Załącznik do Zarządzenia nr 371./2016 Kierownika Ośrodka Pomocy Społecznej Gminy Lubawa z dnia 28 kwietnia 2016r. w sprawie ustalenia planu sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa

Plan sprawdzeń
z zakresu przestrzegania zasad ochrony danych osobowych

na okres od 01 maja 2016r. do 31 grudnia 2016r.

Plan sprawdzeń sporządzony zgodnie z § 3 ust. 2 pkt. 1 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

Przedmiotem sprawdzenia jest zgodność zasad przetwarzania danych osobowych obowiązujących w Ośrodku Pomocy Społecznej Gminy Lubawa z przepisami o ochronie danych osobowych a w szczególności:

- prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbiorów danych,
- funkcjonowanie systemów zabezpieczeń systemowych,
- funkcjonowanie zastosowanych zabezpieczeń fizycznych,
- zasady przechowywania dokumentów zawierających dane osobowe oraz zasady ich zabezpieczania po zakończeniu pracy,
- zasady i sposoby likwidacji oraz archiwizowania zbiorów danych,
- realizacja procedur wdrożonych przez ADO w zakresie ochrony danych osobowych.

Zakres sprawdzeń i ich szczegółowa tematykę:

1. Zgodność opracowanej polityki bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi z obowiązującymi przepisami.
2. Upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych.
3. Ewidencja wydanych upoważnień oraz jej zgodność z wydanymi upoważnieniami.
4. Stosowanie w praktyce zasad określonych w polityce bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych, instrukcji zarządzania systemem informatycznym, w zasadach korzystania z komputerów służbowych oraz ochrony własności intelektualnej.
5. Ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym.
6. Zabezpieczenie dokumentów zawierających dane osobowe (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym).
7. Przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy – na podstawie obserwacji oraz rozmów z nimi.
8. Sposób niszczenia niepotrzebnych dokumentów.
9. Dostęp pracowników do zbiorów danych oraz zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień).
10. Legalność przetwarzania danych osobowych - spełnianie warunków postawionych w art. 23 ust.1 ustawy.
11. Obowiązek informacyjny wynikający z art. 24 ustawy.
12. Respektowane praw osób, których dane są przetwarzane (rozdział 4 ustawy).

13. Zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
14. Przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie.
15. Blokowanie systemu, podczas opuszczenia stanowiska pracy w trakcie dnia pracy.
16. Upoważnienia osób dopuszczonych do pracy w systemie.
17. Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi.
18. Poziom ochrony systemów informatycznych słuŜących do przetwarzania danych osobowych przed osobami trzecimi.
19. Zabezpieczenie systemowe i fizyczne sprzętu komputerowego.
20. Tworzenie kopii zapasowych.
21. Odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywane na danych osobowych przez użytkowników.
22. Sposób niszczenia danych wygenerowanych z systemów.

Plan sprawdzeń z zakresu ochrony danych:

Lp.	Stanowisko podlegające kontroli (pracowik, który zgodnie z zakresem czynności wykonuje dane obowiazki)	Pomieszczenie podlegajace kontroli	Zbiory danych podlegajace kontroli	Systemy teleinformatyczne podlegajace kontroli	Planowany termin i czas trwania kontroli
1.	Asystent rodziny, Specjalista pracy socjalnej,	Pokój w budynku przy ul. 19-go stycznia 25, I piętro	Rodziny korzystające ze wsparcia i sysemu pieczy zastepczej	---	16-17 maja 2016 r.
2.	Inspektor, Podinspektor ds. finansowo-ksiegowych,	Pokój nr 16 Pokój nr 4	Dodatki mieszkaniowe	DODATKI MIESZKANIOWE PUMA	9-10 czerwca 2016r.
3.	Podinspektor,	Pokój nr 16	Baza danych wnioskodawców ubiegajacych się o przyznanie Karty Dużej Rodziny	RI KDR	5 września 2016r.
4.	Starszy specjalista pracy socjalnej, Specjalista pracy socjalnej, Procownik socjalny,	Pokój nr 3	Baza danych wnioskodawców ubiegajacych się o przyznanie zasiłku z systemu pomocy społecznej	---	28-30 września 2016r.
5.	Specjalista pracy socjalnej, Konsultant,	Pokój w budynku przy ul. 19-go stycznia 25, I piętro	Baza danych uczestników i absolwentów Klubu Integracji Społecznej	Microsoft Access	17-18 października 2016r.

Sporządził: Edyta Ochocka

Zatwierdzam:

Kierownik
Ośrodka Pomocy Społecznej
Gminy Lubawa

Adam Roznerski

Sprawdzenia dokonuje się wg poniższego wyszczególnienia:

1. Pierwszy etap – sprawdzenia dokumentacji.
   a) Czy zostały opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi.
   b) Czy oba dokumenty są zgodne z obowiązującymi przepisami.
   c) Czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia.
   d) Czy wszystkie osoby, które mają dostęp do danych osobowych zostały zapoznane z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych.
   e) Czy prowadzona jest ewidencja upoważnień.
   f) Czy ewidencja jest zgodna z posiadanymi upoważnieniami.

2. Nastepny etap – sprawdzanie stanu faktycznego na podstawie obserwacji oraz wywiadów z pracownikami.
   a) Sprawdzamy, czy stosowane są w praktyce zasady określone w polityce bezpieczeństwa.
   b) Sprawdzamy ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym.
   c) Sprawdzamy, czy dokumenty zawierające dane osobowe są odpowiednio zabezpieczone.
   d) Sprawdzamy, czy pracownicy przestrzegają procedur związanych z zabezpieczeniem danych w trakcie pracy – na podstawie obserwacji oraz rozmów z nimi.
   e) Sprawdzamy, czy niepotrzebne dokumenty są we właściwy sposób niszczone.
   f) Ustalamy do jakich zbiorów danych i w jakim zakresie mają dostęp pracownicy i czy otrzymali odpowiednie upoważnienia.
   g) Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia.
   h) Sprawdzamy, czy wszystkie dane są przetwarzane legalnie, czyli czy został spełniony jeden z warunków postawionych w art. 23. ust.1 ustawy.
   i) Sprawdzamy, czy biblioteka wypełnia należycie obowiązek informacyjny wynikający z art. 24 ustawy.
   j) Sprawdzamy, czy respektowane są prawa osób, których dane są przetwarzane (rozdział 4 ustawy).

3. Ostatnim etapem – sprawdzenie bezpieczeństwa teleinformatycznego. Porównujemy stan faktyczny z zapisami z instrukcji zarządzania systemami informatycznymi, w szczególności:
   a) Sprawdzamy zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
   b) Sprawdzamy, czy przestrzegane są zasady rozpoczęcia i zakończenia pracy w systemie.
   c) Czy pracownicy blokują system, podczas opuszczenia stanowiska pracy w trakcie dnia pracy.
   d) Czy osoby dopuszczone do pracy w systemie mają odpowiednie upoważnienia.
   e) Czy stosuje się identyfikatory i hasła dla użytkowników zgodnie z wymogami formalnymi.
   f) Czy systemy informatyczne służące do przetwarzania danych osobowych zapewniają odpowiedni poziom ochrony przed osobami trzecimi.
   g) Czy sam sprzęt komputerowy jest odpowiednio zabezpieczony systemowo i fizycznie (np. przed wyniesieniem).
   h) Czy tworzone są kopie zapasowe i czy umożliwiają odzyskanie danych,
   i) Czy systemy służące do przetwarzania danych osobowych odnotowują wszelkie czynności wykonywane na danych osobowych przez użytkowników.
   j) Czy pracownicy niszczą dane wygenerowane z systemów, gdy są już niepotrzebne.
   k) Przeprowadzamy wywiady z pracownikami, by porównać teorię z praktyką.

Sprawdzenia dokonuje się wg poniższego wyszczególnienia:

4. Pierwszy etap – sprawdzenia dokumentacji.
   g) Czy zostały opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi.
   h) Czy oba dokumenty są zgodne z obowiązującymi przepisami.
   i) Czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia.
   j) Czy wszystkie osoby, które mają dostęp do danych osobowych zostały zapoznane z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych.
   k) Czy prowadzona jest ewidencja upoważnień.
   l) Czy ewidencja jest zgodna z posiadanymi upoważnieniami.

5. Nastepny etap – sprawdzanie stanu faktycznego na podstawie obserwacji oraz wywiadów z pracownikami.
   k) Sprawdzamy, czy stosowane są w praktyce zasady określone w polityce bezpieczeństwa.
   l) Sprawdzamy ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym.
   m) Sprawdzamy, czy dokumenty zawierające dane osobowe są odpowiednio zabezpieczone.
   n) Sprawdzamy, czy pracownicy przestrzegają procedur związanych z zabezpieczeniem danych w trakcie pracy – na podstawie obserwacji oraz rozmów z nimi.
   o) Sprawdzamy, czy niepotrzebne dokumenty są we właściwy sposób niszczone.
   p) Ustalamy do jakich zbiorów danych i w jakim zakresie mają dostęp pracownicy i czy otrzymali odpowiednie upoważnienia.
   q) Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia.
   r) Sprawdzamy, czy wszystkie dane są przetwarzane legalnie, czyli czy został spełniony jeden z warunków postawionych w art. 23. ust.1 ustawy.
   s) Sprawdzamy, czy biblioteka wypełnia należycie obowiązek informacyjny wynikający z art. 24 ustawy.
   t) Sprawdzamy, czy respektowane są prawa osób, których dane są przetwarzane (rozdział 4 ustawy).

6. Ostatnim etapem – sprawdzenie bezpieczeństwa teleinformatycznego. Porównujemy stan faktyczny z zapisami z instrukcji zarządzania systemami informatycznymi, w szczególności:
   l) Sprawdzamy zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
   m) Sprawdzamy, czy przestrzegane są zasady rozpoczęcia i zakończenia pracy w systemie.
   n) Czy pracownicy blokują system, podczas opuszczenia stanowiska pracy w trakcie dnia pracy.
   o) Czy osoby dopuszczone do pracy w systemie mają odpowiednie upoważnienia.
   p) Czy stosuje się identyfikatory i hasła dla użytkowników zgodnie z wymogami formalnymi.
   q) Czy systemy informatyczne służące do przetwarzania danych osobowych zapewniają odpowiedni poziom ochrony przed osobami trzecimi.
   r) Czy sam sprzęt komputerowy jest odpowiednio zabezpieczony systemowo i fizycznie (np. przed wyniesieniem).
   s) Czy tworzone są kopie zapasowe i czy umożliwiają odzyskanie danych,
   t) Czy systemy służące do przetwarzania danych osobowych odnotowują wszelkie czynności wykonywane na danych osobowych przez użytkowników.
   u) Czy pracownicy niszczą dane wygenerowane z systemów, gdy są już niepotrzebne.
   v) Przeprowadzamy wywiady z pracownikami, by porównać teorię z praktyką.