Regulamin Ochrony Danych Osobowych

w Polskim Stowarzyszeniu na rzecz Osób z Niepełnosprawnością Intelektualną Koło w Gryfinie

1.ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ ZAWIERAJĄCEJ DANE OSOBOWE

1.
Osoby upoważnione (osoby upoważnione do przetwarzania danych osobowych w PSONI Koło w Gryfinie) są zobowiązane do stosowania tzw. „Polityki czystego biurka". Polega ona na uniemożliwieniu dostępu osobom postronnym do danych osobowych (wszelkie informacje o zidentyfikowanej lub możliwej do identyfikacji osobie) poprzez fizyczne zabezpieczanie dokumentów.
2.
Dokumenty zawierające dane osobowe znajdujące się np. na biurku powinny być w trakcie pracy niewidoczne dla osób postronnych np. poprzez zasłonienie dokumentów czystą kartką czy schowanie dokumentów w czasie rozmowy z osobą nieupoważnioną.
3.
Przed opuszczeniem stanowiska pracy(czasowym lub po zakończeniu pracy), osoby upoważnione zobowiązane są zabezpieczyć stanowisko pracy -zamknąć okna, uporządkować i zamknąć na klucz dokumentację np. w szafkach, biurku, zamykanym na klucz pomieszczeniu oraz odwiesić klucz w zaszyfrowanej skrzynce lub adekwatnie do okoliczności pozostawić niezabezpieczone stanowisko pracy pod nadzorem innych osób upoważnionych znajdujących się w tym samym pomieszczeniu.
4.
Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w niezamkniętym i nienadzorowanym pomieszczeniu, na korytarzu, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
5.
Dokumenty niszczy się w niszczarkach.
Wyrzucania niezniszczonych dokumentów jest niedozwolone.
6.
Dokumenty zawierające dane osobowe powinny być właściwie oznaczone i przechowywane zgodnie z przepisami prawa i Instrukcją Kancelaryjną PSONI Koło w Gryfinie.

2. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT

1.
Użytkownik (osoba korzystająca z komputera stacjonarnego, laptopa, dysku sieciowego, programu, systemu informatycznego, poczty elektronicznej, z innego sprzętu IT,

Przetwarzająca dane osobowe) zobowiązany jest do zabezpieczenia sprzętu IT (służbowe komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, tablety i smartfony, pendrive) przed zniszczeniem lub uszkodzeniem.

2.
Sprzęt IT jest odpowiednio zabezpieczony- niedozwolone jest więc przetwarzanie danych osobowych na prywatnym sprzęcie IT, a zwłaszcza na podatnym na zgubienie urządzeniu typu pendrive.
3.
Użytkownik jest zobowiązany niezwłocznie zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT do IOD – (Inspektora Ochrony Danych).
4.
Otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń/programów lub podłączanie urządzeń prywatnych lub niewiadomego pochodzenia do sprzętu IT jest niedozwolone. W wyjątkowych sytuacja należy uzyskać zgodę IOD.
5.
Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, nieuprawnionym pracownikom) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. „Polityka czystego ekranu”.
6.
Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni nieupoważnienie użytkownicy (np. podczas współużytkowania komputera, pożyczenia pendrive)
7.
Użytkownik nie jest uprawniony do niszczenia nośników elektronicznych, powinien przekazać je do IOD, wyjątek stanowią płyty CD/DVD, które należy niszczyć w przeznaczonych do tego niszczarkach.
8.
Przed czasowym opuszczeniem stanowiska pracy lub przed zakończeniem pracy Użytkownik zobowiązany jest zabezpieczyć fizycznie i informatycznie sprzęt IT w sposób określony w Rozdziale 3
9.
Zasady wynoszenia sprzętu IT poza obszar PSONI Koło w Gryfinie reguluje Rozdział 4.

3. ZARZĄDZANIE UPRAWNIENIAMI IPROCEDURA ROZPOCZĘCIA,ZAWIESZENIA I ZAKOŃCZENIA PRACY NA SPRZĘCIE IT.

1.
Każdy użytkownik ma nadany własny, indywidualny identyfikator (login) i hasło.
2.
Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
3.
Bezwzględnie zabronione jest umożliwianie innym osobom
Pracy na koncie użytkownika, również w czasie jego nieobecności np. w czasie urlopu.

4.
Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.
5.
Użytkownik jest zobowiązany do powiadomienia IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
6.
W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym IOD.
7.
Przed czasowym opuszczeniem stanowiska pracy użytkowani zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu a po zakończeniu pracy wylogować się z systemu i wyłączyć komputer oraz w każdym przypadku zabezpieczyć stanowisko pracy - zamknąć okna, zamknąć na klucz sprzęt IT np. w szafkach, biurku, zamykanym na klucz pomieszczeniu oraz odwiesić klucz w zaszyfrowanej skrzynce lub adekwatnie do okoliczności pozostawić niezabezpieczone stanowisko pracy pod nadzorem innych osób upoważnionych znajdujących się w tym samym pomieszczeniu.

4. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA OBSZAR ADMINISTRATORA

Dane osobowe papierowe
1.
Niedopuszczalne jest wynoszenie przez osobę upoważnioną dokumentacji papierowej zawierającej dane osobowe poza obszar PSONI Koło w Gryfinie.
2.
Dokumentacja wynoszona na zewnątrz musi być zabezpieczona przed zgubieniem i kradzieżą, zakazane jest pozostawianie dokumentów w miejscach dostępnych publicznie bez nadzoru, np. w samochodzie, restauracji, na szkoleniu, na korytarzu.
3.
Dopuszczalne jest przesyłanie dokumentów zawierających dane osobowe przesyłką poleconą za pośrednictwem Poczty Polskiej S.A.
4.
Dopuszczalny jest obieg dokumentacji zawierającej dane osobowe za pośrednictwem upoważnionego kurier a zatrudnionego w PSONI Koło w Gryfinie. Dane osobowe na nośnikach elektronicznych:
5.
Dopuszczalne jest wynoszenie nośników elektronicznych zawierających dane osobowe – służbowych, zaszyfrowanych komputerów przenośnych oraz służbowych, zaszyfrowanych pen- drive wyłącznie w sytuacjach wyjątkowych po uzyskaniu zgody bezpośredniego przełożonego lub IOD.
6.
Wymóg uzyskania zgody określonej w pkt 5 nie dotyczy kadry zarządzającej, w tym kierowników placówek PSONI Koło w Gryfino, którzy są zobowiązani do zachowania szczególnej ostrożności.

7.
Dopuszczalne jest wynoszenie poza obszar PSONI Koło w Gryfinie służbowych smartfonów/tabletów. Zgoda nie jest wymagana.
8.
Wynoszenie innych nośników elektronicznych niż określone w pkt 5 i 7może nastąpić w wyjątkowych sytuacjach, wyłącznie po uzyskaniu każdorazowej zgody IOD.
9.
Nośniki elektroniczne wynoszone na zewnątrz muszą być zabezpieczone przed zgubieniem i kradzieżą, zakazane jest pozostawianie nośników w miejscach dostępnych publicznie bez nadzoru, np. w samochodzie, restauracji, szkoleniu, na korytarzu.
10.
Komputery przenośne przechowywane są w dedykowanych do tego futerałach/plecakach.
11.
W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia np.z użyciem VPN, Team Viewer.
Uwierzytelnienie dokonuje się w zależności od systemu z użyciem loginu i podania hasła lub poprzez autoryzację adresu.

5.POLITYKA HASEŁ

1.
Komputery i systemy informatyczne są zahasłowane.
2.
Hasła powinny składać się co najmniej z 8 znaków.
3.
Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
4.
Hasła nie mogą być łatwe do odgadnięcia.
W szczególności nie należy jako haseł wykorzystywać: dat typu „Kwiecien2018”, imion i nazwisk wprost typu Kowalski1, typowych zestawów: ciągów liter/cyfr z klawiatury typu Qwerty 12345 , haseł typu Psoni1234, Orew12345, Księgowość1234 itp.).
5.
Hasła nie można ujawniać innym osobom. Nie wolno zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie itp.
6.
W przypadku ujawnienia hasła –należy natychmiast je zmienić.
7.
System wymusza zmianę hasła co 30 dni.
8.
Użytkownik systemu w trakcie pracy może zmienić swoje hasło.

9.
Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10.
Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym.
11.
Zabrania się stosowania takich samych lub podobnych haseł jako zabezpieczenia w dostępie do różnych systemów.

6. ZASADY KORZYSTANIA Z INTERNETU

1.
Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2.
Niedozwolone jest zgrywanie na dysk twardy oraz uruchamianie aplikacji lub programów prywatnych lub niewiadomego pochodzenia, np. wskazanych w formie odnośnika internetowego.
W wyjątkowych sytuacjach należy uzyskać zgodę IOD, który konsultuje się z informatykiem.
3.
Niedozwolone jest wchodzenia na strony internetowe niewiadomego pochodzenia, na których prezentowane są informacje o charakterze przestępczym, hackerskim lub inne budzące wątpliwości.
4.
Zaleca się w opcjach przeglądarki internetowej nie włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5.
W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, zaleca się zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódki) oraz na adres strony internetowej rozpoczynającej się frazą ”https:” W razie wątpliwości należy skontaktować się z IOD, który konsultuje się z informatykiem.
6.
Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.
7.
Niedozwolone jest podłączania do komputerów prywatnych: modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu Blue Connect, i Plus, Orange Go). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.
W wyjątkowych sytuacja należy uzyskać zgodę IOD, który konsultuje się z informatykiem.

7. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1.
Przesyłanie danych osobowych z użyciem poczty e-maila musi odbywać się z zachowaniem szczególnej ostrożności co do podstawy udostępniania danych i poprawności adresu e-mail odbiorcy.
2.
Dane osobowe przesyłane w formie wiadomości e-mail muszą znajdować się w hasłowanych plikach (minimum 8 znaków) np. z użyciem programu 7 Zip, Winzip, Winrar), a hasło powinno być przesłane w inny sposób np. wiadomość sms, telefonicznie, Skype.
3.
Należy zwracać uwagę na ilość odbiorców i związaną z tym opcję „Ukryte do wiadomości – UDW" i „Do wiadomości –DW" tak by nie doszło do naruszenia ochrony danych osobowych.
4.
Zaleca się, aby użytkownik podczas przesyłania danych osobowych zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
5.
Niedozwolone i szczególnie niebezpieczne jest otwieranie wiadomości e-mail niewiadomego pochodzenia lub budzących wątpliwości, w szczególności zakazane jest
Otwieranie załączników (zip, xlsm, pdf exe) oraz otwieranie hiperlinków zawartych w powyższych wiadomościach.
W wyjątkowych sytuacjach należy uzyskać zgodę IOD, który konsultuje się z informatykiem.
6.
Użytkownicy powinni okresowo kasować niepotrzebne maile
7.
Konta pocztowe firmowe są odseparowane od poczty prywatnej
8.
Z poczty e-mail można korzystać wyłącznie w celach służbowy, poza przypadkami sporadycznymi, wynikającym i w zasad współżycia społecznego i ogólnie przyjętych zasad.
9.
Niedozwolone jest przesyłanie wiadomości e-mail zawierających dane osobowe na prywatną pocztę oraz konfigurowania kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny np. pocztę prywatną.

8.OCHRONA ANTYWIRUSOWA

1.
Sprzęt IT oraz systemy informatyczne objęte są ochroną antywirusową.
2.
Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
3.
Niedozwolone jest wyłączanie systemu antywirusowego, jeśli system antywirusowy taką funkcjonalność posiada.

4.
W przypadku podejrzenia lub stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie IOD, który konsultuje się z informatykiem.

9. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻEŃ I NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

1.
Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
a)
niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
b)
niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
c)
nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. nie stosowanie zasady czystego biurka / ekranu, ochrony haseł, nieuprawnione wynoszenie danych poza PSONI Koło w Gryfinie),
d)
niedbałe przetwarzanie danych osobowych,
2.
Do typowych naruszeń bezpieczeństwa danych osobowych należą:
a)
zdarzenia losowe (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności, awarie serwerów, komputerów, oprogramowania),
b)
nieumyślne naruszenia (pomyłki informatyków, użytkowników, pracowników, utrata/zgubienie danych, udostępnienie danych bez podstawy prawnej, błędy w danych osobowych),
c)
umyślne naruszenia (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, świadome ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
3.
Zabrania się świadomego lub nieumyślnego (lekkomyślnego lub wynikającego z niedbalstwa) wywoływania zagrożeń lub naruszeń przez osoby upoważnione do przetwarzania danych.
4.
Osoba upoważniona powiadamia IOD o wystąpieniu zagrożenia lub naruszenia w zakresie wynikającym z jej obowiązków pracowniczych/umownych.

10. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1.
Niedozwolone jest udostępnianie danych osobowych osobom nieuprawnionym (bez podstawy prawnej przetwarzania), w szczególności:
a)
przekazywanie (ujawnianie) danych osobom fizycznym, firmom, instytucjom, organom państwowym, które są nieuprawnione -nie mogą wykazać się podstawą prawną np. do dostępu do takich danych,
b)
przekazywanie bezpośrednio lub przez telefon danych osobowych osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego,
c)
ujawnianie na grupach dyskusyjnych, forach internetowych, blogach, portalach społecznościowych itp. danych osobowych, w tym wizerunku bez podstawy prawnej do ich ujawnienia,
d)
przekazywanie danych osobom uprawnionym w warunkach umożliwiających zapoznanie się z danymi osobowymi przez osoby postronne np. głośna rozmowa w miejscu publicznym,
e)
Plotkowanie, rozmowa z osobami nieuprawnionymi np. znajomi o danych osobowych pozyskanych w związku z wykonywaną praca/umową.
2.
Podstawą prawą przetwarzania danych osobowych jest m.in. zgoda osoby, której dane są przetwarzane, przepis prawa wskazujący na możliwość przetwarzania danych np. prowadzenie dokumentacji medycznej, interes publiczny, realizacja celów statutowych. W razie wątpliwości osoba upoważniona ma obowiązek skonsultować się z bezpośrednim przełożonym lub IOD.
3.
Udostępnianie danych osobowych innym osobom upoważnionym np. współpracownikom w celu wykonywani zadań pracowniczych/umownych jest dozwolone.
4.
Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
a)
przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w zadaniach powierzonych przez PSONI Koło w Gryfinie,
b)
zachowania danych osobowych w tajemnicy tj. nie udostępniania danych osobowych osobom nieuprawnionym (bez podstawy prawnej przetwarzania),
c)
dbałości o bezpieczeństwo i poprawność przetwarzanych przez mnie danych osobowych,
d)
przestrzegania niniejszego Regulaminu Ochrony Danych Osobowych w PSONI Koło w Gryfinie.

5.
Osoby przeszkolone w zakresie ochrony danych osobowych (ewentualnie zapoznane z treścią niniejszego Regulaminu) zobowiązane są podpisać Oświadczenie o poufności.

11. POSTĘPOWANIE DYSCYPLINARNE

1.
Przypadki znacznego zaniechania lub naruszenia obowiązków wynikających z niniejszego dokumentu mogą zostać potraktowane przez pracodawcę/zleceniodawcę jako ciężkie naruszenie obowiązków pracowniczych/naruszenie zasad współpracy.
2.
Dane osobowe są chronione na podstawie powszechnie obowiązujących przepisów prawna, między innymi na podstawie ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) -tzw. RODO.

Zatwierdzono uchwałą obiegową Zarządu Koła PSONI w Gryfinie nr 29/18 z dnia 23 maja 2018 roku