Egz. Nr 2...

SPRAWOZDANIE

z

PRZEPROWADZONEGO

AUDYTU WEWNĘTRZNEGO

w *Urzędzie Starostwa Powiatowego*

w Lubaczowie

na temat: „Ochrona danych osobowych w Starostwie"

Data sporządzenia sprawozdania: *30 listopada 2021 r.*

P R Z E M Y Ś L

2021

Rozdział I

Informacje ogólne

1. WSTĘP

Zgodnie z *Programem zadania audytowego* „Wdrożenie RODO w Starostwie" z dnia 30 sierpnia 2021 r. *Audytor Wewnętrzny* – Lech CZERNECKI, *(uprawnienia nr 636/2004)* dokonał przeglądu w zakresie realizacji zadań związanych z ochroną danych osobowych realizowaną przez Urząd Starostwa Powiatowego w Lubaczowie w myśl obowiązujących przepisów prawa powszechnego.

Analizie poddano obowiązujące w jednostce przepisy prawa wewnętrznego dotyczące audytowanej problematyki.

Termin przeprowadzenia zadania audytowego został zaplanowany na okres od 26 sierpnia 2021 r. do 31 grudnia 2021 r.

Podmiotowy zakres audytu objął Urząd Powiatu Lubaczowskiego reprezentowany przez Inspektora Ochrony Danych Osobowych, zwany dalej „IOD".

W zakresie przedmiotowym audytu problematyka zadania audytowego dotyczyła funkcjonowania ochrony danych osobowych zgodnie z obowiązującymi w tej materii przepisami prawa powszechnego tj.

1) Ustawą z dnia 5 czerwca 1998r. o samorządzie powiatowym (Dz. U. z 2015 r., poz. 1445),
2) Rozporządzeniem PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

oraz stworzonych na ich podstawie przepisów prawa wewnętrznego.

2. PREZENTACJA CELÓW AUDYTU

Powyższe zadanie miało na celu analizę uregulowań wewnętrznych wprowadzonych w Starostwie a służących ochronie danych osobowych w Starostwie Powiatowym w Lubaczowie pod kątem ich zgodności z przepisami prawa powszechnego, spójności oraz aktualności.

W celu upewnienia się, że funkcjonujący system zapewnia Staroście Powiatu Lubaczowskiego racjonalną pewność osiągania celów postawionych jednostce, oceny stanu faktycznego dokonano w oparciu o analizę poszczególnych dokumentów stworzonych na podstawie Rozporządzania Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zawartych w nich treści oraz ich zgodności z obowiązującymi w tym względzie przepisami prawa.

Celem przedstawienia wyników przeprowadzonych czynności audytowych przyjęto następujący sposób ich oceny:

- Zgodność przepisów wewnętrznych w zakresie RODO z obowiązującymi przepisami,
- Aktualność zawartych treści w dokumentach.

3. STRESZCZENIE WYNIKÓW AUDYTU

Przeprowadzone czynności audytowe nie zidentyfikowały znaczących problemów w funkcjonowaniu ochrony danych osobowych w Starostwie Powiatowym w Lubaczowie.

Pewne niedociągnięcia wynikały bardziej z zawiłości przepisów w zakresie ochrony danych osobowych, różnych stanowisk osób szkolących na szkoleniach zewnętrznych czy z ograniczeń organizacyjnych czy finansowych.

Przeprowadzone czynności audytowe nie zidentyfikowały rażących przypadków naruszania Rozporządzenia o ochronie danych osobowych.

Rozdział II

1. *OGÓLNY OPIS DZIAŁALNOŚCI STAROSTWA W AUDYTOWANYM ZAKRESIE*

Przetwarzanie danych osobowych oznacza każdą czynność, która jest związana z ich użyciem. Przede wszystkim mówimy tutaj o zapisywaniu, kopiowaniu, czy też przechowywaniu ich w formie cyfrowej. RODO uzupełnia w tym zakresie zasady uzyskiwania zgody od osób fizycznych. Do podstawowych zasad należą zgoda na przetwarzanie danych osobowych musi być wyrażona konkretnemu podmiotowi; oświadczenie o udzieleniu zgody na przetwarzanie danych osobowych powinno być sformułowane w sposób prosty - tak aby jasno wynikała z niego zgoda na przetwarzanie danych; zgoda na przetwarzanie danych musi być dobrowolna oraz ze zgody musi wynikać cel, w jakim został udzielona, miejsce przetwarzania danych, a także okres przez jaki ona obowiązuje.

Oprócz tych zasad, osoba, która udziela zgody na przetwarzanie danych osobowych, powinna zostać poinformowana o tym, kto jest administratorem jej danych osobowym, a także o tym, że istnieje możliwość cofnięcia takiej zgody.

Obowiązkiem Starosty jest stosowanie się do zasad ochrony danych osobowych. W tym celu muszą być dobrane odpowiednie środki organizacyjne oraz techniczne, które umożliwią odpowiednie przechowywanie danych osobowych. Z przepisów rozporządzenia można wyodrębnić obowiązki, jakich muszą przestrzegać, a są to między innymi:

1. odpowiednie zabezpieczenie przechowywanych danych osobowych,
2. przekazywanie petentom, uczniom, pacjentom informacji na temat przetwarzania ich danych osobowych, a także pozwolenie na wgląd w zmianach tych danych,
3. uzyskanie zgodny na wykorzystanie danych osobowych,
4. prowadzenie dokumentacji przetwarzania danych,
5. wprowadzenie zasady przetwarzania danych tylko niezbędnych do określonej operacji,
6. zgłoszenie organowi nadzorczemu naruszenia bezpieczeństwa danych,
7. przedstawianie dokumentacji na żądanie organu nadzorczego, potwierdzającej przestrzeganie prawa,
8. przechowywanie dokumentów, które potwierdzają, kto wyraził zgodę na przetwarzanie danych osobowych, kiedy oraz w jakim zakresie.

Jednym z obowiązków wynikających z przepisów Rozporządzenia jest instytucja Inspektora Ochrony Danych Osobowych, którego głównymi obowiązkami będzie sprawdzanie zgodności procedur przyjętych w zakresie danych osobowych z wymaganiami rozporządzenia. Reasumując przepisy w zakresie RODO nie określają jak musimy zrobić aby należycie zabezpieczyć i przechowywać dane osobowe, ale nie mogą być one sprzeczne z Rozporządzeniem RODO.

2. PRZEPROWADZONE CZYNNOŚCI I DOKUMENTACJA

Audytor Wewnętrzny przeprowadzając zadanie audytowe dokonał analizy przepisów prawa powszechnie obowiązującego oraz przeglądu funkcjonujących dokumentów i przepisów wewnętrznych w Urzędzie Starostwa Powiatowego w Lubaczowie.
Poprawność oraz funkcjonowanie zaprojektowanych procedur kontroli zarządczej zbadano przy wykorzystaniu dokumentów roboczych, takich jak: kwestionariusze oceny oraz badanie zawartych treści w dokumentach funkcjonujących w ramach audytowanej tematyki.

Weryfikacja uzyskanych danych oraz analiza dokumentów roboczych, stanowiła podstawę do sformułowania wniosków w sprawie poziomu i stopnia realizacji zadań związanych z ochroną danych osobowych.

Powyższe czynności audytowi pozwoliły na sformułowanie poniższych opinii i wniosków.

3. SPOSÓB PRZEDSTAWIENIA WYNIKÓW CZYNNOŚCI AUDYTOWYCH

Treść sprawozdania ostatecznego została podzielona na część ogólną – ustalenia tj. opis podjętych czynności, obowiązki wynikające z przepisów prawa powszechnego oraz część szczególną – rekomendacje odnoszące się do ustaleń dla których potrzebne są działania celem dostosowania funkcjonowania Starostwa w myśl obowiązujących przepisów.

Rozdział III

Ustalenia i rekomendacje

W Starostwie Powiatowym w Lubaczowie powołano Inspektora ochrony danych. Zadania powierzone dla IOD zostały określone w regulaminie organizacyjnym, Polityce ochrony danych oraz umowie cywilnoprawnej.

Ponadto udostępniono projekt Regulaminu funkcjonowania IOD, który na dzień audytu pozostawał w fazie opracowania i uzgodnień. ***Powyższe należy uznać za zgodne*** z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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) a w szczególności art. 37 ust 1, który przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Przez organy i podmioty publiczne obowiązane do wyznaczenia IOD, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się jednostki sektora finansów publicznych czyli np. jednostki samorządu terytorialnego, zgodnie z art. 9 pkt 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

W Starostwie opracowano metodologię oceny ryzyka związanego z przetwarzaniem danych osobowych jak również przeprowadzono analizę ryzyka.

Metodologia uwzględnia zarówno prawdopodobieństwo wystąpienia zdarzenia powodującego naruszenie bezpieczeństwa, jak i jego wagi, poziom ryzyka określono jako iloczyn prawdopodobieństwa wystąpienia zdarzenia oraz jego skutku.
Na gruncie RODO nie została wskazana jedna określona metodyka przeprowadzania procesu zarządzania ryzykiem. Obecnie znanych jest wiele metod, z których można czerpać inspirację i dobre przykłady dla tworzenia własnych rozwiązań. Wybór metody powinien odpowiadać specyfice danego podmiotu, uwzględniać zakres i cele przetwarzania oraz rodzaj danych, a także wielkość, strukturę oraz możliwości organizacyjne, techniczne i finansowe danej jednostki. Dobór odpowiednich środków zapewniających zgodność z przepisami prawa, w tym zapewniających minimalizację ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, zgodnie z przyjętą w RODO koncepcją opartą na ryzyku, należy do administratorów i podmiotów przetwarzających. Oszacowanie ogólnego ryzyka naruszenia ochrony przetwarzanych danych powinno być przeprowadzone z uwzględnieniem takich atrybutów bezpieczeństwa, jak: poufność, integralność i dostępność. Należy zauważyć, że przedstawionej metodologii jak również analizie ryzyka nie uwzględniono atrybutu dostępności. Czynnością, jaką należy wykonać po oszacowaniu ryzyka dla poszczególnych operacji przetwarzania, jest podjęcie decyzji dotyczącej poszczególnych ryzyk. W wyniku przeprowadzonej analizy stwierdzono, iż nie występuje ryzyko nieakceptowalne niemniej jednak należy zauważyć, iż występuje opcjonalne ryzyko, które zgodnie z przyjętymi

założeniami (reakcja na wartość ryzyka) wymaga akceptacji lub działań obniżających ryzyko, które może zastosować Administrator:

a. Przeniesienie - przerzucenie ryzyka (outsourcing, ubezpieczenie)

b. Unikanie - eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)

c. Redukcja - zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie nośników
z danymi wynoszonych poza firmę).

W opisie planowanego działania przewidziano w sposób ogólny „wdrożenie dodatkowych środków zabezpieczenia podejmowane w zależności od wymaganych nakładów". Co istotne nie wykazano, jakie to miałyby być środki, wobec czego nie można szacować ich kosztów. Zgodnie z przyjętymi założeniami ryzyko opcjonalne wymaga akceptacji lub działań. Mając na uwadze, że dokument nie został „zatwierdzony" przez administratora jak również to, że nie, wyznaczono listy zabezpieczeń do wdrożenia, terminu realizacji i osób odpowiedzialnych należy uznać, iż przeprowadzona analiza ryzyka nie spełnia swojej podstawowej roli jaką jest obiektywna ocena stanu faktycznego umożliwiająca dobór adekwatnych środków bezpieczeństwa a tym samym spełnienia wymogu projektowania systemu ochrony w oparciu o analizę ryzyka, której wyniki pomocne będą w doborze metod przetwarzania i środków zapewniania bezpieczeństwa danych osobowych.

Rekomenduje się rozważyć przeprowadzenie analizy ryzyka z wykorzystaniem ww. uwag w tym opracowaniu planu postepowania z ryzykiem lub udokumentowaniem akceptacji ryzyk.

W Starostwie opracowano i wdrożono politykę ochrony danych osobowych. Polityka była, co najmniej raz przeglądnięta pod kątem aktualności zapisów. Dokumentem potwierdzającym dokonanie przeglądu jest notatka. Polityka bezpieczeństwa danych osobowych to centralny dokument wewnętrznej dokumentacji ochrony danych osobowych. Przepisy RODO nie wskazują jednoznacznie na obowiązek opracowania polityki bezpieczeństwa danych osobowych. Mimo to nie należy zapominać o obowiązku udokumentowania przez administratora przestrzegania przepisów w zakresie ich ochrony – ***atrybut rozliczalności***. Polityka bezpieczeństwa danych osobowych powinna nie tylko nakreślać kierunek, jakim jest ogólne zobowiązanie do wdrożenia przepisów o ochronie danych, ale także być dokumentem praktycznym, który pozwala łatwo poruszać się po całej dokumentacji ochrony danych. Z tego względu polityka bezpieczeństwa danych osobowych powinna zawierać wskazanie osób odpowiedzialnych za realizację poszczególnych postanowień oraz zawierać odwołania do wszystkich innych dokumentów dotyczących ochrony danych.

W polityce bezpieczeństwa danych osobowych potrzeba jasnego wskazania osób odpowiedzialnych między innymi za: prowadzenie i stałą aktualizację rejestrów: rejestru czynności przetwarzania, rejestru incydentów czy rejestru odpowiedzi na żądanie osób, których dane dotyczą, przeprowadzanie audytów, przeprowadzanie DPIA i analizy ryzyka, szkoleń personelu, zgłaszanie incydentów i zarządzanie nimi, realizację planów mających na

celu wdrożenie rekomendacji z audytów i analiz oraz monitorowanie zgodności z RODO. Polityka bezpieczeństwa jest dokumentem, który musi żyć i zawsze odzwierciedlać rzeczywisty stan faktyczny postępowania z danymi.

W oparciu o powyższe wskazania rekomenduje się przy kolejnym przeglądzie dokumentacji ochrony mając na uwadze ww. aspekty rozważyć uzupełnienie dokumentacji o zasady realizacji planów mających na celu wdrożenie rekomendacji z audytów i analiz oraz wskazanie osób odpowiedzialnych.

Ustalając czy pracownicy jednostki zostali przygotowani do realizacji obowiązków zgodnie z zasadami RODO a w szczególności, czy zorganizowano szkolenia z zakresu przepisów o ochronie danych osobowych dla osób pełniących funkcje ADO, IOD oraz pracowników uczestniczących w przetwarzaniu danych uzyskano odpowiedź, iż szkolenia odbyły się 3 razy z podziałem na 2 grupy po ok 30 osób. W odpowiedzi nie wykazano by ADO czy IOD uczestniczyli w szkoleniach z zakresu ochrony danych osobowych. Każda osoba upoważniona do przetwarzania danych osobowych musi zostać zaznajomiona zarówno z powszechnie obowiązującymi przepisami o ochronie danych osobowych jak i z wewnętrznymi aktami prawnymi i środkami bezpieczeństwa, do których należy stosować się w miejscu przetwarzania danych osobowych.

Biorąc powyższe pod uwagę rekomenduje się objęcie szkoleniami wszystkie osoby mające dostęp do danych osobowych w tym ADO.

Dane osobowe są przetwarzane wyłącznie przez osoby/podmioty działające na polecenie i z upoważnienia ADO oraz wyłącznie w zakresie niezbędnym do realizacji swoich zadań powyższe ustalono w oparciu o kopie upoważnień. Ustalono również, że administrator dokumentuje proces upoważniania do przetwarzania danych w sposób, który umożliwia ustalenie wszystkich osób zaangażowanych w procesy przetwarzania danych osobowych prowadząc rejestr upoważnień do przetwarzania danych osobowych. ***Mając na uwadze powyższe należy stwierdzić, iż wypełniane są postanowienia art. 29 RODO*** - każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego - Starosty i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba, że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Niemniej jednak należy zauważyć pewne rozbieżności w zakresie wzoru upoważnienia i jego treści a postanowieniami § 5 ust 2 lit. f tj. brak w wydanych upoważnieniach nazwy zbioru/zbiorów przetwarzania zgodnej z nazwą zbioru występującą w rejestrze czynności przetwarzania prowadzonym przez IOD. Upoważnienia nie wskazują zakresu dostępu do danych osobowych a w szczególności do czynności przetwarzania. Przeanalizowane zakresy czynności również nie odwołują się do upoważnienia do przetwarzania danych osobowych w tym nie określają zakresu nadanych uprawnień. Zgodnie natomiast z art. 32 RODO administrator i podmiot przetwarzający uwzględniając stan wiedzy technicznej, koszt

wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający charakterowi prowadzonego przetwarzania i związanego z nim ryzyka. Zgodnie z art. 32 ust. 4 administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego. Zgodnie ze stanowiskiem UODO chodzi o to, aby administrator miał kontrolę nad tym, kto i w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach
i w jaki sposób je przetwarza. Przyjmowane przez administratora i podmiot przetwarzający działania powinny służyć m.in. zapobieganiu nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych oraz zapewnieniu, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem. Dzięki tym środkom osoby, które zostały dopuszczone do przetwarzania danych zostają poinformowane, jaki jest zakres ich uprawnień, co do przetwarzania danych osobowych. Wydawanie upoważnień zgodnie z przyjętą polityką jest jednym z środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania.

Mając na uwadze powyższe rekomenduje się dokonanie ponownej analizy przyjętych środków organizacyjnych a w szczególności w zakresie nadawania upoważnień do przetwarzania danych osobowych lub innych form upoważniania do przetwarzania danych osobowych w tym wypracowania rozwiązań, które będą czytelnie określały zakres dostępu do danych osobowych (czynności przetwarzań).

W trakcie prowadzonych czynności audytowych ustalono, że Starostwo przetwarza dane, jako „procesor" (podmiot przetwarzający) oraz prowadzi Rejestr kategorii czynności przetwarzań. Zgodnie z art. 30 ust. 2 RODO Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu, którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Biorąc powyższe pod uwagę należy stwierdzić, iż omawiany rejestr zawiera wszystkie elementy wskazane w RODO. Niemniej jednak mając na uwadze wzór rejestru zaprezentowany przez UODO zasadnym wydaje się rozważenie uzupełnienia go o dwa elementy tzn. czas trwania przetwarzania oraz dane dotyczące podprzetwarzającego. Zwrócić należy uwagę, że zgodnie ze wzorem zamieszczonym w załączniku do Polityki ochrony danych każdy arkusz rejestru powinien być podpisany przez IOD lub osobę upoważnioną. W udostępnionych arkuszach widnieje jedynie data.

Ustalono, że administrator – Starosta powierza przetwarzanie danych w swoim imieniu innym podmiotom. Powierzenie odbywa się z wykorzystaniem umowy powierzenia danych. Ponadto Starosta prowadzi rejestr umów powierzenia. W załączniku do polityki opracowano wzór umowy powierzenia. Zgodnie z art. 28 ust 3 RODO 3. przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki wymagane na mocy art. 32;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

4. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Wobec niewystąpienia przypadku zakończenia umowy powierzenia danych nie poddano analizie sposobu realizacji zobowiązania do usunięcia albo zwrotu wszelkich danych osobowych oraz ich istniejących kopii po zakończeniu świadczenia usług.

W omawianym zakresie nie wnosi się uwag.

Ustalając czy administrator przetwarza dane osobowe, w oparciu o uzyskaną zgodę (art. 6 ust 1 lit. a lub art. 9 ust 2 lit a RODO) uzyskano odpowiedź, niejednoznaczną („Posiada

procedurę zgodnie z Polityką Ochrony Danych Osobowych. Jeżeli istnieje podstawa przetwarzania zgodnie z art.6 ust. 1 lit. a lub 9 ust.2 lit a RODO, to wówczas administrator pozyskuje i gromadzi klauzule zgody.").

W zakresie obowiązującego systemu rejestrowania i zarządzania bieżącą zgodą na przetwarzanie danych osobowych uzyskano informację, że „Polityka ochrony danych zawiera procedury". Dodatkowo ustalono, że opracowano wzór „zgody". Analizując powyższy obszar należy zauważyć, że co do zasady Polityka ochrony danych odnosi się do problematyki zbierania zgód oraz prowadzenia rejestrów udzielonych zgód jednak trudno oprzeć się wrażeniu, że nie są one w praktyce stosowane. Zasadnym wydaje się odniesienie do ogólnych zasad oraz wzoru (sposobu) odwołania udzielonej zgody. Mając na uwadze fakt, iż zgodnie z RODO odwołanie zgody powinno być tak samo proste jak jej udzielenie pominięcie ww. obszaru w regulacjach wewnętrznych należy uznać za brak, który należy jak najszybciej uzupełnić.

Rekomenduje się dokonanie stosownych sprawdzeń w zakresie stanu faktycznego zarządzania zgodą oraz uzupełnienie dokumentacji o wzór odwołania zgody oraz procedurę postępowania z chwilą otrzymania powyższego żądania.

W związku z informacją, że nie odnotowano wniosku dot. odwołania zgody na przetwarzanie danych nie dokonano oceny powyższego.

W trakcie prowadzonych czynności audytowych ustalono, że opracowano treść klauzuli informacyjnej dla osób, od których dane osobowe będą pozyskiwane (odrębnie dla każdego procesu przetwarzania). Na podstawie przedstawionych klauzul informacyjnych stwierdzić należy, iż administrator - Starosta przygotował się do realizacji wymogu art. 13 RODO.

W zakresie realizacji praw osób, których dane są przetwarzane ustalono, iż nie wpłynął do podmiotu wniosek o:
a) sprostowanie albo usunięcie danych osobowych podlegających przetwarzaniu,
b) ograniczenie przetwarzania dane osobowe,
c) przeniesienie danych osobowych
Nie odnotowano również wniesienia sprzeciwu osoby wobec przetwarzania danych osobowych

Należy zauważyć, że załącznik nr 8 do polityki ochrony danych zatytułowany „Prawa osoby, której dane dotyczą – procedury" szczegółowo określa postępowanie w przypadku otrzymania wniosku o realizację uprawnień osoby. Oceniając rozwiązania proceduralne nie wnosi się uwag.

Przeprowadzone czynności audytowe pozwoliły stwierdzić, że prowadzony jest rejestr czynności przetwarzania danych. Przedmiotowy rejestr jest prowadzony w formie pisemnej. Rejestr papierowy funkcjonujący w Starostwie zawiera elementy wskazane w RODO. ***Rekomenduje się uzupełnienie kolumny podstawa prawna o właściwy art. 6 lub 9 RODO***

wobec braku konsekwencji i jednolitości dla wszystkich czynności przetwarzań. Powyższe ułatwi tworzenie klauzuli informacyjnej w tym określenie katalogu praw osób wynikających z RODO. Wyznaczono również osobę, której powierzono prowadzenie rejestru czynności przetwarzania danych. Na uwagę zasługuje fakt, iż zgodnie ze wzorem załączonym do polityki ochrony danych arkusze poszczególnych czynności przetwarzań winny być opatrzone datą oraz podpisem IOD lub osoby upoważnionej. Nie wykazano również rejestru zmian w dokumencie udostępniony materiał opatrzono zapisem „tekst jednolity z dnia 2.09.2021r."

W kwestionariuszu audytowym wskazano, że administrator danych nie odnotował przypadków naruszenia ochrony danych osobowych, które skutkują ryzykiem naruszenia praw lub wolności osób fizycznych.

Wobec braku przypadku nie dokonano zgłaszania naruszenia ochrony danych osobowych do organu nadzorczego jak również powiadomienia osoby, której dotyczyło naruszenie.

Ponadto wskazano, że nie jest prowadzony rejestr naruszeń ochrony danych osobowych wobec braku zdarzeń jednocześnie wskazując, że procedura zakłada prowadzenie takiego rejestru. Zgodnie z art. 33 ust. 5 RODO Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Mając powyższe na uwadze zaleca się wprowadzenie w życie takiego rejestru.

Zgodnie z odpowiedzią w arkuszu audytowym ustalono, że wszyscy pracownicy zobowiązani są do składania oświadczenia o zachowaniu poufności danych osobowych. Ponadto opracowano wzór oświadczenia o zachowaniu poufności. ***W zakresie powyższego obszaru uwag nie wnosi się.***

Na podstawie przeprowadzonych czynności audytowych ustalono, że w Starostwie prowadzona jest ewidencja systemów oraz programów używanych do przetwarzania danych osobowych zawierająca nazwę programu oraz dane dot. licencji.

W kwestionariuszu audytowym wskazano, iż w Starostwie wyznaczono zespół osób odpowiedzialnych za zarządzanie użytkownikami systemów informatycznych oraz że prowadzona jest ewidencja użytkowników systemów informatycznych.

Ponadto opracowano zasady nadawania/odbierania uprawnień w systemie informatycznym

Zgodnie z Instrukcją Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Lubaczowie oraz załącznikiem Nr 1 do „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Lubaczowie" – wnioski o nadawanie i cofanie uprawnień, IZSI.

W Starostwie opracowano dokumenty regulujące obszary przetwarzania:

- instrukcję przetwarzania danych w systemach informatycznych,
- politykę realizacji praw osób, których dane są przetwarzane,
- zasady wykorzystywania poczty służbowej,
- zasady wykorzystywania urządzeń mobilnych służących do przetwarzania danych osobowych.

Nie opracowano polityki przetwarzania danych osobowych w ramach pracy zdalnej, wobec nie wprowadzenia pracy zdalnej w Starostwie .

Przepisy w zakresie RODO nie zawierają praktycznie żadnych wytycznych odnoszących się do sposobu prowadzenia dokumentacji przetwarzania danych osobowych, jak również jej zawartości. Nie oznacza to jednak, że administrator danych nie jest zobligowany do posiadania żadnej dokumentacji w tym zakresie. RODO nie określa formalnych wymagań dotyczących dokumentacji przetwarzania danych osobowych dając tym samym dużą swobodę w tym zakresie administratorom danych. Decydujące znaczenie dla obszaru i zakresu informacji, jakie powinny być zawarte w dokumentacji przetwarzania jest wymóg wykazania przez administratora przestrzegania przepisów RODO zawarty w art. 24, którego brzmienie jest następujące. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator – administrator (Starosta) wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki o których mowa powyżej, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Wymaganie zawarte art. 24 RODO stanowiące, że administrator powinien być w stanie wykazać przestrzeganie przepisów RODO oznacza w praktyce, że sposób przetwarzania danych, związane z nim procedury jak i zastosowane zabezpieczenia techniczne i organizacyjne, również powinny zostać zawarte w przedmiotowej dokumentacji, jako spełnienie obowiązku wykazania, że przestrzegane są wymagania RODO. Ponadto obowiązek prowadzenia dokumentacji przetwarzania danych wynika pośrednio również z art. 32 RODO dotyczącego bezpieczeństwa przetwarzania, który stanowi, że: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (...).

Mając powyższe na uwadze nie wnosi się uwag do omawianego obszaru.

Na podstawie udzielonych odpowiedzi w arkuszu audytowym ustalono, że w Starostwie stosowany jest monitoring wizyjny natomiast nie stosuje się monitorowania poczty służbowej oraz monitoringu wykorzystującego dane lokalizacyjne. O stosowaniu monitoringu wizyjnego poinformowano pracowników o poprzez zapoznanie z regulaminem

monitoringu wizyjnego oraz przedstawieniem klauzuli informacyjnej dot. monitoringu wizyjnego.
W ramach regulacji wewnętrznych opracowano regulamin monitoringu (w chwili obecnej zawarty w regulaminie organizacyjnym). W zakresie retencji danych określono okres przechowywania danych oraz zasady niszczenia tj. 7 dni jest rejestrowany (nadpisywany) później automatycznie kasowany.

Na pytanie czy obszar objęty monitoringiem wizyjnym został oznakowany oraz prośbę o opis sposobu spełnienia obowiązku informacyjnego w związku ze stosowanym monitoringiem wizyjnym wraz z stosownymi kopiami uzyskano informację szczątkową „Tak" w załączeniu przekazano klauzulę informacyjną. Administrator określił podstawę prawną uprawniającą do stosowania monitoringu wynikającą z art. 6 ust. 1 lit f) RODO – prawnie uzasadniony interes administratora, tj. zapewnienie względów bezpieczeństwa, wykorzystanie służy do monitorowania pomieszczeń przed nieautoryzowanym dostępem, co umożliwia przepis art. 22^2 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy. Analizując omawiany obszar należy zauważyć, iż podstawy stosowania monitoringu w omawianym przypadku określono również w art. 4b ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym.

Istotne znaczenie ma realizacja wobec osoby obserwowanej obowiązku informacyjnego ujętego w art. 13 RODO. Musi on być, zgodnie z art. 12 rozporządzenia, realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część przepisów szczególnych wskazuje dodatkowo znaki lub ogłoszenia dźwiękowe, którymi należy oznaczyć pomieszczenia i teren monitorowany. Pełna informacja o monitoringu, obejmująca wszystkie wymogi art. 13 RODO, powinna być dostępna w miejscu monitorowanym, np. na tablicach albo w formie dokumentu dostępnego w recepcji czy też u przedstawiciela administratora. Czyli możliwa jest realizacja obowiązku informacyjnego poprzez podanie informacji podstawowych i uzupełnienie ich w kolejnych warstwach informacyjnych. Znaki informujące o stosowaniu monitoringu powinny być dostępne przed wejściem w obszar obserwowany. Jednym z obowiązków wprowadzonych zapisami kodeksu pracy jest przekazanie pracownikowi przed dopuszczeniem do pracy informacji o celach, zakresie oraz sposobie zastosowania monitoringu na piśmie. Zapoznanie z regulaminem monitoringu wszystkich pracowników mając na uwadze zasadę rozliczalności wydaje się rozwiązaniem niekompletnym. Pracodawca ma obowiązek poinformowania pracowników o wykorzystywaniu w zakładzie pracy monitoringu wizyjnego. Realizacja tego obowiązku wymaga ustalenia, a następnie przekazania pracownikom informacji o celu, zakresie oraz sposobie stosowania monitoringu przed jego wprowadzeniem. W przypadku zakładu pracy, w którym monitoring wizyjny już funkcjonuje, pracodawca powinien dopełnić obowiązku informacyjnego w tym zakresie każdorazowo przy zatrudnieniu nowego pracownika. Korzystanie przez zakład pracy z monitoringu wizyjnego wymaga dopełnienia przez pracodawcę formalności ściśle określonych w Kodeksie pracy. Pierwszą z nich jest obowiązek ustalenia w układzie zbiorowym pracy lub w regulaminie pracy, a jeżeli pracodawca nie został objęty układem zbiorowym pracy lub nie jest zobowiązany do ustalenia

regulaminu pracy, to w obwieszczeniu, zasad funkcjonowania takiego monitoringu, a przede wszystkim wskazania jego: celu, zakresu, sposobu zastosowania. Następnie pracodawca ma obowiązek poinformowania wszystkich pracowników o wprowadzeniu monitoringu. Przekazanie takiej informacji powinno nastąpić nie później niż 2 tygodnie przed jego uruchomieniem. Natomiast w przypadku pracodawcy, u którego monitoring wizyjny już działa, konieczne jest każdorazowe przekazanie informacji o jego funkcjonowaniu przed dopuszczeniem nowo zatrudnionego pracownika do pracy.

Zauważyć należy różnicę w zapisach regulaminu oraz klauzuli dot. stosowanego monitoringu w pierwszym dokumencie określono czas przechowywania, jako 7 dni w drugim natomiast 14 dni.

Rekomenduje się, uzupełnienie informacji o stosowanym monitoringu w sposób zapewniający skuteczne poinformowanie osoby o objęciu nadzorem wizyjnym. Co do zasady jednym z rozwiązań jest warstwowe przekazywanie informacji rozpoczynając od znaków graficznych, ogólnych informacji dot. celu, zakresu, danych administratora do pełnej klauzuli wynikającej z art. 13 RODO. Ważnym elementem będzie również określenie jednolitego okresu przechowywania danych uzyskanych w związku ze stosowanym monitoringiem.

Na pytanie zadane w arkuszu audytowym czy opracowano zasady przeglądu danych osobowych opublikowanych w BIP lub stronie internetowej podmiotu pod kątem ich aktualności oraz zasadności dalszego publikowania uzyskano odpowiedź, że regulamin korzystania z BIP znajduje się w opracowaniu.

Rekomenduje się opracowanie dokumentu wewnętrznego regulującego zasady przetwarzania danych osobowych w BIP a w szczególności umożliwiającego kontrolę okresu retencji dla danych znajdujących się w BIP, tak by nie były one dostępne w przypadkach gdy okres przechowywania minął.

Na pytania w arkuszu audytowym dot. przetwarzania danych w ramach ZFŚS otrzymano nw. odpowiedzi.

Czy w Starostwie przetwarzane są dane osobowe w ramach ZFŚS oraz czy dostosowano regulamin świadczeń socjalnych do znowelizowanej ustawy a w szczególności art. 8 ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych:

a) w zakresie udostępnienia pracodawcy danych osobowych osoby uprawnionej do korzystania z funduszu, w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z funduszu i ustalenia ich wysokości,

Udostępnienie pracodawcy danych osobowych osoby uprawnionej do korzystania z Funduszu, w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z Funduszu i ustalenia ich wysokości, następuje w formie oświadczenia. Pracodawca może żądać

udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia. Potwierdzenie może odbywać się w szczególności na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu.

Administrator danych wypełnia również obowiązek informacyjny wynikający z art. 13 i 14 RODO.

a) w zakresie dopuszczenia do przetwarzania danych osobowych dotyczących zdrowia, wyłącznie osób mających pisemne upoważnienie do przetwarzania takich danych, wydane przez pracodawcę.
Członkowie Komisji ZFŚS otrzymują upoważnienie do przetwarzania danych osobowych w związku z wykonywaniem czynności w pracach Komisji ZFŚS, są one zobowiązane do zachowania tajemnicy.
b) w zakresie dopuszczania do przetwarzania danych osobowych dotyczących zdrowia osób, które są obowiązane do zachowania ich w tajemnicy,
Członkowie Komisji ZFŚS otrzymują upoważnienie do przetwarzania danych osobowych w związku z wykonywaniem czynności w pracach Komisji ZFŚS, są one zobowiązane do zachowania tajemnicy.
c) w zakresie okresu przechowywania danych,
Pracodawca przetwarza dane osobowe przetwarzane w ZFŚS przez okres niezbędny do przyznania ulgowej usługi lub świadczenia, dopłaty z Funduszu oraz ustalenia ich wysokości, a także przez okres niezbędny do dochodzenia praw lub roszczeń. Przegląd danych jest dokonywany, co roku i wtedy dokonuje się oceny, co do zasadności dalszego przechowywania.
e) w zakresie przeglądu danych osobowych, nie rzadziej niż raz w roku kalendarzowym w celu ustalenia niezbędności ich dalszego przechowywania, że zgodnie z art. 8d ustawy o ZFŚS administrator danych dokonuje przeglądu danych osobowych w zakresie okresu przechowywania danych, usuwania danych osobowych, zbędnych do celów określonych w art. 8 ust. 1a i 1c.
f) w zakresie usuwania danych osobowych, zbędnych do celów określonych w art. 8 ust. 1a i 1c. zgodnie z art. 8d ustawy o ZFŚS administrator danych dokonuje przeglądu danych osobowych w zakresie okresu przechowywania danych, usuwania danych osobowych, zbędnych do celów określonych w art. 8 ust. 1a i 1c.
Administrator danych wypełnia również obowiązek informacyjny wynikający z art. 13 i 14 RODO.

Udzielenie odpowiedzi sugerują, że obowiązki pracodawcy w ramach przetwarzania danych ZFŚS są realizowane.

Mając na uwadze fakt, iż na dzień audytu nie dostosowano regulaminu świadczeń socjalnych do znowelizowanych przepisów należy stwierdzić, iż omawiany obszar wymaga aktualizacji regulacji wewnętrznych obejmujących co najmniej stosowne wzory dokumentów (wnioski,

oświadczenia o zachowaniu danych w poufności, upoważnienia do przetwarzania danych, sprawozdania z przeglądu danych itp.).

ZGODNOŚĆ ZE STANDARDAMI

Zadanie audytowe: „Ochrona danych osobowych w Starostwie" zostało przeprowadzone zgodnie z "Międzynarodowymi Standardami Profesjonalnej Praktyki Audytu Wewnętrznego", opracowanymi przez The Institute of Internal Auditors ogłoszonymi Komunikatem Nr 2 Ministra Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych opublikowanym w Dzienniku Urzędowym Ministra Rozwoju i Finansów z dnia 16 grudnia 2016 r., poz. 28.

AUDYTOR WEWNĘTRZNY
Lech CZERNECKI
Zaświadczenie MF nr 636/2004