ZARZĄDZENIE Nr 4 /2021
Dyrektora Miejsko Gminnego Ośrodka Kultury
w Bystrzycy Kłodzkiej
z dnia 07 kwietnia 2021 roku
w sprawie wyznaczenia Administratora Systemów Informatycznych
w MGOK w Bystrzycy Kłodzkiej

Działając w oparciu o art. 24 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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),

wyznaczam Pana Łukasza Wróbla

na funkcję Administratora Systemów Informatycznych (ASI).

Do zadań ASI należy w szczególności;

1. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania.
2. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery przenośne nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych.
3. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności osoby upoważnionej przez administratora.

   W innym przypadku powinna być zawarta umowa powierzenia przetwarzania danych.
4. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym określającej sposób

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

5. Aktualizacja Instrukcji Zarządzania Systemem Informatycznym i Polityki Bezpieczeństwa pod kątem bezpieczeństwa teleinformatycznego.

6. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

7. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.

8. Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych.

9. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

10. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.

11. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie.

12. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło).

13. Monitorowanie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią.

14. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych, o którym mowa w § 20 KRI (Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).
15. Monitorowanie i dokonywanie przeglądów systemu zarządzania bezpieczeństwem informacji (audyty bezpieczeństwa IT).

Niniejsze wyznaczenie wygasa z chwilą ustania Pana zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania Pana przez Administratora z pełnienia ww. funkcji. Jednocześnie informuję, że zobowiązany jest Pan do zachowania w tajemnicy informacji w zakresie danych osobowych i sposobów ich zabezpieczania, również po odwołaniu Pana z pełnienia ww. funkcji, a także po ustaniu zatrudnienia lub współpracy.

Bystrzyca Kł. 07.04.2021 r.
.....
miejscowość, data

.....
podpis administratora

RADCA PRAWNY
Marek Ociepa

DYREKTOR
mgr Ewelina Walczak