Zarządzenie Nr 17/2020
Starosty Kętrzyńskiego
z dnia 28 lutego 2020 r.

o zmianie Zarządzenia Nr 79/2019 Starosty Kętrzyńskiego z dnia 29 października 2019 r. w sprawie wprowadzenia dokumentacji zapewniającej ochronę przetwarzania danych osobowych w Starostwie Powiatowym w Kętrzynie wraz z opisem środków technicznych i organizacyjnych stosowanych w jednostce.

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2019 r. poz. 511 z późn. zm.), ***zarządzam co następuje:***

§ 1.

W załączniku nr 1 do Zarządzenia Nr 79/2019 Starosty Kętrzyńskiego z dnia 29 października 2019 r. w sprawie wprowadzenia dokumentacji zapewniającej ochronę przetwarzania danych osobowych w Starostwie Powiatowym w Kętrzynie wraz z opisem środków technicznych i organizacyjnych stosowanych w jednostce wprowadza się następujące zmiany:

1. Punkt 3.2 otrzymuje brzmienie:

   „ **OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)**
   W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator przetwarzający dane osobowe (patrz załącznik nr 1 Wykaz zbiorów danych osobowych) zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy zapewnić, że:
   1. dane te są legalnie przetwarzane (na podstawie art. 6, 9),
   2. dane te są adekwatne w stosunku do celów przetwarzania,
   3. dane te są przetwarzane przez określony czas (retencja danych),
   4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
   5. opracowano klauzule informacyjne dla powyższych osób (patrz załącznik nr 3 Klauzule informacyjne),
   6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28) zgodnie z załącznikiem nr 4 Umowa powierzenia (wykaz podmiotów przetwarzających prowadzony jest w załączniku nr 5 Rejestr umów powierzenia). Administrator sprawuje nadzór nad powierzonymi danymi osobowymi (załącznik nr 4a).
   7. potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w załączniku nr 1 Wykaz zbiorów danych osobowych."

2. Punkt 13 otrzymuje brzmienie:

   „**13 SPIS ZAŁĄCZNIKÓW**
   1. Załącznik nr 1 - Wykaz zbiorów danych osobowych (rejestr czynności przetwarzania/arkusz oceny skutków/arkusz analizy ryzyka)
   2. Załącznik nr 2 - Lista potencjalnych aktywów
   3. Załącznik nr 3 – Klauzula informacyjna
   4. Załącznik nr 4 – Umowa powierzenia
   5. Załącznik nr 4a – Ankieta dla podmiotów przetwarzających
   6. Załącznik nr 5 – Rejestr umów powierzenia
   7. Załącznik nr 6 – Lista potencjalnych zagrożeń
   8. Załącznik nr 7 – Lista potencjalnych zabezpieczeń
   9. Załącznik nr 8 – Arkusz analizy ryzyka
   10. Załącznik nr 9 – Upoważnienie do przetwarzania danych osobowych
   11. Załącznik nr 10 – Ewidencja osób upoważnionych

12. Załącznik nr 11 – Formularz rejestracji incydentu
13. Załącznik nr 12 – Regulamin ochrony danych osobowych
14. Załącznik nr 13 – Oświadczenie o poufności
15. Załącznik nr 14 – Plan szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych
16. Załącznik nr 15 – Szkolenie wewnętrzne RODO
17. Załącznik nr 16 – Procedura projektowania nowych procesów
18. Załącznik nr 17 – Rejestr czynności prowadzony przez Podmiot przetwarzający
19. Załącznik nr 18 – Procedura audytu
20. Załącznik nr 19 – Plan ciągłości działania
21. Załącznik nr 20 – Wykaz zabezpieczeń RODO."

3. Do Polityki Ochrony Danych Osobowych w Starostwie Powiatowym w Kętrzynie, wprowadzonej zarządzeniem nr 79/2019 Starosty Kętrzyńskiego z dnia 29 października 2019 r., dodaje się załącznik nr 4a - Ankieta dla podmiotów przetwarzających, stanowiący załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi z życiem z dniem podpisania.

STAROSTA

Michał Kochanowski

Sporządziła: Agata Kowalska-Skórka

Uzgodniono pod względem formalno-prawnym
Ewelina Łukaszewicz
radca prawny

Załącznik Nr 4a
Do Polityki Ochrony Danych Osobowych
w Starostwie Powiatowym w Kętrzynie
wprowadzonej Zarządzeniem nr 79/2019
Starosty Kętrzyńskiego z dnia 29 października 2019 r.

ANKIETA SPEŁNIENIA WYMOGÓW BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZEZ PODMIOT PRZETWARZAJACY

Działając na podstawie Artykułu 28 pkt 3 lit h) Ogólnego Rozporządzenia o ochronie danych osobowych działając, jako administrator danych osobowych przekazanych Państwu jako podmiotowi przetwarzającemu, wnosimy o udzielenie odpowiedzi na poniższe pytania poprzez zakreślenie odpowiedniej odpowiedzi kółkiem lub w przypadku wypełniania elektronicznego podkreślenia tekstu i odesłanie wypełnionej i podpisanej przez Państwa jednostkę ankiety w formie skanu, zwrotnie na adres mailowy, z którego otrzymali ją Państwo, lub w formie papierowej na adres siedziby naszej jednostki w terminie do 30 dni od daty jej otrzymania.

1. **Oznaczenie podmiotu (nazwa, adres, NIP, REGON)** .....

2. **Zdalny dostęp i VPN: Metoda Dostępu**
   a) Nie wdrożone: Różne metody dostępu i związane z nimi procesy; Brak kontroli poświadczeń dostępu; Nieograniczony dostęp do sieci;
   b) Częściowo wdrożone: Jednolita metodologia dostępu i związany z nią proces wymagający uwierzytelnienia; Nazwy użytkowników i hasła są współdzielone; Dostęp do wydzielonego segmentu sieci;
   c) Wdrożone: Jednolita metodologia dostępu i związany z nią proces wymagający uwierzytelniania wieloskładnikowego; Unikalne nazwy użytkowników i hasła; Dostęp tylko do wymaganych docelowych zasobów;

3. **Zdalny dostęp i VPN: Szyfrowanie**
   a) Nie wdrożone: Brak szyfrowania
   b) Częściowo wdrożone: Szyfrowanie przy użyciu przestarzałych standardów
   c) Wdrożone: Szyfrowanie przy użyciu aktualnych i bezpiecznych standardów

4. **Zdalny dostęp i VPN: Audyt**
   a) Nie wdrożone: Brak dziennika audytu lub audyt, który może być wyłączony, usunięty lub zmieniony przez użytkownika
   b) Częściowo wdrożone: Obowiązkowy dziennik audytu z ograniczonym zakresem i szczegółami
   c) Wdrożone: Obowiązkowy dziennik audytu rejestrujący uwierzytelnianie użytkowników, czas sesji i główne działania (jeśli uznać że logi z Cisco spełniają te wymagania)

5. **Ochrona urządzeń końcowych: Antywirus**
   a) Nie wdrożone: Brak ochrony antywirusowej

b) Częściowo wdrożone: Brak centralnie zarządzanego rozwiązania (możliwość występowania różnych narzędzi lub różnych zasad ochrony dla tych samych narzędzi)

c) Wdrożone: Wdrożony centralnie zarządzany program antywirusowy na wszystkich urządzeniach końcowych, do których stosuje się obowiązujące zasady

6. **Ochrona urządzeń końcowych: Ochrona przed złośliwym oprogramowaniem (malwarem)**

a) Nie wdrożone: Brak ochrony przed złośliwym oprogramowaniem na urządzeniach końcowych

b) Częściowo wdrożone: Ochrona przed złośliwym oprogramowaniem na bazie sygnatur. Brak behawioralnej ochrony przed złośliwym oprogramowaniem (testowanie zachowania plików); Użytkownicy mogą: a) umieścić na czarnej liście znane złośliwe strony, b) skanować urządzenie końcowe pod kątem złośliwych treści, c) filtrować zawartość

c) Wdrożone: Ochrona przed złośliwym oprogramowaniem na bazie sygnatur jak i zachowania plików (ochrona behawioralna); Centralnie egzekwowane polityki a) umieszczanie na czarnej liście znanych złośliwych witryn, b) skanowanie w poszukiwaniu złośliwych treści na wszystkich urządzeniach końcowych, c) filtrowanie treści

7. **Ochrona urządzeń końcowych: Aktualizacje**

a) Nie wdrożone: Brak aktualizacji

b) Częściowo wdrożone: Brak możliwości centralnej instalacji i weryfikacji, czy aktualizacje są obecne na urządzeniach końcowych. Zaktualizowane oprogramowanie antywirusowe i antymalware nie jest wymagane by uzyskać dostęp do sieci.

c) Wdrożone: Aktualizacje są sprawdzane i instalowane za pomocą scentralizowanych narzędzi i polityk, możliwość sprawdzania statusu i raportowania. Udane połączenia do sieci wymaga posiadania zaktualizowanego oprogramowania zapobiegającego złośliwemu oprogramowaniu i antywirusowego o zielonym statusie (oznaczającym, że nie wykryto żadnego złośliwego oprogramowania ani wirusa).

8. **Zarządzanie dostępem i hasła: Dostęp do budynków i obszarów wrażliwych**

a) Nie wdrożone: Brak procedur ograniczających dostęp fizyczny

b) Częściowo wdrożone: Określono zasady monitorowania dostępu do budynków

c) Wdrożone: Wprowadzono politykę monitorowania dostępu do budynków i obszarów wrażliwych

9. **Zarządzanie dostępem i hasła: Dostęp do systemów**

a) Nie wdrożone: Zasady zarządzania dostępem nie są zdefiniowane

b) Częściowo wdrożone: Zasady zarządzania dostępem są zdefiniowane, dzięki czemu informacje są udostępniane w zależności od potrzeb.

c) Wdrożone: Wdrożona jest polityka zarządzania dostępem, zapewniająca dzielenie się informacjami w oparciu o regułę "Musi Wiedzieć" ("Need-to-know"), a użytkownicy są identyfikowani w sposób unikalny. Wyjątki są monitorowane i uzasadnione.

10. Zarządzanie dostępem i hasła: Polityka haseł

a) Nie wdrożone: Polityka haseł nie jest zdefiniowana
b) Częściowo wdrożone: Polityka haseł jest zdefiniowana
c) Wdrożone: Silna polityka haseł jest egzekwowana we wszystkich systemach i aplikacjach

11. Zarządzanie dostępem i hasła: Uprawnienia administracyjne

a) Nie wdrożone: Wszyscy użytkownicy są administratorami
b) Częściowo wdrożone: Większość użytkowników nie jest administratorami
a) Wdrożone: Żadni użytkownicy nie są administratorami - rola wymaga eskalacji lub oddzielnego logowania

12. Zarządzanie dostępem i hasła: Logi audytowe

a) Nie wdrożone: Logi audytowe nie są monitorowane
b) Częściowo wdrożone: Procedury wprowadzają do logów audytowych informacje o modyfikacji danych osobowych
c) Wdrożone: Procedury wprowadzają do logów audytowych informacje o modyfikacji danych osobowych oraz o dostępie do nich, określony jest okres przechowywania danych, a niezależny departament (zespół) dokonuje przeglądów logów i okresów przechowywania danych, zapewniając jednocześnie rozdział obowiązków w tym zakresie.

13. Zasady zarządzania lukami (vulnerabilities) i ich usuwanie (patching): Polityka aktualizacji systemów operacyjnych (Windows, Linux itp.)

a) Nie wdrożone: Konfiguracja domyślna lub nieistniejąca
b) Częściowo wdrożone: Instalacje aktualizacji zgodnie z regułą "najlepiej jak to możliwe" ("Best effort")
c) Wdrożone: Istnieje polityka / standard wymagająca by wszystkie poprawki wgrywane były w ciągu 30 dni od ich wydania

14. Zasady zarządzania lukami (vulnerabilities) i ich usuwanie (patching): Polityka aktualizacji aplikacji i dodatków (np. DB, Office, Java, Adobe, Flash, ...)

a) Nie wdrożone: Konfiguracja domyślna lub nieistniejąca
b) Częściowo wdrożone: Instalacje aktualizacji zgodnie z regułą "najlepiej jak to możliwe" ("Best effort")

c) Wdrożone: Istnieje polityka / standard wymagająca by wszystkie poprawki wgrywane były w ciągu 30 dni od ich wydania.

15. Zasady zarządzania lukami (vulnerabilities) i ich usuwanie (patching): Proaktywne zarządzanie podatnościami

a) Nie wdrożone: Brak
b) Częściowo wdrożone: Roczne skanowanie środowiska
c) Wdrożone: Kwartalny skan środowiska z poprawkami instalowanymi w ciągu 60 dni

16. Kopie zapasowe, archiwizacja, odzyskiwanie, przechowywanie i czyszczenie danych: Polityka kopii zapasowych

a) Nie wdrożone: Kopie zapasowe wykonywane są dla krytycznych aplikacji
b) Częściowo wdrożone: Kopie zapasowe wykonywane są dla krytycznych aplikacji, a testy ich odzyskiwania przeprowadzane są nieregularnie
c) Wdrożone: Kopie zapasowe wykonywane są dla aplikacji, a testy ich odzyskiwania wykonywane są co najmniej 1 raz w roku

17. Kopie zapasowe, archiwizacja, odzyskiwanie, przechowywanie i czyszczenie danych: Polityka retencji i archiwizacji

a) Nie wdrożone: Brak polityki archiwizacji lub rozproszona dokumentacja dotycząca procedur archiwizacji
b) Częściowo wdrożone: Zaimplementowana jest polityka archiwizacji i zdefiniowane okresy przechowywania
c) Wdrożone: Zasady archiwizacji i przechowywania są zaimplementowane, są zarządzane centralnie, łącznie z mechanizmami usuwania danych

18. Kopie zapasowe, archiwizacja, odzyskiwanie, przechowywanie i czyszczenie danych: Polityka niszczenia informacji

a) Nie wdrożone: Brak polityki niszczenia informacji
b) Częściowo wdrożone: Określono politykę niszczenia informacji obejmującą przechowywanie papieru i nośników elektronicznych
c) Wdrożone: Wprowadzono politykę niszczenia informacji, obejmującą przechowywanie papieru i nośników elektronicznych dla wszystkich urządzeń, a informacja niszczona jest w sposób nieodwracalny.

19. **Zarządzanie incydentami: Pisemny proces zarządzania incydentami, który obejmuje naruszenie danych lub utratę danych**
    a) Nie wdrożone: Brak, incydenty są zarządzane na zasadzie ad-hoc – a przynajmniej ja nic o tym nie wiem
    b) Częściowo wdrożone: Obowiązki są zdefiniowane, ale procedury i skrypty do zarządzania incydentami nie są udokumentowane
    c) Wdrożone: Istnieje dobrze zdefiniowany i udokumentowany proces zarządzania incydentami bezpieczeństwa obejmujący incydenty różnego typu i testowany corocznie

20. **Zarządzanie incydentami: Utrzymanie procesu rejestrowania incydentów lub nagrywania**
    a) Nie wdrożone: Brak, brak rejestracji incydentów
    b) Częściowo wdrożone: Istnieje, Oparty o arkusz kalkulacyjny lub w podobny sposób
    c) Wdrożone: Centralne ustrukturyzowane repozytorium do śledzenia drobnych i poważnych incydentów

21. **Audyty bezpieczeństwa i certyfikacja: Audyty bezpieczeństwa wykonywane wewnętrznie**
    a) Nie wdrożone: Brak
    b) Częściowo wdrożone: Przeprowadzono roczny przegląd bezpieczeństwa
    c) Wdrożone: Coroczny przegląd bezpieczeństwa przeprowadzany przez personel spoza IT

22. **Audyty bezpieczeństwa i certyfikacja: Audyty bezpieczeństwa wykonywane przez zewnętrznych doradców**
    a) Nie wdrożone: Brak
    b) Częściowo wdrożone: Wykonany w ciągu ostatnich 3 lat i obejmujący całą infrastrukturę – trzeba by go jednak zrobić
    c) Wdrożone: Wykonywany corocznie dla całej infrastruktury, początkujący utworzenie planu naprawczego

23. **Audyty bezpieczeństwa i certyfikacja: Certyfikaty bezpieczeństwa firmy i pracowników**
    a) Nie wdrożone: Brak
    b) Częściowo wdrożone: Przynajmniej jedna certyfikacja związana z bezpieczeństwem (np. CISSP, CISM, ISO27000) w zespole IT lub InfoSec
    c) Wdrożone: Przynajmniej jedna osoba z certyfikatem bezpieczeństwa w zespole odpowiedzialnym za bezpieczeństwo lub certyfikat ISO27000 firmy

24. **Kodeks postępowania i polityki: Istnienie kodeksu postępowania**

a) Nie wdrożone: Brak polityki dotyczącej zachowania jej pracowników lub istnieją rozproszone procedury
b) Częściowo wdrożone: Istnieje polityka prywatności i bezpieczeństwa informacji
c) Wdrożone: Wprowadzono kodeks postępowania, obejmujący kwestie prywatności i bezpieczeństwa informacji, wraz z regularnymi inicjatywami podnoszącymi świadomość.

25. Kodeks postępowania i polityki: Istnienie procesu zarządzania ryzykiem

a) Nie wdrożone: Brak procesu zarządzania ryzykiem
b) Częściowo wdrożone: Zarządzanie ryzykiem nie jest działaniem samoistnym, i zapewniane jest przez różne działy / departamenty
c) Wdrożone: Proces zarządzania ryzykiem jest wdrożony i jest poddawany przeglądom.

26. Kodeks postępowania i polityki: Istnienie zespołu ds. bezpieczeństwa informacji

a) Nie wdrożone: Brak zespołu ds. bezpieczeństwa informacji
b) Częściowo wdrożone: Istnieje zespół ds. Bezpieczeństwa informacji, jednakże raportuje do obszarów operacyjnych
c) Wdrożone: Zespół ds. Bezpieczeństwa informacji jest oddzielony od obszarów operacyjnych i raportuje do Kierownictwa Wyższego Szczebla.

27. Kodeks postępowania i polityki: Istnienie zespołu ds. danych osobowych

a) Nie wdrożone: Brak zespołu ds. danych osobowych.
b) Częściowo wdrożone: Istnieje świadomość dotycząca bezpieczeństwa danych osobowych, wspierana przez bezpieczeństwo prawne i informacji lub przez jeden z tych działów (zespołów)
c) Wdrożone: Zespół ds. Danych Osobowych istnieje, jest oddzielony od obszarów operacyjnych i raportuje do Kierownictwa Wyższego Szczebla.

Stan na dzień .....

Podpis osoby upoważnionej do reprezentowania jednostki.....

Pieczęć jednostki .....