| SPRAWOZDANIE Z ZADANIA ZAPEWNIAJĄCEGO | |
|---|---|
| **Nazwa zadania zapewniającego:**<br>*Ocena systemu nadawania i likwidacji uprawnień do przetwarzania danych osobowych*<br>**Nr zadania zapewniającego:** 2/2018 (KAW.1720.04.2018) | |
| **Nazwa jednostki audytowanej:** Urząd Miasta Jastrzębie - Zdrój | |
| **Audytor:** | **nr upoważnienia:** |
| Agnieszka Marszałek<br>Edyta Pyrtek | KAW.1720.02.2018<br>KAW.1720.03.2018 |
| **Data rozpoczęcia zadania zapewniającego:** 17.05.2018r. | |
| **Wykonał:**<br>Data i podpis: .....<br>Data i podpis: .....<br>**Zatwierdził:** Data i podpis: ..... | KIEROWNIK WYDZIAŁU KONTROLI<br>URZĘDU MIEJSKIEGO<br>Agnieszka Marszałek |

## I. Cel:

Uzyskanie racjonalnego zapewnienia, że system nadawania i likwidacji uprawnień do przetwarzania danych osobowych funkcjonuje prawidłowo .

## II. Zakres:

1. Podmiotowy:
    1. Publiczne Przedszkole nr 17
    2. Publiczne Przedszkole nr 21
    3. Szkoła Podstawowa nr 12
    4. Szkoła Podstawowa nr 21
    5. Zespół Szkół Zawodowych
    6. Centrum Kształcenia Praktycznego
    7. Publiczny Żłobek nr 1

Wyboru Jednostek do zadania audytowego dokonano w drodze doboru próby losowej, zgodnie z załącznikiem nr 1 do sprawozdania.

2. Przedmiotowy:
    - Ocena funkcjonowania systemu nadawania i likwidacji uprawnień do przetwarzania danych osobowych.

**Przedmiot testów i badań w zrealizowanym zadaniu audytowym stanowiły stosowane rozwiązania systemowe w obszarze nadzoru nad nadawaniem i likwidacją uprawnień do przetwarzania danych osobowych.**

DATA WPŁYWU
27. 03. 2019 19. 02. 2019

## III. Obiekty audytu:

1. System nadawania i likwidacji uprawnień do przetwarzania danych osobowych.

## IV. Analiza ryzyka:

| Obiekty audytu | Jednostka Audytowana | Kategorie ryzyk | | | | | Końcowa ocena ryzyka |
|---|---|---|---|---|---|---|---|
| | | istotność | jakość | kontrola | czynniki zew. | czynniki operac. | |
| | | 0,20 | 0,20 | 0,25 | 0,15 | 0,20 | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Obiekt 1 | zgodnie z zakresem podmiotowym | 2-10% | 3-15% | 4-25% | 2-7,5% | 4-20% | **77,50%** |

## V. METODYKA:

- analiza dokumentacji (ewidencje, zakresy czynności, upoważnienia),
- testy przeglądowe,
- testy wiarygodności,
- wyjaśnienia pracowników związanych z realizacją procesu.

## VI. TERMIN: 40 dni robocze objęte wykonaniem zadania audytowego.

## VII. KRYTERIA OGÓLNE

1. Legalność :
   czy wszelkie działania prowadzone są zgodnie z przepisami obowiązującego prawa (wewnętrznego, zewnętrznego).

2. Celowość :
   czy działania prowadzone na każdym audytowanym etapie mieściły się w celach określonych dla nich przez przepisy prawa.

3. Nadzór:
   czy opracowane procedury są prawidłowe oraz czy są prawidłowo stosowane, czy wszelkie odstępstwa są monitorowane i wyciągane wnioski.

4. Rzetelność:
   czy pracownicy wypełniali swoje obowiązki z należytą starannością, sumiennie i we właściwym czasie.

## VIII. USTALENIA

### 1. Obiekt 1

**System nadawania i likwidacji uprawnień do przetwarzania danych osobowych.**

## 1.1. Kryteria szczegółowe

- Czy opracowano procedury wewnętrzne odnośnie ochrony danych osobowych?
- Czy procedury zostały prawidłowo wdrożone w Jednostce?
- Czy wprowadzone mechanizmy kontroli, w zakresie audytowanego procesu, były wystarczające aby zabezpieczyć interesy ADO?
- Czy funkcjonujący system nadawania i likwidacji uprawnień zapewniał wypełnienie zasad RODO; rzetelności, przejrzystości i zgodności z prawem?

## 1.2. Wnioski, opinie, rekomendacje

**Przedmiot zadania audytowego – dobór próby**

Podmiotowy zakres zadania audytowego ustalono na podstawie doboru próby zgodnie z załącznikiem nr 1 do sprawozdania.

Przedmiotem przeprowadzonych czynności audytowych była ocena funkcjonowania systemu nadawania i likwidacji uprawnień do przetwarzania danych osobowych .

Dla celów przeprowadzenia zadania przyjęto następujące kryteria w zakresie ustalenia przedmiotu zadania audytowego:

- upoważnienia wystawione dla wszystkich pracowników administracji i pedagogów zatrudnionych w danej Jednostce na dzień prowadzenia czynności audytowych;
- upoważnienia nadane pracownikom administracji i pedagogom, z którymi rozwiązano stosunek pracy w okresie od 01.01.2017r. do 30.11.2018r.;
- z zadania wyłączono pracowników obsługi.

Wyboru dokonano na podstawie sporządzonych przez Jednostkę wykazów pracowników (w oparciu o powyższe kryteria), ze szczególnym uwzględnianiem podziału na pracowników administracji oraz pedagogów.

Biorąc pod uwagę specyfikę zadania audytowego analizie poddano prawie wszystkich pracowników administracji (zgodnie z opisem dotyczącym danej Jednostki) oraz losowo wybranych pedagogów, przy uwzględnieniu próby 5 do 10% populacji.

## Upoważnienia

Zgodnie z definicją zawartą w art.7 RODO

**Dane osobowe** oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna, to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:

- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji, identyfikator internetowy,
- jeden bądź kilka szczególnych czynników określających fizyczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

**Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie**

Zbiory danych mogą być prowadzone zarówno w systemie informatycznym, jak i przetwarzane tradycyjnie.

Dane osobowe można podzielić na trzy kategorie tj.:

- **dane tzw. zwykłe**: imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód itp.
- **szczególne kategorie danych osobowych** (art.9 RODO):
  - pochodzenie rasowe lub etniczne,
  - poglądy polityczne,

- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne, biometryczne,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

➢ **dane dotyczące wyroków skazujących** (art.10 RODO). W celu przetwarzania danych tzw. wrażliwych należy wypełnić dodatkowe warunki ich ochrony wskazane w art.9 ust.2 i art.10 RODO.

O celach i sposobach przetwarzania danych decyduje **Administrator danych osobowych**. Zgodnie z art.24 ust.1 RODO do obowiązków administratora należy wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać i w razie potrzeby poddawać przeglądom i uaktualniać.

Zgodnie z definicją wprowadzoną art.4 pkt 7 RODO, Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Ponadto administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych osobowych tj. musi być w stanie wykazać ich przestrzeganie. Wskazuje się, iż w przypadku gdy administratorem jest Dyrektor placówki, to on ponosi odpowiedzialność za działania wszystkich osób upoważnionych do przetwarzania danych osobowych.

**Zasady przetwarzania danych osobowych** (art.5 RODO):

- zgodność z prawem, rzetelność, przejrzystość;
- ograniczenie celu;
- minimalizacja danych;
- prawidłowość;
- ograniczenie przechowywania;
- integralność i poufność.

Art.37 RODO nakłada na placówki oświatowe obowiązek powołania **Inspektora ochrony danych**, którego zadania zostały sformułowane w art.39 RODO.

Inspektorem ochrony danych może być osoba zatrudniona w szkole lub osoba wykonująca zadania na podstawie umowy o świadczenie usług.

W RODO nie określono wprost jak należy udokumentować organizację przetwarzania i zarządzania bezpieczeństwem przetwarzania danych, wymagane jest jednak takie zastosowanie środków bezpieczeństwa i wdrożenie odpowiednich polityk aby podejmowane w tym zakresie działania można było wykazać.

**Procedura nadawania upoważnień** to jeden z wymaganych elementów, które składają się na Politykę ochrony danych zgodnych z RODO.
Każda Instytucja tworząc Politykę ochrony danych osobowych powinna się opierać na zidentyfikowaniu słabych i mocnych stron swojej organizacji oraz odpowiednio dostosować treść do indywidualnych potrzeb.
Zgodnie z powyższymi założeniami dopuszcza się możliwość różnych uregulowań w audytowanym zakresie, przez poszczególne Jednostki.

Zgodnie z regulacją zawartą w art.32 ust.4 RODO, ADO 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.
RODO nie normuje w sposób bezpośredni obowiązku formalnego nadawania upoważnienia, przepisy RODO wskazują jednakże znaczenie przetwarzania „wyłącznie na polecenie" przez osoby fizyczne „działające z upoważnienia", które jest bliżej niezdefiniowane.
Forma pisemna upoważnienia nie wynika wprost z przepisów RODO, ważne jednak jest odpowiednie udokumentowanie faktu nadania upoważnienia, co pozwoli administratorowi na wykazanie, iż dochował wymogu „upoważnienia" osoby „upoważnionej".
Przepisy RODO nie określają jakie dane powinny zostać uwzględnione w treści upoważnienia, jednakże (uwzględniając rolę jaką upoważnienie do przetwarzania danych pełni) zdaniem audytora powinno ono zawierać min.:

- datę i miejscowość,
- oświadczenie podpisane wraz z datą
- wykaz systemów informatycznych, w których przetwarzane są dane osobowe
- termin obowiązywania upoważnienia
- podpis ADO
- numer zgodny z prowadzoną ewidencją.

Wskazuje się, iż trzon RODO stanowi **zasada podejścia opartego na ryzyku** (risk based approach). Powyższa zasada oznacza, że administratorzy i podmioty przetwarzające samodzielnie przeprowadzają szczegółową analizę prowadzonych procesów przetwarzania danych w jednostce i samodzielnie dokonują oceny ryzyka, na jakie przetwarzanie danych w konkretnym przypadku jest narażone. Art. 24 RODO zobowiązuje administratorów i podmioty przetwarzające do uwzględnienia charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia oraz odpowiednio do nich dobierać i wdrażać środki techniczne i organizacyjne, tak aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Zdaniem audytora opracowanie zasad nadawania i likwidacji upoważnień do przetwarzania danych osobowych stanowi jeden z elementów skutecznej kontroli nad procesem przetwarzania danych osobowych.

Administrator decydując o tym, którzy pracownicy potrzebują upoważnienia do przetwarzania danych osobowych musi najpierw ustalić, którzy pracownicy w ogóle przetwarzają dane, a następnie ustalić zakres przetwarzanych danych.

Warto zaznaczyć, iż formalne nadanie upoważnienia stanowi dla ADO z jednej strony zabezpieczenie dowodowe w przypadku zmaterializowania się ryzyka nieuprawnionego ujawnienia danych osobowych, a z drugiej umożliwia skuteczną kontrolę zarządczą.

## Opis audytowanych Jednostek

## 1.3. Ocena kontroli zarządczej.

Obszar *„System nadawania i likwidacji uprawnień do przetwarzania danych osobowych"* audytor ocenia **pozytywnie z uchybieniami.**

W trakcie zadania audytowego stwierdzono, iż w niektórych Jednostkach nie wszyscy pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych. Powyższe stoi w sprzeczności z zapisami **standardu nr 2 (kompetencje zawodowe)**, który wskazuje, iż osoby zarządzające oraz pracownicy powinni posiadać wiedzę, umiejętności i doświadczenie pozwalające skutecznie i efektywnie wypełniać powierzone zadania. Ponadto pracodawca powinien zapewnić rozwój kompetencji zawodowych pracowników.

Zgodnie z zapisami **standardu nr 4 (delegowanie uprawnień)** zakres uprawnień delegowanych poszczególnych osobowo należało określić w sposób precyzyjny, a przyjęcie delegowanych uprawnień winno być potwierdzone podpisem. Z kolei czynności audytowe wykazały, iż w części analizowanych przypadków zakres przydzielonych uprawnień do zbiorów informatycznych nie był zgodny z realizowanym zakresem czynności przez pracowników. Pracownicy przetwarzali dane osobowe w systemach informatycznych, do których nie mieli nadanych uprawnień w formie upoważnień lub zakres wskazanych w upoważnieniu systemów nie pokrywał się z zapisami w zakresie w czynności.

**Tabela nr 1**
**Zbiorczy kwestionariusz**

| | [redacted] | [redacted] | PP17 | [redacted] | [redacted] | [redacted] | [redacted] |
|---|---|---|---|---|---|---|---|
| Czy audytorom nadano upoważnienia do przetwarzania danych osobowych w zakresie objętym audytem? | tak | tak | tak | tak | tak | tak | tak |
| Czy upoważnienia nadane audytorom zostały ujęte w ewidencji upoważnień? | nie | nie | tak | tak | nie | tak | tak |
| Czy upoważnienia nadane audytorom posiadały numer? | nie | tak | tak | nie | nie | tak | nie |
| Czy upoważnienie nadane audytorom zawierało oświadczenie? | nie | nie | tak | tak | nie | tak | tak |
| Czy oświadczenie zostało podpisane przez audytorów z datą? | nd | nd | tak | tak | nd | tak | tak |
| Czy Polityka bezpieczeństwa została wprowadzona zarządzeniem Dyrektora Jednostki? | nie | tak | tak | nie | tak | nie | tak |
| Czy Polityka bezpieczeństwa została ujęta w Księdze zarządzeń? | nie | tak | tak | nie | nie | nie | tak |
| Czy Polityka (w treści) lub Zarządzenie określało czas wejścia w życie? | nie | tak | tak | nie | tak | nie | nie |
| Czy Zarządzenia są ewidencjonowane zgodnie z JRWA? | nie | nie | nie | nie | nie | nie | nie |
| Czy Polityka bezpieczeństwa została zatwierdzona przez Dyrektora Jednostki? | nie | tak | tak | tak | tak | tak | tak |
| Czy Polityka bezpieczeństwa była kompletna tj. zawierała wszystkie załączniki? | nie | tak | tak | tak | nie | nie | tak |
| Czy w Polityce bezpieczeństwa usankcjonowano instrument zabezpieczający jakim jest upoważnienie? | tak | tak | tak | tak | tak | tak | tak |
| Czy upoważnieniom nadano numery? | nie | nie | nie | tak | nie | nie | nie |
| Czy numery upoważnień były zgodne z ewidencją? | nd | nd | nd | nie | nd | nd | nd |
| Czy ewidencja upoważnień była prowadzona chronologicznie? | tak | tak | tak | tak | nie | nie | tak |
| Czy została przeprowadzona analiza ryzyka | tak | tak | tak | tak | nie | nie | tak |
| Czy w Jednostce funkcjonuje JRWA? | tak | tak | tak | tak | tak | tak | tak |
| Czy JRWA zostało zatwierdzone przez Archiwum Państwowe? | nie | tak | tak | tak | | tak | tak |
| Czy JRWA zostało wprowadzone Zarządzeniem Dyrektora? | nie | tak | tak | nie | tak | tak | tak |

*wysłano pismo do Archiwum Państwowego

W **tabeli numer 1** ujęto zbiorcze zestawienie pod kątem dokonania oceny kontroli zarządczej, funkcjonującej w audytowanych Jednostkach.

Poniższy opis dotyczy nieprawidłowości wykazanych w tabeli nr 1.

*Wyjaśnienia Dyrektora PP17 z dnia 27.02.2019:*
*„Zakwestionowano /Zbiorczy kwestionariusz – Tabela nr 1/ kompletność Polityki bezpieczeństwa obowiązującej w Publicznym Przedszkolu nr 17 im. Majki Jeżowskiej z powodu braku załączników. Pragnę wyjaśnić, że segregator zawierający dokumentację ochrony danych osobowych obowiązującą na placówce, zawierał wszystkie załączniki określone w Polityce, które ze względu na ich praktyczną przydatność nie zostały „wypożyczone" audytorom na okres kontroli wraz z Polityką bezpieczeństwa. Znajdowały się one jednak w wyżej wymienionej dokumentacji, do której kontrolujący mieli nieograniczony wgląd w trakcie udostępnienia jej podczas czynności audytowych prowadzonych na terenie placówki".*
Wyjaśnienia przyjęto i uwzględniono w Tabeli nr 1.

Zgodnie z treścią Komunikatu nr 23 z dnia 16 grudnia 2009 roku *w sprawie standardów kontroli zarządczej dla sektora finansów publicznych*, standardy kontroli zarządczej w zakresie mechanizmów kontroli, stanowią zestawienie podstawowych mechanizmów, które mogą funkcjonować w ramach systemu kontroli zarządczej. Zwraca się jednak uwagę, iż nie jest to katalog zamknięty, ponieważ system kontroli zarządczej powinien być elastyczny i dostoswany do specyficznych potrzeb jednostki.
Wytyczne **standardu nr 11 (dokumentacja systemu kontroli zarządczej)** wskazują, iż procedury wewnętrzne (do których zalicza się Politykę bezpieczeństwa danych osobowych), dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników (w tym upoważnienia do przetwarzania danych osobowych), stanowią dokumentację systemu kontroli zarządczej. Sposób prowadzenia tej dokumentacji, w powiazaniu z zapisami **standardu nr 15, określającym mechanizmy kontroli dotyczące systemów informatycznych**, z jednej strony powinien zapewnić bezpieczeństwo danych i systemów informatycznych, a z drugiej zapewniać wypełnienie zasad przetwarzania danych osobowych wskazanych w art.5 ust 1 lit.b RODO tj.: zgodności z prawem, rzetelności i przejrzystości. W przedmiotowym zakresie stwierdzono nieprawidłowości polegające na:

- upoważnienia do przetwarzania danych osobowych, wystawione dla audytorów wewnętrznych, nie zostały ujęte w Ewidencji upoważnień;
- brak numeracji upoważnień utrudniający powiązanie wystawionych upoważnień z prowadzoną Ewidencją;
- upoważnienia wystawione audytorom wewnętrznym nie posiadały oświadczeń zobowiązujących do przestrzegania zasad ochrony danych osobowych;
- Ewidencja upoważnień nie była prowadzona chronologicznie;

Należy wskazać, iż powyższe nieprawidłowości zdaniem audytora, w znacznym stopniu utrudniają skuteczne sprawowanie kontroli zarządczej przez Administratora Danych Osobowych. Prowadzenie dokumentacji w sposób przejrzysty i rzetelny zapewnia ADO, iż jest w stanie wykazać na każdy moment działania Jednostki, którzy pracownicy, jakie dane i w jakich systemach przetwarzają. Powyższe ma szczególne znaczenie w sytuacji gdy nastąpiłoby nieuprawnione udostępnienie danych osobowych, za które w pierwszej kolejności odpowiadałby ADO - dlatego tak ogromne znaczenie ma **wprowadzenie skutecznych mechanizmów zabezpieczających interesy ADO**.

Ponadto wskazuje się na potrzebę uporządkowania dokumentacji w zakresie procedur wewnętrznych tj.:

- każda Polityka bezpieczeństwa danych osobowych powinna zostać wprowadzona w formie Zarządzenia Dyrektora z określeniem daty wejścia w życie;
- Zarzadzanie powinny być numerowane zgodnie z przyjętym JRWA;
- zatwierdzone przez Archiwum Państwowe JRWA należy wprowadzić w formie Zarządzenia Dyrektora.

**Rekomendacja**

**W przypadku procedur wewnętrznych oraz dokumentacji, prowadzonych w ramach ochrony danych osobowych, stosować się do zasady przejrzystości i rzetelności RODO oraz do zapewnienia skutecznej kontroli zarządczej przez Dyrektora Jednostki tj. stosowanie JRWA, wprowadzanie procedur w formie Zarządzeń Dyrektora, chronologiczna Ewidencja upoważnień powiązana z ich numeracją itp .**

*Wyjaśnienia Dyrektora PP17 z dnia 27.02.2019:*

*„Nie zgadzam się z kwestionowanym brakiem spójności ewidencjonowania wprowadzanych Zarządzeń Dyrektora Przedszkola zgodnie z Jednolitym*

*Rzeczowym wykazem Akt obowiązującym na placówce /Zbiorczy kwestionariusz – Tabela nr 1/. Wyjaśniam, iż podczas kontroli audytorzy mieli wgląd do wszystkich Zarządzeń Dyrektora Przedszkola wydanych w roku 2012 zgromadzonych i przechowywanych w skoroszycie. Pierwsza kartka umieszczona w tym skoroszycie zawierała między innymi symbol oznaczenia teczki – 0221, pod którym widniał pełny wykaz zewidencjonowanych Zarządzeń Dyrektora z roku 2012 – pierwsza strona ewidencji w załączeniu - co jest zgodne z obowiązującym na placówce JRWA. Sposób numerowania Zarządzeń Dyrektora jest powszechnie przyjęty i stosowany we wszystkich placówkach oświatowych /oraz innych jednostkach w Jastrzębiu-Zdroju/, gdyż ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych – dalej r.i.k. określa instrukcję kancelaryjną, sposób klasyfikowania i kwalifikowania dokumentacji w formie jednolitych rzeczowych wykazów akt oraz instrukcję w sprawie organizacji i zakresu działania archiwów zakładowych jedynie dla organów gminy i związków międzygminnych, organów powiatu, organów samorządów województwa i organów zespolonej administracji rządowej w województwie, a także urzędów obsługujących te organy. Zatem przepisy zawarte w r.i.k. nie dotyczą szkół i przedszkoli. W przypadku wątpliwości proponuję wystąpić o opinię w tej sprawie do archiwum państwowego."*

Audyt wykazał w trakcie zadania audytowego prawidłowość stosowania i używana narzędzia kontroli zarządczej jakim jest stosowanie JRWA, natomiast Dyrektor Jednostki podejmuje decyzje o sposobie prowadzenia dokumentacji, tak aby zapewnić skuteczny nadzór nad działalnością Jednostki. Sposób prowadzenia dokumentacji nie był przedmiotem zadania audytowego w zakresie zgodności z JRWA, a wskazane przez Audytorów uwagi w przedmiotowym zakresie miały jedynie za zadanie zwrócenie uwagi Kierowników na kwestie porządkowe, które można wprowadzić w Jednostce. Wskazana w sprawozdaniu rekomendacja została sformułowana w sposób bardzo ogólny tak aby to Dyrektor Jednostki, po uwzględnieniu stopnia ryzyka, wprowadził takie mechanizmy kontroli, które uważa za skuteczne.

Artykuł 24 RODO wskazuje na przyjęcie podejścia opartego na ryzyku poprzez wdrożenie (przez ADO) odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z niniejszym Rozporządzeniem i aby

móc to wykazać. Środki te w razie potrzeby należy poddawać przeglądom i uaktualniać. W RODO pojęcie ryzyka odnosi się do naruszenia praw i wolności osób, których dane są przetwarzane (art.25 ust.1 RODO). Szacowanie ryzyka jest podstawą budowy systemu ochrony danych osobowych. W procesach przetwarzania danych osobowych do naruszenia przedmiotowych praw i wolności może dojść w wyniku nieprawidłowo skonstruowanych procedur przetwarzania, w tym niewłaściwego ich zabezpieczenia – niewłaściwej ochrony przed dostępem osób nieuprawnionych. Jak wcześniej wykazano, we wszystkich audytowanych jednostkach, w procedurach wewnętrznych usankcjonowano instrument zabezpieczający jakim jest upoważnienie tj. najważniejszy dokument na mocy, którego ADO nadaje uprawnienia.

Czynności audytowe wykazały, iż w sześciu Jednostkach na siedem audytowanych, przeprowadzono analizę ryzyka w tym: w pięciu sporządzono Arkusze zarządzania ryzykiem (o bardzo zbliżonej treści zarówno dla przedszkoli jak i zespołów szkół) a w jednym przypadku Analizę zagrożeń i ryzyka (bardzo ogólne zapisy). Arkusze te zawierały jedynie analizę samych zagrożeń. Natomiast zgodnie z art. 25 oraz art. 26 RODO, elementem niezbędnym do tego aby dokonać analizy ryzyka w organizacji jest ocena tego, jakie aktywa biorą udział w przetwarzaniu danych osobowych. Aktywem organizacji jest każdy element, który ma dla niej wartość. Mogą to być pracownicy, sprzęt ale także procesy biznesowe, klienci czy też mechanizmy działania w ramach organizacji.

Dopiero drugim etapem analizy ryzyka, który powinien być przeprowadzony po identyfikacji aktywów, biorących udział w przetwarzaniu danych osobowych, jest stworzenie listy potencjalnych zagrożeń dla przetwarzania danych osobowych.

Ponadto wskazać należy, iż szacowanie ryzyka w audytowanych jednostkach określono w Tabeli jako POZIOM RYZYKA który zawierał mnożnik prawdopodobieństwa do skutku, a wynik świadczyć miał o poziomie tego ryzyka. Jednakże nie wskazano w jaki sposób z przyjętej macierzy ryzyka (brak jej określenia) kwalifikowano na poziom niski, średni lub wysoki.

Analiza ryzyka we wszystkich przypadkach została przygotowana przez Inspektora Ochrony Danych Osobowych, którego funkcje w sześciu Jednostkach była sprawowana przez *Przedsiębiorstwo Usługowo – Szkoleniowe* [redacted] a w jednej *Twoja Bezpieczna Firma*. Obowiązek powołania IODO przez instytucje publiczne wynikał z zapisów art.37 ust.1a RODO, z kolei jego zadania określono w art.39 RODO, gdzie w ustępie drugim niniejszego artykułu

wskazano, iż IODO wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cel przetwarzania.

**Rekomendacja**

**Analizę ryzyka przeprowadzać przy uwzględnieniu aktywów biorących udział przy przetwarzaniu danych osobowych oraz określić sposób kwalifikacji poziomu ryzyka .**

**Pouczenie dla naczelnika/kierownika audytowanej jednostki**

Zgodnie z par. 19 *Rozporządzenia w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz.U. z 2015 poz.1480)* audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając na piśmie Naczelnika Wydziału Kontroli i Audytu Wewnętrznego oraz Prezydenta Miasta, na formularzu stanowiącym załącznik do sprawozdania.

W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko Prezydentowi Miasta i audytorowi wewnętrznemu.

Słownik:

| | |
|---|---|
| *RODO* | - ROZPORZĄDZENIE 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) |

Załączniki:

1. Dobór próby do zadania
2. Opis ZSZ
3. Opis PŻ nr 1
4. Opis PP nr 17
5. Opis CKP
6. Opis SP nr 12
7. Opis SP nr 21
8. Opis PP nr 21

Egzemplarz sprawozdania otrzymują:

1. Prezydent Miasta
2. Naczelnik Wydziału Edukacji
3. Dyrektor Zespołu Szkół Zawodowych
4. Dyrektor Publicznego Żłobka nr 1
5. Dyrektor Publicznego Przedszkola nr 17
6. Dyrektor Centrum Kształcenia Praktycznego
7. Dyrektor Szkoły Podstawowej nr 12
8. Dyrektor Publicznego Przedszkola nr 21
9. Dyrektor Szkoły Podstawowej nr 21