DOKUMENTACJA DO PRZEPROWADZENIA AUDUTU

WEWNĘTRZNEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Fundamentem RODO jest zasada rozliczalności

Akty Prawne

- **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)**
- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24)**
- **Kodeks Pracy** - (t. j. Dz. U. z 2018 r. poz. 917 z późn. zm.). **art. 100**

  § 1. Pracownik jest obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub umową o pracę.

  § 2. Pracownik jest obowiązany w szczególności:

  5) przestrzegać tajemnicy określonej w odrębnych przepisach,

art. 5 ust. 2 RODO:

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (rozliczalność);

art. 24 ust. 1 RODO:

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze administrator

wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się

zgodnie z niniejszym rozporządzeniem i aby móc to wykazać;

Do zakresu obowiązków IOD, związanych z realizacją zadań audytowych, należy:

- powiadomienie komórki audytowanej o planowanej realizacji zadania audytowego,
- założenie i prowadzenie dokumentacji zadania audytowego oraz pozostałej dokumentacji audytu wewnętrznego,
-przeprowadzenie narady otwierającej (uzgodnienie z audytowanym kryteriów oceny mechanizmów kontrolnych w obszarze działalności jednostki objętym zadaniem),
- przeprowadzenie czynności audytowych,
- odpowiednie udokumentowanie ustaleń audytu,
- przeprowadzenie narady zamykającej (uzgodnienie z audytowanym wstępnych wyników audytu wewnętrznego, w szczególności ustaleń i propozycji zaleceń),
- zapoznanie się ze zgłoszonymi przez audytowanego zastrzeżeniami do wstępnych wyników audytu,
- sporządzenie i przekazanie sprawozdania z audytu,
- monitorowanie realizacji zaleceń,
- przeprowadzanie czynności sprawdzających,
- wykonywanie czynności doradczych.

SPOTKANIE OTWIERAJĄCE

1. **Przedstawienie IOD.**
   Marek Łochocki

2. **Przedstawienie celu audytu i zatwierdzenie go przez audytowanego.**

- ocena skuteczności ochrony danych osobowych;

- weryfikacja zgodności wynikającej z dokumentów normatywnych;

- spełnienie przez organizację wymagań w zakresie ochrony danych osobowych stosując zasadę rozliczalności na podstawie przepisów zawartych w – ROZPORZĄDZENIU 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) i Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24

- zbadanie aktualnego stanu ochrony danych osobowych według RODO.

- sprawdzenie opracowanej dokumentacji dotyczącej ochrony danych osobowych wynikającej
  z zasady rozliczalności.

  Audyt przeprowadzany jest na poziomie ochrony danych osobowych nie obejmuje zatem kontroli poprawności konfiguracji sprzętu informatycznego i oprogramowania oraz testów penetracyjnych).

3. **Przedstawienie zakresu audytu według zasady rozliczalności w zakresie:**

   1) Prawnym

   a) informacje, klauzule dotyczące przetwarzania danych osobowych na stronie www , BiP jednostki organizacyjnej.

4. **Przedstawienie metodyki audytu.**

   Metod bezpośredniej analizy dokumentów na stronie www/BiP

   Zbieranie informacji i sprawdzenie, czy na stronie www/BiP umieszczone są wszystkie niezbędne informacje dot. przetwarzania danych osobowych.

5. **Przedstawienia planu audytu**.

   - przedstawienie planu audytu (zał. Plan Audytu)

6. **Ustalenie osób ze strony organizacji audytowanej biorących udział w audycie (udzielających odpowiedzi na pytania, dostarczających dokumenty, udział informatyka)**

   - **Wiesława Godziebiewska**
   - **Anna Siekierska**
   - **Monika Stafiej**
   - brak ograniczeń do przeprowadzenia audytu.

8. **Przedstawienie metody raportowania**.

   Wyniki audytu przedstawiane będą w formie raportu z audytu. Odbiorcą raportu będzie Dyrektor jednostki, w której audyt był prowadzony. Zapisy w raporcie będą jasne i zrozumiałe dla odbiorcy. Identyfikacja nieścisłości będzie poparta dowodem, czyli danymi świadczącymi o jej istnieniu. Dowody mogą być zdobyte przez udzielone odpowiedzi audytowanych, obserwacje.

   Celem dokumentowania nieścisłości jest określenie skutecznych działań naprawczych. Punktem wyjściowym do wprowadzenia działań naprawczych, realizowanych na podstawie zawartych w raporcie zaleceń, jest zrozumienie problemu. Dobrze sformułowany opis niezgodności może być pomocny w określeniu efektu występującego problemu i wskazaniu jego przyczyny. To z kolei znacznie ułatwi dobór zabezpieczeń w celu usunięcia problemu lub zmniejszenia ryzyka jego ponownego wystąpienia.

   Opis nieścisłości będzie opierał się na porównaniu:

   1) zastanego stanu faktycznego w zakresie ochrony danych osobowych z zapisami zawartymi w RODO i zasadami rozliczalności,

   Nieścisłość wynikająca z porównania będzie miała miejsce wówczas, gdy nie została opracowana dokumentacja i procedury w zakresie ochrony danych osobowych oraz niewłaściwie realizowana jest w organizacji ochrona danych osobowych.

   W momencie, gdy IOD stwierdzi, że istnieją wystarczające przesłanki do stwierdzenia niezgodności (tzn. zebrał dowody na istnienie niezgodności) powinien poinformować o tym audytowanego. IOD nie powinien ukrywać swoich obserwacji i obaw wynikających z wykrytych niezgodności aż do zakończenia audytu. Po uzgodnieniu faktów audytowany powinien dowiedzieć się o zapisaniu niezgodności. Wszystkie zidentyfikowane niezgodności powinny być omówione z audytowanym i przez niego podpisane. Takie podejście świadczy o rzetelności audytu.

   Opis niezgodności powinien być zwięzły, konkretny i poparty dowodami. Z jednej strony musi być na tyle obszerny, aby zawarte były w nim wszystkie istotne fakty i okoliczności odkrycia niezgodności, a z drugiej strony na tyle krótki, jak to tylko jest możliwe.

   Przy opisywaniu niezgodności, w celu utrzymania dokładności i zwięzłości, należy rozpatrzyć następujące kwestie:

1) gdzie zaobserwowano niezgodność? — wskazanie miejsca pozwoli na podjęcie działań prewencyjnych lub natychmiastowych działań korygujących, zależnie od skali niezgodności

2) dlaczego jest to niezgodnością? — odniesienie do naruszonego wymagania

Każda zapisana niezgodność powinna być oceniona w przyjętej przez audytora skali. **Z praktyki wynika, Przyjętą skalą do klasyfikacji niezgodności jest określenie poziomu zgodności w skali trzystopniowej. Najwygodniej poziom zgodności opisać cyframi 1, 2, 3 lub literami A, B, C, przy czym I (A) - niezgodność mała, 2 (B) — niezgodność średnia, 3 (C) — niezgodność duża. Jeżeli niezgodności nie występują – to uważamy ten obszar za spełniający wymagania.**

W momencie określania poziomu zgodności dla sformułowanej niezgodności należy rozważyć jak duże konsekwencje będzie miała ta niezgodność na system ochrony danych osobowych, jeżeli nie zostanie poprawiona, jakie jest prawdopodobieństwo wystąpienia tych konsekwencji oraz jak szybko i przy jakim wysiłku niezgodność może być usunięta.

Niezależnie od przyjętej konwencji klasyfikacji IOD zawsze musi umieć ocenić, czy wykryta niezgodność jest poważna i trudna do usunięcia, czy mała i nie pociąga za sobą zasadniczej zmiany systemu ochrony danych osobowych.

9. Zamknięcie spotkania otwierającego.

Uczestnicy Narady

- **Wiesława Godziebiewska**
- **Anna Siekierska**
- **Monika Stafiej**

(pieczątka i podpis kierownika komórki audytowanej) (pieczątka i podpis IOD

Protokół ze Spotkania Zamykającego

Temat Zadania Audytowego - Ocena funkcjonowania ochrony danych osobowych w Szkole Podstawowej w Łążynie

Cel Zadania Audytowego – przedstawione cele audytu przedstawione na spotkaniu otwierającym zostały osiągnięte.

Uzgodnienie wstępnych wyników audytu (w tym ustaleń i propozycji zaleceń)
Obszar edytowany spełnia wymagania. Na stronie www szkoły znajdują się wszystkie niezbędne klauzule informacyjne oraz informacja i dane osobowe inspektora danych osobowych.

Uczestnicy spotkania

- **Wiesława Godziebiewska**
- **Anna Siekierska**
- **Monika Stafiej**

Data spotkania
02.07.2020 r.

(pieczątka i podpis kierownika komórki audytowanej) (podpis IOD)