70 Kal. A.F. + d/w DZ

31.03.2016.

SPRAWOZDANIE Z PRZEPROWADZONEGO ZADANIA ZAPEWNIAJĄCEGO

Temat zadania zapewniającego: Funkcjonowanie jednostek organizacyjnych Powiatu Sępoleńskiego – ochrona danych osobowych

Cel zadania zapewniającego: wydanie oceny na temat zgodności realizacji procedur w ramach przepisów ustawy o ochronie danych osobowych

Podmiotowy zakres zadania zapewniającego (jednostka audytowana): Zarząd Drogowy w Sępólnie Krajeńskim

Przedmiotowy zakres zadania zapewniającego: weryfikacja organizacji ogólnego procesu kontroli zarządczej

Imię i nazwisko audytora wewnętrznego przeprowadzającego zadanie: Tomasz Niedźwiedź

Data rozpoczęcia zadania zapewniającego: 19.11.2015

ZARZĄD DROGOWY
w Sępólnie Krajeńskim
wpł. dn. 31. 03. 2016
l. zał. ..... l. dz. 644
Podpis .....

Nied

STRESZCZENIE WYNIKÓW AUDYTU ORAZ OPINIA W SPRAWIE ADEKWATNOŚCI, SKUTECZNOŚCI I EFEKTYWNOŚCI KONTROLI ZARZĄDCZEJ W OBSZARZE RYZYKA OBJĘTYM ZADANIEM ZAPEWNIAJĄCYM

Podczas realizacji czynności zadania audytowego nie stwierdzono nieprawidłowości / uchybień z zakresu przepisów ustawy ochronie danych osobowych.

W trakcie prowadzonych prac uzyskano wiarygodne dowody stanowiące podstawę do formułowania wniosków na temat ryzyk (w tym potencjalnych ryzyk) występujących w jednostce audytowanej w zakresie przeprowadzonego audytu.

Szczegółowy opis zawarty jest w części sprawozdania - ustalenie stanu faktycznego.

System organizacji nadzoru oraz kontroli zarządczej w jednostce audytowanej określony został odpowiednimi dokumentami / aktami wewnętrznymi wprowadzającymi stosowanie m.in.:

- Zarządzenie nr ZD-PO.120.06.2015.AF Dyrektora Zarządu Drogowego w Sępólnie Krajeńskim z dnia 18.06.2015 w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Zarządzie Drogowym w Sępólnie Krajeńskim

Kontrola zarządcza (wewnętrzna) realizowana jest poprzez system kontroli funkcjonalnej.

W zakresie badanego obszaru nie wydano żadnej rekomendacji.

Opinia w sprawie adekwatności, skuteczności i efektywności systemu kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym.

Badanie systemu kontroli zarządczej było przeprowadzone w takim zakresie, w jakim wiąże się ono z obowiązkami nałożonymi przez przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

Przeprowadzone badanie testowe, ocena dokumentów źródłowych oraz procedur, pozwalają ocenić funkcjonowanie systemu kontroli zarządczej na poziomie wystarczającym

Obszary objęte badaniem audytora:

1. DOKUMENTACJA OPISUJĄCA PRZETWARZANIE DANYCH
2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI
3. SZKOLENIA
4. EWIDENCJA OSÓB UPOWAŻNIONYCH
5. OBOWIĄZEK INFORMACYJNY

USTALENIE STANU FAKTYCZNEGO WRAZ Z ICH KRYTERIAMI OCENY; WSKAZANIE SŁABOŚCI KONTROLI ZARZĄDCZEJ ORAZ ANALIZA ICH PRZYCZYN; SKUTKI LUB RYZYKA WYNIKAJĄCE ZE WSKAZANYCH SŁABOŚCI KONTROLI ZARZĄDCZEJ; ZALECENIA W SPRAWIE WYELIMINOWANIA SŁABOŚCI KONTROLI ZARZĄDCZEJ LUB WPROWADZENIE USPRAWNIEŃ

1. DOKUMENTACJA OPISUJĄCA PRZETWARZANIE DANYCH

kryterium

ustawa o ochronie danych osobowych

Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

§ 3.[Instrukcja] 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".

2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 4.[Polityka bezpieczeństwa] Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 5.[Zawartość instrukcji] Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe,
b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Ustalenia
Zarządzenie nr ZD-PO.120.06.2015.AF Dyrektora Zarządu Drogowego w Sępólnie Krajeńskim z dnia 18.06.2015 w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Zarządzie Drogowym w Sępólnie Krajeńskim
Załącznik do zarządzania. Polityka bezpieczeństwa.
Załącznik nr 1 do Polityki Bezpieczeństwa. Upoważnienie dla ABI.
Załącznik nr 2 do Polityki Bezpieczeństwa. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.
Załącznik nr 3 do Polityki Bezpieczeństwa. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
Załącznik nr 4 do Polityki Bezpieczeństwa. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.
Załącznik nr 5 do Polityki Bezpieczeństwa. Oświadczenie pracowników.
Załącznik nr 6 do Polityki Bezpieczeństwa. Ewidencja osób przetwarzających dane.
Załącznik nr 7 do Polityki Bezpieczeństwa. Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
Załącznik nr 8 do Polityki Bezpieczeństwa. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych.
Załącznik do zarządzania. Instrukcja zarządzania systemem informatycznym.

Audytor nie zgłosił żadnych zastrzeżeń do ww. procedur.

2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Kryterium
Ustawa o ochronie danych osobowych
Art. 36a. 1. Administrator danych może powołać administratora bezpieczeństwa informacji.
2. Do zadań administratora bezpieczeństwa informacji należy:
1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7.

3. Rejestr, o którym mowa w ust. 2 pkt 2, jest jawny. Przepis art. 42 ust. 2 stosuje się odpowiednio.

4. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2.

5. Administratorem bezpieczeństwa informacji może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;

3) nie była karana za umyślne przestępstwo.

6. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w ust. 5.

7. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

8. Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2.

Art. 36b. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.

Art. 46b. 1. Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

2. Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:

1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;

2) dane administratora bezpieczeństwa informacji:

a) imię i nazwisko,

b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,

c) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 1;

3) datę powołania;

4) oświadczenie administratora danych o spełnianiu przez administratora bezpieczeństwa informacji warunków określonych w art. 36a ust. 5 i 7.

3. Zgłoszenie odwołania administratora bezpieczeństwa informacji powinno zawierać:

1) dane, o których mowa w ust. 2 pkt 1 i pkt 2 lit. a i b;

2) datę i przyczynę odwołania.

4. Na żądanie administratora danych lub administratora bezpieczeństwa informacji Generalny Inspektor wydaje zaświadczenie o zarejestrowaniu administratora bezpieczeństwa informacji.

5. Administrator danych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w ust. 2, w terminie 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.

Ustalenia

Administrator danych zgłosił powołanie Administratora Bezpieczeństwa Informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
Data powołania ABI od 18.06.2015.

3. SZKOLENIA

Kryterium

Norma PN-ISO/IEC 17799, pkt 6.2, zaleca się szkolenie użytkowników w zakresie procedur bezpieczeństwa i właściwego użycia urządzeń do przetwarzania informacji w celu zminimalizowania możliwego ryzyka związanego z bezpieczeństwem.
Ponadto zaleca się, aby wszyscy pracownicy instytucji, a jeśli jest to konieczne, także użytkownicy – osoby trzecie – pochodzący spoza instytucji, przeszli właściwe, okresowo uaktualniane, przeszkolenie w zakresie polityk i procedur obowiązujących w instytucji, zanim zostanie im przyznany dostęp do informacji lub usług.

ustalenia

Osoba powołana na ABI uczestniczyła w dniu:
- 02.03.2015 w seminarium pn. „Nowelizacja ustawy o ochronie danych osobowych"
- 27.07.2015 w szkoleniu pn. „Ochrona danych osobowych dla ABI"

Jednostka audytowana (ABI) przeprowadzała w dniu 18.06.2015 szkolenia wewnętrzne pracowników z zakresu ustawy ochrony danych osobowych.
Brak uwag.

4. EWIDENCJA OSÓB UPOWAŻNIONYCH

Kryterium

Ustawa o ochronie danych osobowych
Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
Art. 39. 1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
1) imię i nazwisko osoby upoważnionej;
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Ustalenia

Na podstawie przeglądu stwierdzono nadanie pracownikom stosownych upoważnień do przetwarzania danych osobowych.
Jednostka audytowana prowadzi ewidencję osób przetwarzające dane. Zakres danych ewidencji: Lp., imię i nazwisko, stanowisko służbowe, data nadania upoważnienia, data ustania upoważnienia,

wykaz zbiorów danych wynikających z upoważnienia, identyfikator (jeżeli dane są przetwarzane w systemie informatycznym).

Upoważnienie do przetwarzania danych osobowych nadawane jest na czas pełnienia obowiązków służbowych. W upoważnieniu zostały określone zasoby (zbiory) danych osobowych w celu ich przetwarzania. Upoważnienie zostało podpisane przez pracownika.

Oświadczenie: Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności Polityki Bezpieczeństwa oraz respektowania zapisów ustawy o ochronie danych osobowych. Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami ustawy o ochronie danych osobowych oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Brak uwag.

5. OBOWIĄZEK INFORMACYJNY

Kryterium

Ustawa o ochronie danych osobowych

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) prawie dostępu do treści swoich danych oraz ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;

2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Nieobj

Ustalenia

W aktach spraw prowadzonych przez Zarząd Drogowy zamieszczono zapis „Administratorem Pana/Pani danych osobowych jest Dyrektor Zarządu Drogowego w Sępólnie Krajeńskim Powiatu Sępoleńskiego z siedzibą przy ul. Koronowskiej 5 w Sępólnie Krajeńskim. Dane są przetwarzane wyłącznie w celu ustosunkowania się i udzielenia odpowiedzi na Pana/Pani korespondencję, jak również w celu archiwizacji. Przysługuje Panu/Pani prawo dostępu do treści swoich danych osobowych oraz ich poprawiania. Podanie danych jest dobrowolne, jednakże niezbędne do udzielenia Panu/Pani odpowiedzi."

Brak uwag.

6. KOMENTARZ. ZAPIS O CHARAKTERZE DORADCZO / INFORMACYJNYM.

A. Szkolenia w zakresie bezpieczeństwa danych osobowych.

Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe winien być poddany przeszkoleniu w zakresie przepisów prawnych dotyczących ochrony danych osobowych obowiązujących przy korzystaniu z systemu informatycznego w jednostce. Za przeprowadzenie szkolenia odpowiada administrator bezpieczeństwa informacji, za jego zorganizowanie odpowiada przełożony szkolonych pracowników. Szkolenie w szczególności powinno obejmować:

- Przedstawienie ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych
- Przedstawienie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji
- Przedstawienie podstawowych zasad ochrony danych osobowych przetwarzanych w systemie informatycznym w jednostce, a m.in.:
  - strategii i polityki jednostki w zakresie ochrony danych osobowych przetwarzanych w systemie informatycznym,
  - odpowiedzialności za zabezpieczenie przetwarzanych danych przez użytkowników systemu informatycznego,
  - zabezpieczeń technicznych, z którymi zetkną się użytkownicy systemu informatycznego i z których będą korzystać,
  - zasad zarządzania dostępem do danych osobowych przetwarzanych w systemie informatycznym,
  - obowiązku użytkowników w zakresie zabezpieczenia i zachowania w tajemnicy użytkowanych haseł,
  - zasad ochrony antywirusowej obowiązujących w jednostce, a zwłaszcza powinność użytkowników systemu informatycznego przetwarzającego dane osobowe,
  - zasad użytkowania nośników przenośnych zawierających dane osobowe,
  - zasad bezpiecznego serwisowania sprzętu informatycznego służącego do przetwarzania i przechowywania danych osobowych,
  - zasad zabezpieczenia wydruków danych osobowych,
  - zabezpieczenia dostępności danych osobowych przez tworzenie kopii zapasowych przetwarzanych danych osobowych,
  - zasad korzystania z komputerów przenośnych przetwarzających dane osobowe,
  - sposobu reagowania na incydenty związane z utratą bezpieczeństwa danych osobowych, a zwłaszcza poinformowania administratora bezpieczeństwa informacji i zabezpieczenia dowodów incydentu,

- konsekwencji w przypadku nieprzestrzegania zasad zabezpieczenia procesów przetwarzania danych osobowych w systemie informatycznym.

Szkolenie zostaje zakończone podpisaniem przez słuchacza dokumentu zawierającego: imię i nazwisko słuchacza, datę odbycia szkolenia, imię i nazwisko osoby prowadzącej, oświadczenie o wzięciu udziału w szkoleniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia obowiązujących zasad korzystania z systemu informatycznego przetwarzającego dane osobowe oraz zasad ochrony tych danych.

Dokument ten jest przechowywany przez administratora bezpieczeństwa informacji i stanowi podstawę do podejmowania działań w celu nadania pracownikowi uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

B. Zarządzanie ryzykiem

Administrator bezpieczeństwa informacji jest odpowiedzialny za koordynację działań związanych z zarządzaniem ryzykiem w zakresie przetwarzania danych osobowych w systemie informatycznym. Zarządzanie ryzykiem w zakresie przetwarzania danych osobowych obejmuje: identyfikację danych osobowych przetwarzanych w systemie informatycznym; identyfikację procesów krytycznych dla ciągłości funkcjonowania jednostki związanych z przetwarzaniem danych osobowych; identyfikację i wartościowanie zagrożeń mających wpływ na bezpieczeństwo przetwarzanych danych osobowych; identyfikację i określenie znaczenia podatności systemu informatycznego na zagrożenia związane z bezpieczeństwem danych osobowych; określenie aktualnego poziomu ryzyka związanego z przetwarzaniem danych osobowych; określenie sposobu postępowania z ryzykiem – akceptacji lub zmniejszenia ryzyka poprzez wdrożenie właściwych mechanizmów zabezpieczających; określenie mechanizmów zabezpieczających i określenie ryzyka po wdrożeniu mechanizmów zabezpieczających; akceptację ryzyka po wdrożeniu mechanizmów zabezpieczających – ryzyka szczątkowego.

Istotne jest żeby każdy kierownik komórki organizacyjnej jednostki zobowiązany był do zidentyfikowania, we współpracy z administratorem bezpieczeństwa informacji, danych osobowych przetwarzanych w podległej sobie komórce organizacyjnej, zgodnie z art. 6 ustawy o ochronie danych osobowych.

Identyfikacja procesów krytycznych powinna być przeprowadzana na podstawie m.in. wywiadów z kierownikami komórek organizacyjnych jednostki lub osobami przez nich upoważnionymi. Za identyfikację procesów krytycznych w zakresie przetwarzania danych osobowych odpowiada administrator bezpieczeństwa informacji.

Wywiady mające na celu identyfikację procesów krytycznych obejmują: ustalenie procesów realizowanych w komórce organizacyjnej, w trakcie których odbywa się przetwarzanie danych osobowych; opisanie potencjalnych skutków przerwania realizacji procesu na okres: np. jednej godziny, czterech godzin, jednego dnia, czterech dni, jednego tygodnia, dwóch tygodni; określenie, czy istnieje okres np. koniec miesiąca, wybrane miesiące w roku, w którym skutki przerwania procesu mogą być mniejsze lub większe; zakwalifikowanie, wraz z uzasadnieniem, procesu do jednej z poniżej wymienionych grup: procesy krytyczne, procesy istotne i procesy wspomagające.

Administrator bezpieczeństwa informacji jest odpowiedzialny za przeprowadzenie identyfikacji zagrożeń związanych z przetwarzaniem danych osobowych w systemie informatycznym oraz za określenie częstotliwości występowania zagrożeń w ciągu roku

Analiza zagrożeń obejmuje m.in. poniższe zdarzenia: pożar, powódź, wyładowania atmosferyczne, wysokie i niskie temperatury, awaria zasilania, kradzież mienia jednostki, wahania napięcia w sieci

energetycznej, awaria sieci wodociągowej (brak wody, pęknięcie rury), awaria sprzętu informatycznego, awaria oprogramowania, awaria systemów klimatyzacyjnych, awaria innych urządzeń technicznych wspomagających działanie systemu informatycznego, błędne wprowadzenie danych do systemu informatycznego, błędne operacje wykonywane przez pracowników w systemie informatycznym, promieniowanie elektromagnetyczne, przypadkowe i celowe zablokowanie działania systemu informatycznego itp.

Administrator bezpieczeństwa informacji jest odpowiedzialny za oszacowanie ryzyka związanego z przetwarzaniem danych osobowych w systemie informatycznym w sposób umożliwiającym przypisanie poziomu ryzyka: poszczególnym elementom systemu informatycznego i procesów związanych z zarządzaniem nim i użytkowaniem go w jednostce; poszczególnym podatnościom występującym w elementach systemu informatycznego i procesach związanych z zarządzaniem nim i użytkowaniem go w jednostce – w celu określenia odpowiednich zabezpieczeń.

USTALENIA, PRZYCZYNY, SKUTKI, REKOMENDACJE:

Poniżej przedstawiono podsumowanie kluczowych kwestii, jakie wynikają z przeprowadzonego zadania audytowego. W poniższej tabeli audytor wewnętrzny odniósł się jedynie do systemów jakie zostały przebadane w obszarze będącym przedmiotem działań audytorskich w toku realizacji zadania audytowego.

Poniższa tabela podsumowuje kwestie ustaleń, zaleceń i rekomendacji (z podkreśleniem ich istotności), które zostały szczegółowo przedstawione w rozdziale ustalenia i zalecenia.

Obszar objęty badaniem audytora	Liczba rekomendacji wraz z określeniem nadanego im znaczenia			Ocena zaleceń / rekomendacji
	Zalecenia / Rekomendacje kluczowe	Zalecenia / Rekomendacje znaczące	Zalecenia / Rekomendacje wymagające uwagi	
1. DOKUMENTACJA OPISUJĄCA PRZETWARZANIE DANYCH, str. 3-4	Nie wydano rekomendacji.			
2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI, str. 4-6	Nie wydano rekomendacji.			
3. SZKOLENIA, str. 6	Nie wydano rekomendacji.			
4. EWIDENCJA OSÓB UPOWAŻNIONYCH, str. 6-7	Nie wydano rekomendacji.			
5. OBOWIĄZEK INFORMACYJNY, str. 7-8	Nie wydano rekomendacji.			
KOMENTARZ. ZAPIS O CHARAKTERZE DORADCZO / INFORMACYJNYM – str. 8-10 *A. Szkolenia w zakresie bezpieczeństwa danych osobowych.* *B. Zarządzanie ryzykiem.*				

Dokonano klasyfikacji ustaleń według następujących hierarchii przypisanych im ryzyk:

Wysokie – oznacza, że dana kategoria stanowi ryzyko obarczone poważnymi następstwami finansowymi bądź mają duże znaczenie dla efektywności badanego systemu. Występujące błędy powodują: znaczące straty materialne, utratę dochodów budżetowych, naruszenie przepisów prawa (brak reakcji rodzi odpowiedzialność karną lub dyscypliny finansów publicznych), destabilizują pracę jednostki, nieprawidłowości w korzystaniu z funduszy UE, wywołują zdecydowanie negatywną reakcję opinii publicznej, prowadzą do nieuzasadnionego ekonomicznie lub nieefektywnego wykorzystania czasu – pieniędzy personelu lub innych zasobów jednostki, powodują, że istotne informacje lub sprawozdania są niedostępne lub niewiarygodne.

Średnie – oznacza słabe punkty, które nie mają implikacji tak istotnych jak wyżej wymienione dla funkcjonowania systemu, stanowią jednak ryzyko dla JSFP i muszą zostać usprawnione, po to by obniżyć to ryzyko do akceptowalnego poziomu. Kwestie te powinny zostać uregulowane w krótkim okresie czasu. Powtarzające się błędy mogą spowodować w krótkim okresie czasu znaczące straty materialne, brak reakcji może doprowadzić do naruszenia prawa lub dyscypliny finansów publicznych, powtarzające się błędy mogą spowodować zakłócenia w funkcjonowaniu jednostki, występujące błędy powodują, że mniej istotne informacje są niedostępne lub niewiarygodne,

Nieobs

występujące błędy powodują pogorszenie efektywności wykorzystania zasobów jednostki, występujące błędy mogą mieć negatywny wpływ na opinię publiczną.
Niskie – oznacza drobne uchybienia, sytuację lub czynności, które wymagają usprawnienia w celu bardziej skutecznego działania, co powinno być zrobione w okresie krótkim do średnie-go. Występujące nieprawidłowości: w dłuższym okresie czasu mogą spowodować niewielkie straty materialne jednocześnie nie powodują zakłóceń w funkcjonowaniu jednostki, nie powodują naruszenia prawa ani nie rodzą odpowiedzialności dyscypliny finansów publicznych, stanowią naruszenie wewnętrznych uregulowań (instrukcji, regulaminów) lub zasad współżycia społecznego, powodują brak satysfakcji pracowników.

Ustalenia, zalecenia / rekomendowane działania usprawniające zostały sformułowane odpowiednio do ustaleń poczynionych przez audytora i odnoszą się do poszczególnych elementów badanych w toku zadania audytowego.
Mają one na celu udzielenie racjonalnego zapewnienia, że istniejące struktury wewnętrzne oraz funkcjonujący system kontroli zarządczej gwarantuje odpowiedni poziom i jakość wykonywanych zadań.

Wszystkie rekomendacje zostały ocenione w skali od 1 do 3 w celu określenia ich znaczenia dla prawidłowego funkcjonowania jednostki audytowanej. Skala od A do C została zastosowana w celu wskazania okresu, w jakim działania wskazane przez rekomendacje powinny zostać podjęte

Ocena	*Ryzyko*	*Znaczenie nadanej oceny*	
1	*Wysokie*	*Kluczowa*	*system kontroli zarządczej jest niedostateczny*
2	*Średnie*	*Znacząca*	*system kontroli zarządczej jest niedostateczny pod kilkoma istotnymi względami*
3	*Niskie*	*Wymagająca uwagi*	*dostrzeżono słabości w systemie kontroli zarządczej, wobec których należy podjąć stosowne działania*
A	*Natychmiast*		*działania winny zostać podjęte bezzwłocznie*
B	*W krótkim okresie*		*działania winny zostać podjęte w ciągu 2 - 6 miesięcy*
C	*W średnim okresie*		*działania winny zostać podjęte w ciągu 12 miesięcy*

Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego (wyciąg)
§ 25. 1. Kierownik komórki audytu wewnętrznego albo audytor usługodawcy przekazuje sprawozdanie kierownikom komórek audytowanych objętych zadaniem zapewniającym. W przypadku objęcia zakresem zadania zapewniającego kilku komórek audytowanych audytor wewnętrzny może przekazać kierownikowi komórki audytowanej tylko tę część sprawozdania, która dotyczy działalności kierowanej przez niego komórki.
2. **Po otrzymaniu sprawozdania kierownik komórki audytowanej może zgłosić na piśmie dodatkowe wyjaśnienia lub umotywowane zastrzeżenia do treści sprawozdania, w terminie określonym przez audytora wewnętrznego nie krótszym niż 7 dni kalendarzowych od dnia otrzymania sprawozdania.**

[Audytor określił ww. termin na 7 dni kalendarzowych]

3. W przypadku otrzymania dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania audytor wewnętrzny dokonuje ich analizy i w miarę potrzeby podejmuje dodatkowe czynności wyjaśniające w tym zakresie, a w przypadku stwierdzenia w części albo w całości ich zasadności zmienia lub uzupełnia treść sprawozdania.
4. W przypadku nieuwzględnienia dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania, w części albo w całości, audytor wewnętrzny przekazuje na piśmie swoje stanowisko wraz z uzasadnieniem kierownikowi komórki audytowanej.
5. Dodatkowe wyjaśnienia lub umotywowane zastrzeżenia do treści sprawozdania oraz kopię stanowiska, o którym mowa w ust. 4, audytor wewnętrzny włącza do akt bieżących.
§ 26. 1. Po rozpatrzeniu dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania audytor wewnętrzny przekazuje sprawozdanie kierownikowi jednostki i kierownikowi komórki audytowanej, a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, także dyrektorowi generalnemu urzędu.
2. W przypadku niezgłoszenia dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania audytor wewnętrzny, po upływie terminu, o którym mowa w § 25 ust. 2, przekazuje sprawozdanie kierownikowi jednostki, a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, także dyrektorowi generalnemu urzędu, informując o tym kierownika komórki audytowanej.
3. Kierownik komórki audytowanej – a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, także dyrektor generalny urzędu – w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania może przedstawić na piśmie kierownikowi jednostki swoje stanowisko wobec przedstawionego sprawozdania.
§ 27. 1. Kierownik komórki audytowanej w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne, wyznacza osoby odpowiedzialne za ich realizację oraz ustala sposób i termin ich realizacji, powiadamiając o tym pisemnie audytora wewnętrznego oraz kierownika jednostki – a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, także dyrektora generalnego urzędu – w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.
2. W przypadku odmowy realizacji zaleceń kierownik komórki audytowanej powiadamia pisemnie audytora wewnętrznego oraz kierownika jednostki – a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, także dyrektora generalnego urzędu – o przyczynach odmowy w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.
3. W przypadku gdy kierownik komórki audytowanej, o której mowa w § 2 pkt 2 lit. a, c albo e, nie dokona czynności wymienionych w ust. 1 lub odmówi realizacji zaleceń, kierownik jednostki – w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne – wyznacza osoby odpowiedzialne za ich realizację oraz ustala termin ich realizacji, powiadamiając o tym audytora wewnętrznego oraz, w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu, dyrektora generalnego urzędu.
4. W przypadku gdy kierownik komórki audytowanej, o której mowa w § 2 pkt 2 lit. b albo d, nie dokona czynności wymienionych w ust. 1 lub odmówi realizacji zaleceń, kierownik jednostki – w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne – w ramach uprawnień posiadanych na podstawie odrębnych przepisów wyznacza osoby odpowiedzialne za ich realizację oraz ustala termin ich realizacji, powiadamiając o tym audytora wewnętrznego.

§ 28. 1. Audytor wewnętrzny po upływie terminów realizacji zaleceń, o których mowa w § 27 ust. 1, 3 i 4, zwraca się do kierowników komórek audytowanych objętych zadaniem o informację na temat działań podjętych w celu realizacji zaleceń oraz stopnia ich realizacji.
2. Audytor wewnętrzny dokonuje analizy informacji, o których mowa w ust. 1, uwzględniając w szczególności ocenę ryzyka występującego w obszarze ryzyka objętym zadaniem zapewniającym.
3. Audytor wewnętrzny może przeprowadzić czynności sprawdzające, dokonując oceny działań jednostki podjętych w celu realizacji zaleceń.
4. Ustalenia poczynione w trakcie czynności sprawdzających oraz ich ocenę audytor wewnętrzny zamieszcza w notatce informacyjnej, którą przekazuje kierownikowi jednostki oraz kierownikowi komórki audytowanej, w której byty przeprowadzane czynności sprawdzające.
5. W przypadku przeprowadzania czynności sprawdzających w komórkach audytowanych, o których mowa w § 2 pkt 2 lit. b i d, audytor wewnętrzny przekazuje notatkę informacyjną kierownikowi jednostki oraz kierownikom tych komórek.

DATA SPORZĄDZENIA SPRAWOZDANIA, 28.12.2015

AUDYTOR WEWNĘTRZNY
mgr Tomasz Niedźwiedź
zaświadczenie Min. Fin. 494/2004

KANCELARIA [illegible]
Tomasz [illegible]
ul. [illegible]
NIP [illegible]
tel. [illegible]