ZARZĄDZENIE NR 36/2017
KIEROWNIKA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ W POSTOMINIE

z dnia 5 października 2017 r.

w sprawie planu sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych

Na podstawie §13 ust. 3 Statutu Gminnego Ośrodka Pomocy Społecznej w Postominie nadanego Uchwałą Rady Gminy XXIX/345/04 Rady Gminy Postomino z dnia 17 grudnia 2004 r. z późn. zm. w związku Rozporządzeniem 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 (Dz.U. z 2015 poz. 745)

zarządzam co następuje:

§ 1. Powołuję zespół kontrolny w składzie:

1) Mariusz Wilawer- Administrator Bezpieczeństwa Informacji w Gminnym Ośrodku Pomocy Społecznej w Postominie,
2) Jarosław Modliszewski- Administrator Systemu Informatycznego w Gminnym Ośrodku Pomocy Społecznej w Postominie.

§ 2. Zatwierdzam plan sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych przedstawiony przez administratora bezpieczeństwa informacji zgodnie z § 5 Rozporządzenia, stanowiący załącznik do niniejszego zarządzenia.

§ 3. Zobowiązuje zespól kontrolny po przygotowania sprawozdania po zakończeniu każdego z planowanych sprawdzeń.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Kierownik
Gminnego Ośrodka Pomocy
Społecznej w Postominie
Krystyna Ślebioda

Załącznik nr 1
do Zarządzenia nr 36/2017
Kierownika GOPS
z dnia 05.10.2017

Plan sprawdzeń
z zakresu przestrzegania zasad ochrony danych osobowych

na okres od 09 października 2017 r. do 31 października 2017r.

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 Gminnym Ośrodku Pomocy Społecznej w Postominie 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 z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016, poz. 922).

11. Obowiązek informacyjny wynikający z art. 24 w/w 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 służących 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	Pomieszczenie podlegające kontroli	Zbiory danych podlegający kontroli	System teleinformatyczny podlegający kontroli	Planowany termin i czas trwania kontroli
1.	Referent ds. świadczeń rodzinnych i funduszu alimentacyjnego Młodszy referent ds. świadczeń wychowawczych	Pok. 1	Fundusz Alimentacyjny Świadczenia Rodzinne Pomoc materialna uczniom o charakterze socjalnym Karta Dużej Rodziny Świadczenia wychowawcze	Fundusz Alimentacyjny Świadczenia Rodzinne Pomoc materialna uczniom o charakterze socjalnym BIG InfoMonitor SEPI Karta Dużej Rodziny Rodzina 500+	09- 11 październik 2017

Sporządził:
Mariusz Wilawer Administrator Bezpieczeństwa Informacji
w Gminnym Ośrodku Pomocy Społecznej w Postominie

Zatwierdzam:

Wzór sprawdzamy wg poniższego wyszczególnienia:

Zazwyczaj kontrolę rozpoczyna się od przeprowadzenia sprawdzenia dokumentacji.

23. Czy zostały opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi.
24. Czy oba dokumenty są zgodne z obowiązującymi przepisami.
25. Czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia (na tym etapie sprawdza się tylko, czy administrator wystawia takie upoważnienia i czy ich wzór jest zgodny z przyjętym i obowiązującym w bibliotece).
26. Czy wszystkie osoby, które mają dostęp do danych osobowych zostały zapoznane z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych (administrator powinien mieć ich oświadczenia w tym zakresie).
27. Czy prowadzona jest ewidencja upoważnień.
28. Czy ewidencja jest zgodna z posiadanymi upoważnieniami.

Kolejnym etapem jest sprawdzanie stanu faktycznego na podstawie obserwacji oraz wywiadów z pracownikami.

1. Sprawdzamy, czy stosowane są w praktyce zasady określone przez bibliotekę w polityce bezpieczeństwa.
2. Sprawdzamy ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym.
3. Sprawdzamy, czy dokumenty zawierające dane osobowe są odpowiednio zabezpieczone (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym).
4. Sprawdzamy, czy pracownicy przestrzegają procedur związanych z zabezpieczeniem danych w trakcie pracy – na podstawie obserwacji oraz rozmów z nimi (uwaga należy zadawać pytania, ale nie komentować, nie krytykować, nie zwracać uwagi na złe zachowania).
5. Sprawdzamy, czy niepotrzebne dokumenty są we właściwy sposób niszczone.
6. Ustalamy do jakich zbiorów danych i w jakim zakresie mają dostęp pracownicy i czy otrzymali odpowiednie upoważnienia.
7. Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia.
8. Sprawdzamy, czy wszystkie dane są przetwarzane legalnie, czyli czy został spełniony jeden z warunków postawionych w art. 23. ust.1 w/w ustawy.
9. Sprawdzamy, czy biblioteka wypełnia należycie obowiązek informacyjny wynikający z art. 24 w/w ustawy.
10. Sprawdzamy, czy respektowane są prawa osób, których dane przetwarza biblioteka (rozdział 4 w/w ustawy).

Ostatnim etapem jest sprawdzenie bezpieczeństwa teleinformatycznego. Porównujemy stan faktyczny z zapisami z instrukcji zarządzania systemami informatycznymi, w szczególności:

1. Sprawdzamy zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
2. Sprawdzamy, czy przestrzegane są zasady rozpoczęcia i zakończenia pracy w systemie.
3. Czy pracownicy blokują system, podczas opuszczenia stanowiska pracy w trakcie dnia pracy.
4. Czy osoby dopuszczone do pracy w systemie mają odpowiednie upoważnienia.
5. Czy stosuje się identyfikatory i hasła dla użytkowników zgodnie z wymogami formalnymi.
6. Czy systemy informatyczne służące do przetwarzania danych osobowych zapewniają odpowiedni poziom ochrony przed osobami trzecimi.

7. Czy sam sprzęt komputerowy jest odpowiednio zabezpieczony systemowo i fizycznie (np. przed wyniesieniem).
8. Czy tworzone są kopie zapasowe i czy umożliwiają odzyskanie danych,
9. Czy systemy służące do przetwarzania danych osobowych odnotowują wszelkie czynności wykonywane na danych osobowych przez użytkowników.
10. Czy pracownicy niszczą dane wygenerowane z systemów, gdy są już niepotrzebne.
11. Przeprowadzamy wywiady z pracownikami, by porównać teorię z praktyką.