

Na podstawie:

art. 5, ust. 1, lit f 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. L 119 z 4.5.2016)

**REGULAMIN KORZYSTANIA Z PRYWATNYCH URZĄDZEŃ
INFORMATYCZNYCH DO CELÓW SŁUŻBOWYCH
W III LICEUM OGÓLNOKSZTAŁCĄCYM Z ODDZIAŁAMI DWUJĘZYCZNYMI
IM. BOHATERÓW WESTERPLATTE W GDAŃSKU**

§ 1

1. Niniejszy regulamin dotyczy pracowników **III Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi im. Bohaterów Westerplatte w Gdańsku**, którzy w ramach wykonywania obowiązków służbowych przetwarzają dane osobowe za pomocą prywatnych urządzeń informatycznych.
2. Ilekroć w regulaminie jest mowa o:
 - 1) **Administratorze Danych Osobowych** - należy przez to rozumieć **III Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi im. Bohaterów Westerplatte w Gdańsku** ku reprezentowanej przez Dyrektora **III Liceum Ogólnokształcącego z Oddziałami Dwujęzycznymi im. Bohaterów Westerplatte w Gdańsku**, Małgorzatę Mroczkowską;
 - 2) **Użytkownika systemu** – należy przez to rozumieć osobę przetwarzającą dane osobowe za pośrednictwem systemu informatycznego, posiadającą upoważnienie wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną dopuszczoną do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
 - 3) **Osobie uprawnionej** – należy przez to rozumieć osobę wskazaną przez Administratora Danych Osobowych do zarządzania systemami informatycznymi, w tym do nadawania dostępu do przetwarzania danych osobowych w systemach informatycznych oraz do podejmowania czynności w sytuacji podejrzenia naruszenia

ochrony danych osobowych przetwarzanych za pośrednictwem systemów informatycznych;

- 4) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zastosowanych w celu przetwarzania danych osobowych;
- 5) **Urządzeniu informatycznym** – należy przez to rozumieć elementy fizyczne wchodzące w skład systemu informatycznego służące do przetwarzania danych osobowych. W skład urządzeń informatycznych wchodzi stacje robocze (stacjonarne oraz przenośne – notebooki i netbooki), tablety, smartfony, elementy służące do przechowywania danych osobowych (dyski optyczne, dyski magnetyczne, elektroniczne nośniki pamięci), urządzenia wyjściowe (drukarki oraz urządzenia wielofunkcyjne zawierające pamięć wewnętrzną).

§ 2

1. Korzystać z prywatnych urządzeń informatycznych do celów służbowych mogą wyłącznie osoby posiadające pisemną zgodę wydaną przez Administratora Danych Osobowych.
2. Osoby wykorzystujące prywatne urządzenia informatyczne do celów służbowych zobowiązane są stosować się do procedury rozpoczęcia, zawieszenia oraz zakończenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych wprowadzonego odrębnym zarządzeniem.
3. Osoby, które będą przenosić dane osobowe za pomocą prywatnych urządzeń wyposażonych w wewnętrzną pamięć (np. komputery przenośne, smartfony, tablety) lub nośniki danych (np. dyski optyczne, elektroniczne nośniki pamięci) zobowiązane są stosować się do regulaminu przetwarzania danych osobowych poza obszarem administratora.
4. Każda osoba korzystająca z prywatnych urządzeń informatycznych do celów służbowych w momencie uzyskania zgody, o której mowa w ust. 1 składa pisemne oświadczenie o spełnieniu wymogów wynikających z instrukcji zarządzania informatycznymi, niniejszego regulaminu oraz spełnienie wymogów, o których mowa w ust. 2-3.

§ 3

1. Stacja robocza (komputer stacjonarny, notebook, netbook) wykorzystywana do przetwarzania danych osobowych musi spełniać następujące wymagania:

- 1) System operacyjny musi być legalny oraz musi być na nim aktywna funkcja automatycznej aktualizacji;
 - 2) Wszelkie oprogramowanie wykorzystywane w trakcie pracy musi być legalne, a jego licencja musi umożliwiać wykorzystywanie w innych celach niż osobiste;
 - 3) Oprogramowanie antywirusowe musi być stale włączone z aktywną funkcją automatycznej aktualizacji;
 - 4) Oprogramowanie służące ochronie przed zagrożeniami płynącymi z sieci publicznej (zapora ogniowa) musi być stale włączone z aktywną funkcją automatycznej aktualizacji;
 - 5) System operacyjny musi zostać wyposażony w konto użytkownika wykorzystywane wyłącznie przez upoważnionego użytkownika systemu. Hasło do konta użytkownika musi pozostać poufne i wykorzystywane wyłącznie przez użytkownika systemu informatycznego;
 - 6) System operacyjny musi być wyposażony w funkcję automatycznego wygaszenia ekranu, po którego aktywacji wznowienie będzie wymagało podania hasła do konta użytkownika;
2. Jeżeli w ramach przetwarzania danych osobowych korzystając z prywatnych urządzeń informatycznych następuje komunikacja za pośrednictwem sieci publicznej (wchodzenie na strony internetowe, wysyłanie i odbieranie wiadomości elektronicznych, wykorzystywanie oprogramowania służącego wymianie informacji w sieci publicznej) dostęp do sieci musi być zabezpieczony poprzez zastosowanie hasła dostępu.
3. Użytkownik prywatnych urządzeń informatycznych wykorzystywanych do przetwarzania danych osobowych zobowiązany jest w przypadku ich zgubienia lub kradzieży do bezzwłocznego powiadomienia Administratora Danych Osobowych.