Prezydent Miasta
Skarżyska-Kamiennej

Skarżysko – Kamienna, dnia 01.09.2023 r.

KA.1710.1.2023

Świętokrzyski Urząd Wojewódzki
25-516 Kielce
Aleja IX Wieków Kielc 3

W nawiązaniu do wystąpienia pokontrolnego z dnia 2.08.2023r. (Znak:OK.V.431.4.2023MT) dotyczącego przeprowadzonej kontroli w Urzędzie Miasta w Skarżysku – Kamiennej – kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych, przedkładam informację o sposobie wykorzystania uwag i wniosków wskazanych w wyżej wymienionym wystąpieniu:

1. **rozszerzenie dokumentacji o ochronę danych innych niż dane osobowe**

Zasady zarządzania bezpieczeństwem informacjami w Urzędzie Miasta w Skarżysku – Kamiennej, zostały określone przez Prezydenta Miasta Zarządzeniem nr 358/2019 z dnia 12 grudnia 2019 r. w sprawie zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miasta w Skarżysku – Kamiennej. Prezydent Miasta ww. Zarządzeniem wprowadził :

- Politykę Ochrony Danych Osobowych (PODO), która określiła regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych oraz ich zabezpieczenia zarówno przetwarzanych tradycyjnie, jak i w systemie informatycznym.
- Instrukcję Zarządzania Systemem Informatycznym, która stanowi integralna część Polityki bezpieczeństwa i określa sposób zarządzania systemem informatycznym.

Zespól ds. Zarządzania Bezpieczeństwem Informacji jest w trakcie opracowywania regulacji dotyczących zapewnienia bezpieczeństwa wszystkich informacji przetwarzanych w Urzędzie.

2. **regularne przeglądanie i aktualizowanie dokumentacji z ochrony danych**

Zgodnie z postanowieniami PODO Zespól ds. Zarządzania Bezpieczeństwem Informacji, powołany przez Prezydenta Miasta Skarżyska – Kamiennej, Zarządzeniem nr 366/2018 dokonuje okresowych przeglądów ww. dokumentacji, nie potwierdzając tego faktu pisemnie. Fakt dokonywania przeglądów dokumentacji, będzie dokumentowany w formie pisemnej.

Jednocześnie informuję, że oczywista omyłka pisarska dot. numeracji rozdziałów w Polityce Ochrony Danych Osobowych została poprawiona (zmiana nie wpłynęła na treść zapisów regulacji).

3. **proces analizy ryzyka**

Proces analizy zagrożeń związanych z przetwarzaniem informacji zostanie przeprowadzony przez Zespół ds. Zarządzania Bezpieczeństwem Informacji na zasadach i w trybie określonym w procedurach zarządzania ryzykiem w Urzędzie Miasta w Skarżysku – Kamiennej.

4. **proces odbierania uprawnień**

Procedurę nadawania oraz odbierania uprawnień do przetwarzania danych i ich rejestrowanie w systemie informatycznym określa Polityka Ochrony Danych Osobowych (procedura nadawania, modyfikowania oraz odbierania upoważnień i uprawnień) oraz Instrukcja Zarządzania Systemem Informatycznym. Podstawę nadania uprawnień pracownikom stanowi upoważnienie do przetwarzania danych osobowych, które jest

nadawane tylko i wyłącznie w zakresie wykonywanych przez pracownika zadań, na podstawie wniosku bezpośredniego przełożonego i aktualnego zakresu obowiązków. Upoważnienie do przetwarzania danych osobowych oraz uprawnienia do pracy w systemie informatycznym są przekazywane uprawnionym na piśmie (na wzorach określonych w PODO i IZSI). Nadzór i kontrolę nad procesem rejestracji uprawnień w systemie informatycznym sprawuje Kierownik Zespołu Informatycznego. Każdorazowo pracownik, któremu dokonano zmiany zakresu przetwarzania danych (zakresu obowiązków), w tym w systemie informatycznym otrzymuje przed rozpoczęciem pierwszej czynności we wnioskowanym zakresie zmienione upoważnienie (lub uprawnienie).

Zgodnie z przyjętymi procedurami określono sposób odbierania uprawnień pracownikom, którzy kończą pracę w Urzędzie Miasta. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy z pracownikiem. Jak wynika z przyjętych procedur (zapisy PODO) - obligatoryjnym wygaśnięciem upoważnienia lub uprawnienia następują m.in. w przypadku przesunięcia pracownika na inne stanowisko pracy; rozwiązania stosunku pracy. Po wygaśnięciu nadanego upoważnienia/uprawnienia informatyk ma obowiązek zablokować konto użytkownika w systemie informatycznym.

W ramach zarządzania uprawnieniami chronologicznie prowadzony jest rejestr osób upoważnionych do przetwarzania danych osobowych oraz rejestr użytkowników systemu. Wszelkie zmiany ww. rejestrach są odnotowywane na podstawie informacji przekazywanych przez komórkę prowadzącą kadry w Urzędzie (ustanie zatrudnienia, przeniesienie pracownika na inne stanowisko oraz numer kolejnego upoważnienia). Ponadto zobowiązano kierowników komórek organizacyjnych właściwego przestrzegania zasad nadawania i odbierania uprawnień pracownikom w kierowanych przez nich komórkach organizacyjnych.

5. szkolenia z bezpieczeństwa informacji

Przepisy nie określają jednoznacznie, jak często powinno być przeprowadzane szkolenie pracowników z zakresu ochrony danych . Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniu w trakcie, którego wszyscy uczestnicy są zapoznawani z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz obowiązującymi w Urzędzie Miasta procedurami wewnętrznymi (w tym dotyczącymi bezpieczeństwa systemów informatycznych). Tematyka szkoleń jest przygotowywana przez Inspektora Ochrony Danych w uzgodnieniu z Kierownikiem Zespołu Informatycznego. Ponadto pracownicy uczestniczą w szkoleniach merytorycznych (z zakresu wykonywanej pracy) organizowanych przez firmy zewnętrzne, na których trenerzy omawiają z uczestnikami zasady bezpieczeństwa informacji w zakresie objętym tematyką szkoleniem (potwierdzenie programy szkoleń).

Informuję, że w miesiącu lipcu i sierpniu br. wszyscy pracownicy Urzędu zostali w szkoleni z zakresu cyberbezpieczeństwa, z elementami ochrony danych osobowych. Szkolenie zostało zakończone egzaminem, którego wyniki będą przechowywane w aktach osobowych pracowników.

6. procedura pracy zdalnej i zasady dostępu do prac zdalnej pracowników

Praca na odległość i mobilne przetwarzanie danych – procedura ochrony danych osobowych spoza obszarem przetwarzania (dot. dokumentacji papierowej, komputerów przenośnych) została

określona w PODO. W celu przeciwdziałania COVID-19 i jego rozpowszchniania wprowadzono w Urzędzie możliwość wykonywania pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (pracę zdaną). Warunki i zasady pracy zdalnej określa instrukcja pracy zdalnej przyjęta Zarządzeniem Nr 260/2020 Prezydenta Miasta Skarżyska – Kamiennej z dnia 5 października 2020 r. Rozwiązanie to było jednak rozwiązaniem czasowym, wprowadzonym na okres trwania pandemii. Nowe regulacje o pracy zdalnej, wskazane Kodeksem pracy zostaną uregulowane w regulaminie pracy.

7. **okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji.**

Plan audytu na rok 2023 uwzględnia przeprowadzenie zadania zapewniającego w obszarze bezpieczeństwa informacji (zgodnie z KRI).

8. **wykonywanie kopii zapasowych i prowadzenie ewidencji**

Przedstawiony w trakcie kontroli rejestr taśm zawiera numery seryjne taśm użytkowanych w automatycznej bibliotece, oprogramowanie do wykonywania backapów tworzy automatycznie logi systemowe dotyczące zdarzeń określając: jednoznacznie kiedy dany backup został wykonany, rejestrując jednocześnie status jego wykonania.

W związku z powyższym prowadzenie odrębnego rejestru i powielanie w/w zapisów zostanie poddane analizie oraz uszczegółowieniu w dokumentacji IZSI.

9. **usuniecie z pomieszczenia serwerowi nieużywanego sprzętu**

Ze względu na podwójną przeprowadzkę tj. do siedziby tymczasowej oraz powrót do siedziby pierwotnej - w serwerowniach były chwilowo przechowywany sprzęt wycofany z użytkowania, W trakcie oględzin prowadzonych przez kontrolę trwały prace porządkowe, które ze względu na ograniczone zasoby ludzkie rozłożone są w czasie.
Serwerownia została uporządkowana.

10. **dokumentowanie testów przywracania funkcjonowania systemów informatycznych po awarii**

Podobnie jak w pkt 8, istnieją zapisy w logach systemowych odnośnie przywracanych kopii zapasowych, dlatego też nie jest prowadzona w/w dokumentacja. Wymaga uszczegółowienia w dokumentacji IZSI.

11. **przeglądanie logów systemowych**

Ze względu na mnogość systemów zastosowano zakupiony w ramach projektu „ Cyfrowa Polska" oprogramowanie SIEM/SOAR umożliwiające pełną skuteczną analizę logów. Oprogramowanie to jest na etapie wdrażania i uwzględnia kontrolowane systemy . Użytkowany jest także Fortianlizer celem analizy ruchu przychodzącego i wychodzącego, nie mniej nie dotyczy to kontrolowanych systemów.

12. **Poprawienie obsługi stron internetowych za pomocą klawiatury**

Uchybienia przekazano do projektantów stron celem naniesienia stosownych poprawek.

z up. Prezydenta Miasta
Krzysztof Myszka
Zastępca Prezydenta Miasta