

**OBOWIĄZKI PRACOWNIKA
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
W SZKOLE PODSTAWOWEJ NR 2 W MILANÓWKU**

Mając na uwadze przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1), dalej: RODO, uprzejmie informuję, że dla zapewnienia zgodności przetwarzania danych osobowych z powyższym rozporządzeniem oraz odpowiedniego zabezpieczenia danych osobowych **pracownik jest zobowiązany do:**

- 1) zapoznania się z przepisami prawa dotyczącymi ochrony danych osobowych, polityką oraz procedurami z zakresu ochrony danych osobowych obowiązującymi w Szkole Podstawowej nr 2 w Milanówku;
- 2) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez administratora i tylko w celu wykonywania powierzonych mu obowiązków służbowych;
- 3) zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania, o ile z przepisów prawa nie wynika ich udostępnienie, a także złożenia pisemnego oświadczenia o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobów zabezpieczenia, a także przestrzegania zasad przetwarzania danych u administratora;
- 4) do nieutrwalania bez uprzedniej zgody rodzica lub opiekuna prawnego wizerunku dziecka, a także nieudostępniania go lub nierozpowszechniania zwłaszcza z wykorzystaniem Internetu, w tym w szczególności portal społecznościowego;
- 5) odpowiedniego zabezpieczania danych przed ich udostępnieniem osobom nieuprawnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- 6) pilnego strzeżenia nośników danych, w tym dokumentów, płyt, pamięci przenośnych i komputerów przenośnych, których nie należy pozostawiać bez kontroli w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie;
- 7) ustawienia ekranów komputerowych tak, aby osoby postronne nie mogły oglądać ich zawartości, korzystania z wygaszacza ekranu lub innych rozwiązań zabezpieczających;
- 8) niepodłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia;
- 9) dbania o prawidłową wentylację komputerów;
- 10) przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń inspektora ochrony danych;
- 11) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe, pod nieobecność osoby upoważnionej do przetwarzania danych osobowych;
- 12) opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
- 13) prowadzenia korespondencji służbowej przy użyciu wyłącznie służbowej skrzynki mailowej;
- 14) niewynoszenia poza obszar przetwarzania na jakichkolwiek nośnikach zbiorów danych lub ich części, chyba że do takiego działania pracownik jest uprawniony przez administratora lub jest to nieodłącznie związane z wykonywanymi przez niego obowiązkami; zaleca się, by wówczas wynoszone dane miały postać zaszyfrowaną;
- 15) wykonania kopii danych, na których się pracuje, tak często, jak to niezbędne, aby zapobiec ich utracie;
- 16) kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika oraz wyłączeniu komputera, a także zabezpieczeniu pomieszczenia lub miejsca pracy, w którym on się znajduje;
- 17) chowania do szaf zamykanych na klucz wszelkich dokumentów zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;

- 18) usuwania przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy, tak by ich ponowne wykorzystanie nie było możliwe;
- 19) nieużywania powtórnego jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe;
- 20) w przypadku korzystania z drukarek ogólnodostępnych, niezwłocznego zabierania wydruków z drukarki;
- 21) w przypadku korzystania z kserokopiarki, dopilnowania, aby po zakończeniu kopiowania nie pozostawały w niej kopiowane dokumenty;
- 22) umieszczaniu kluczy do pomieszczeń i do szaf w ustalonym, przeznaczonym do tego miejscu po zakończonym dniu pracy i nieujawnianie osobom nieupoważnionym informacji o miejscu przechowywania kluczy;
- 23) zamykania okien w razie zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
- 24) zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
- 25) zabezpieczenia pomieszczenia lub miejsca, w którym przetwarza się dane osobowe, w taki sposób, by nie mogły być one pozyskane przez osobę trzecią;
- 26) składania kluczy w przeznaczonym do tego miejscu wskazanym przez administratora po zakończeniu pracy;
- 27) wykorzystywania przyznanego pracownikowi dostępu do Internetu zgodnie z zakresem powierzonych obowiązków, przy czym pracownik pozostaje świadom, że jego praca w systemach informatycznych, w tym w zakresie korzystania ze stron internetowych jest monitorowana, a nieuprawnione lub nieprawidłowe użycie tego systemu może być podstawą do odebrania mu uprawnień a także pociągnięcia do odpowiedzialności prawno-pracowniczej lub cywilnej;
- 28) niezwłocznego informowania administratora lub IOD o naruszeniu ochrony danych osobowych.