisji Rady Powiatu Bydgoskiego.

Upoważnienie wystawione przez Przewodniczącego Rady Powiatu Bydgoskiego do przeprowadzenia kontroli (znak: OR-III.1711.6.2024 z 13 sierpnia 2024 r.).

2) Przedmiot kontroli.

Kontrola systemu i procedur ochrony danych osobowych w Starostwie Powiatowym w Bydgoszczy w okresie 2021 -2023.

3) Skład zespołu kontrolującego.

Grzywacz Iwona	- Przewodniczący zespołu kontrolującego
Dobek Maciej	- Członek zespołu kontrolującego
Kubiak Andrzej	- Członek zespołu kontrolującego

4) Miejsce i termin kontroli.

Starostwo Powiatowe w Bydgoszczy
ul. Juliusza Słowackiego 3, 85-008 Bydgoszcz

Data rozpoczęcia kontroli: 4 września 2024 r.

Data zakończenia kontroli: 10 września 2024 r.

5) Przebieg i opis stanu faktycznego.

Zespół kontrolujący realizował czynności kontrolne w siedzibie Starostwa Powiatowego w Bydgoszczy w dniu 10 września 2024 r. W trakcie kontroli wyjaśnienia składali:

- pan Karol Czerkowski – Sekretarz Powiatu,
- pani Barbara Kalińska – Inspektor Ochrony Danych, Kierownik Referatu Kadr.

Zespół skontrolował następujące dokumenty:

- a) Raport z Audytu Bezpieczeństwa Informacji z dnia 27 października 2021 r.
- b) Raport z Audytu Bezpieczeństwa Informacji z dnia 28 października 2022 r.
- c) Raport z Audytu Zgodnego z KRI z dnia 2 października 2023 r. wraz z załącznikiem: "Raport z testów socjotechnicznych symulujących ataki phishingowe"
- d) Zarządzenie Nr 27/2020 Starosty Bydgoskiego z dnia 29 września 2020 r. w sprawie wprowadzenia Dokumentacji Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Bydgoszczy wraz z załącznikiem "Dokumentacja Systemu Zarządzania Bezpieczeństwem"

- e) Sprawozdanie nr 2/2019/2020 z zadania "Audyt organizacyjny z uwzględnieniem przestrzegania obowiązujących procedur na wieloosobowym stanowisku ds. kadr"
- f) Dokumentacja związana ze szkoleniem z zakresu ochrony danych osobowych, które odbyło się w pierwszym półroczu 2024 w tym:
 - Listy obecności poszczególnych sesji treningowych,
 - Umowa z firmą organizującą szkolenie,
 - Konspekt szkolenia - Cyberbezpieczeństwo i działania socjotechniczne,
 - Agenda szkolenia,
 - opinia o firmie prowadzącej szkolenie.

W trakcie kontroli przedstawiciele Starostwa zwrócili uwagę, że jednostka nie korzysta z zewnętrznych instytucji by wypełnić obowiązki związane z ochroną danych osobowych. Wszystkie zadania z tego zakresu prowadzone są we własnym zakresie. Osobą odpowiedzialną za bezpieczeństwo danych jest Starosta jako Administrator Danych. Administratora w realizacji zadań wspiera Inspektor Ochrony Danych. Innymi osobami funkcyjnymi odpowiedzialnymi za bezpieczeństwo danych w poszczególnych obszarach przetwarzania są dyrektorzy wydziałów Starostwa.

Zespół kontrolujący został poinformowany, że co roku procedury Starostwa dotyczące ochrony danych są sprawdzane przez zewnętrzną firmę. W ramach sprawdzenia odbywa się też audyt, który każdorazowo obejmuje inny zakres związany z ochroną danych. Po kontroli sporządzany jest raport, który nie jest upubliczniany w BIP. W dalszej części kontroli zespół zapoznał się z raportami wykonanymi w latach 2021-2023.

Przeanalizowano tematy związane z wewnętrznymi sposobami kontrolowania i audytowania pracowników. Zespół został poinformowany, że IOD wraz z odpowiednimi strukturami Starostwa (IT, dyrektorzy wydziałów) sprawdza czy pracownicy Starostwa w codziennej pracy przestrzegają procedur (polityka czystego biurka, polityka kluczy, polityka postępowania z nośnikami danych). Tego typu kontrole odbywają się przez cały rok ale nie są dokumentowane.

W ciągu roku odbywają się również szkolenia przypominające o zasadach RODO. Szkolenia odbywają się także w przypadku zmiany przepisów. Zespół zapoznał się z dokumentacją związaną z jednym ze szkoleń, które odbyło się w pierwszej połowie roku 2024. Sprawdzone m.in. tematykę szkolenia oraz listę przeszkolonych pracowników.

W trakcie kontroli omówiono także zasady związane z zatrudnianiem nowych pracowników - etap rekrutacji (postępowanie z przesłanymi CV oraz kwestionariuszami osobowymi) oraz szkolenia nowych pracowników z zasad RODO.

Przeanalizowano szczegółowo poszczególne polityki ochrony danych - zasady pracy z nośnikami danych, politykę kluczy, politykę pracy zdalnej. Poruszono również temat analizy ryzyk związanych z ochroną danych osobowych wraz z głównymi ryzykami oraz działaniami mającymi to ryzyko obniżyć.

Jednym z przedmiotów kontroli był również wpływ stopni alarmowych na terenie RP na działanie Starostwa w zakresie ochrony danych, w tym kwestie związane z ochroną serwerów i innych sprzętów IT.

6) Wykaz nieprawidłowości ustalonych przez zespół z podaniem dowodów, a zwłaszcza dokumentów, wyjaśnień, oględzin dokonanych w trakcie kontroli.

Zespół kontrolujący nie stwierdził nieprawidłowości pozytywnie oceniając stan ochrony danych osobowych w Starostwie Powiatowym.

7) Uwagi oraz propozycje wniosków i zaleceń.

Zespół zwrócił uwagę, że część działań związanych z wewnętrznymi kontrolami ad-hoc powinno być dokumentowane.

8) Adnotacja o zapoznaniu z protokołem Zarząd/kierownika kontrolowanej jednostki potwierdzoną podpisem.

Starosta Bydgoski

STAROSTA BYDGOSKI
Piotr Kozłowski

9) Wykaz załączników.

Brak.

10) Podpisy członków zespołu kontrolującego.

Grzywacz Iwona

Dobek Maciej

Kubiak Andrzej

Grzywacz Iwona
Dobek Maciej
Kubiak Andrzej

Stwierdzam
w zgodności z oryginałem

Bydgoszcz, dnia 2024-09-19

Główny Specjalista
ds. obsługi Rady Powiatu
oraz spraw obywatelskich

Paulina Wengler

1955