*Załącznik **nr 14***
do UCHWAŁY NR 6/2/2022 ZARZĄDU Związku Gmin
i Powiatów Kanału Elbląskiego i Pojezierza Iławskiego
z 17 października 2022 roku

WZÓR KARTY SZKOLENIA WSTĘPNEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Administrator: **ZWIĄZEK GMIN I POWIATÓW KANAŁU ELBLĄSKIEGO I POJEZIERZA IŁAWSKIEGO z siedzibą w Ostródzie**

Adres: **ul. Adama Mickiewicza 24, 14-100 Ostróda,**

Kontakt: **tel. (89) 642 94 00, e-mail: zwiazek@um.ostroda.pl**

Imię i nazwisko osoby odbywającej szkolenie:

……..

Stanowisko:

……..

Instruktaż przeprowadzony:

……..
(data)

STANISŁAWA PAŃCZUK na podstawie materiałów PIOTRA ROBAKOWSKIEGO
(imię i nazwisko przeprowadzającego instruktaż)

W ramach szkoleniach poruszone zostały następujące tematy i zagadnienia:

Zgodnie z Polityką Ochrony Danych Osobowych i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych Związku Gmin i powiatów Kanału Elbląskiego i Pojezierza Iławskiego wymaga się tego, aby:

1) Dostęp do danych osobowych mają osoby posiadające upoważnienie do przetwarzania danych osobowych **(NR …/20… z …… roku).**
2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.
3) Dane były chronione przed dostępem do nich osób nieupoważnionych.
4) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora Danych Osobowych.
7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy.
8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9) Szafy, w których przechowywane są dane, powinny być zamykane na klucz.
10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do szaf.
13) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy.
14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
15) W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
16) Nie należy udostępniać osobom nieupoważnionym tych komputerów.

17) W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności.

18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.

19) Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie.

20) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi.

Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych osobowych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy.
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.
10) Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.
12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane.
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.). Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Uwagi:

……..

Przeczytałem poniższy instruktaż, w pełni go zrozumiałem i zaakceptowałem. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem*

……
(data i podpis osoby, której udzielono instruktażu)

……
(administrator danych - nazwa, pieczątka)

……
(miejscowość, data)

** Podpis jest potwierdzeniem odbycia instruktażu i zapoznania się z przepisami oraz zasadami przetwarzania i ochrony danych osobowych. Podpisaną kartę przechowuje się w aktach osobowych pracowników/stażystów/wolontariuszy.*

Opracowanie: PIOTR ROBAKOWSKI
email: aton.sfb@gmail.com
tel. 691 81 10 02