

Zarządzenie Nr 114/2018 Burmistrza Miasta i Gminy Pieszycy z dnia 21 maja 2018 roku

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Pieszycy

Regulamin Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Pieszycy

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1	Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów	2
2	Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy.....	2
3	Polityka haseł	2
4	Zabezpieczenie dokumentacji papierowej z danymi osobowymi	3
5	Zasady wnoszenia nośników z danymi poza firmę/organizację	3
6	Zasady korzystania z internetu.....	4
7	Zasady korzystania z poczty elektronicznej.....	4
8	Ochrona antywirusowa	5
9	Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.....	5
10	Obowiązek zachowania poufności i ochrony danych osobowych	6
11	Postępowanie dyscyplinarne	6

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT
3. Samowolne instalowanie otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów)
5. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia.
6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych a wykonywane przez informatyków-administratorów
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze)
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia informatyków-administratorów o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje
8. W przypadku, gdy użytkownik podczas próby załogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyków-administratorów
9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS) lub wylogować się z systemu bądź z programu.
11. Zabrania się uruchamiania jakiegokolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. Po zakończeniu pracy, użytkownik zobowiązany jest:
 - a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
 - b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe

3 POLITYKA HASEŁ

1. Hasła powinny składać się z np. 12 znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty
4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić
6. Hasła muszą być zmieniane co **90** dni
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła
8. Użytkownik systemu w trakcie pracy w aplikacji 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 organizacji
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANymi OSOBOWymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczeniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

5 ZASADY WYNOszENIA NOŚNIKÓw Z DANymi POZA FIRME/ORGANIZACJĘ

1. Użytkownicy nie mogą wnosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy. Do takich nośników zalicz się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash
2. Dane osobowe wnoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach
4. Należy korzystać ze sprawdzonych firm kurierskich
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
6. Zabrania się wnoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twarde dyski z zapisanymi danymi osobowymi i pendrive bez zgody ADO
7. Dane osobowe wnoszone poza obszar dokumentacji na nośnikach elektronicznych muszą być zaszyfrowane
8. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
 - a. adresat powinien zostać powiadomiony o przesyłce
 - b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą
 - c. stosować bezpieczne koperty depozytowe
 - d. przesyłkę należy przesyłać przez kuriera

6 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych
2. Zabrania się zgrzywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupelniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel
7. 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 naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przestać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH
7. **WAŻNE:** Nie wolno „kliknąć” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili
9. Zabrania się Użytkownikom rozsyłania „niezawodowych” emaili w formie „tańcuszków szczęścia”, np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile
12. Konta pocztowe służbowe są odseparowane od poczty prywatnej
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych

14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
18. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
20. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

8 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcję posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

9 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, 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. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardej dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
 - a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
 - b. dokumentacja jest niszczone bez użycia niszczarki
 - c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
 - d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe

- e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
- f. wnoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy
- g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
- h. telefoniczne próby wyłudzenia danych osobowych
- i. kradzież, zagubienie komputerów lub CD, twarde dyski, Pen-drive z danymi osobowymi
- j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
- l. hasła do systemów przyklejone są w pobliżu komputera

10 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
 - a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach
 - b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę
 - c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę
 - d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
 - e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

11 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.