

Sprawozdanie

Przeprowadzenie kontroli wewnętrznej z dostosowania i stosowania aktualnych przepisów Ochrony Danych Osobowych (RODO)

1) Oznaczenie administratora danych i adres jego siedziby:

*Kierownik biblioteki – Aneta Juraszek
ul. 1-go Maja , 58-520 Janowice Wielkie
(podać pełną nazwę oraz adres)*

2) Imię i nazwisko Inspektora Ochrony Danych - IOD:

Adam Szumowski

3) Wykaz czynności podjętych przez Inspektora Ochrony Danych (IOD) w toku sprawdzenia:

Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych?

Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?

Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?

Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?

Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?

Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?

Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?

Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?

Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?

Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany?

Czy każdy pracownik otrzymuje unikalny identyfikator do systemów informatycznych?

Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby?

Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób?

Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?

Czy w organizacji jest stosowana polityka tzw. „czystego biurka”?

Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamkniętych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?

Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?

Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane?

Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?

Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe?

Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?

Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych?

Gdzie są przechowywane kopie zapasowe?

Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?

Czy organizacja prowadzi ocenę skutków dla ochrony danych?

Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?

4) Datę rozpoczęcia i zakończenia sprawdzenia:

Kontrola jednodniowa 2024-01-08

5) WYNIK KONTROLI:

NARUSZENIA. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem:

- Stwierdzono brak powołania ASI (Administratora Systemów Informatycznych)

6) Działania podjęte po stwierdzeniu naruszeń:

- Pouczono pracownika o przestrzeganiu polityki bezpieczeństwa publicznego i Instrukcji zarządzania systemem

- Zgłoszono prośbę o wywieszenie w widocznym miejscu klauzul informacyjnych dla pracowników

- Zgłoszono ADO prośbę aby pracownicy odpowiedzialny za dane osobowe zweryfikowali słuszność i ilość przetwarzanych danych osobowych , oraz czy czas jaki można było je przetwarzać nie minął.

7) Wyszczególnienie załączników stanowiących składową część sprawozdania:

Brak

8) Plan następnych kontroli:

a. Sprawdzenie wdrożenia i stosowania zaleceń z obecnej kontroli

.....2024-01-08 Adam Szumowski.....

Podpisano cyfrowo przez Adam Szumowski

Data, miejsce i podpis Inspektora Ochrony Danych Osobowych

.....

Data, miejsce i podpis Administratora Danych Osobowych