

ZARZĄDZENIE NR 234/06/2018
PREZYDENTA MIASTA STAROGARD GDAŃSKI
z dnia 15 czerwca 2018 r.

w sprawie określenia zasad i trybu zabezpieczenia komputerów oraz dokumentów i materiałów zawierających dane osobowe oraz inne informacje prawnie chronione wynoszonych poza obszar pomieszczeń Urzędu Miasta Starogard Gdański

Na podstawie art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994 z późn. zm.¹⁾) oraz art. 32 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. Urz. UE L 2016.119.1) – zwane dalej RODO - zarządza się, co następuje:

§ 1. Pracownicy Urzędu Miasta Starogard Gdański, zwanego dalej Urzędem, z wyłączeniem przypadków określonych w § 2, zobowiązani są do przestrzegania zakazu wnoszenia poza obszar pomieszczeń biurowych Urzędu dokumentów i materiałów, nośników informatycznych oraz komputerów przenośnych zawierających:

- 1) dane osobowe w rozumieniu art. 4 pkt 1 RODO;
- 2) inne informacje prawnie chronione na podstawie ustaw szczególnych.

§ 2. 1. Pracownicy zobowiązani do realizacji zadań służbowych poza obszarem obiektów biurowych Urzędu, w przypadkach wymagających posługiwania się przez nich nośnikami, dokumentami i materiałami, o których mowa w § 1, oraz komputerami przenośnymi, obowiązani są posiadać na tę okoliczność zgodę Prezydenta Miasta Starogard Gdański lub uprawnionych przez Prezydenta osób funkcyjnych oraz przestrzegać zasad postępowania określonych w § 3.

2. Formę zgody, o której mowa w ust. 1 stanowią - po podpisaniu przez Prezydenta Miasta Starogard Gdański:

- 1) zapis w zakresie czynności służbowych pracownika wskazujący na konieczność posługiwania się przez niego w realizacji tych czynności poza obszarem pomieszczeń biurowych Urzędu nośnikami, dokumentami i materiałami, o których mowa w § 1 lub komputerem przenośnym,
- 2) pełnomocnictwa procesowe dla radcy prawnego,
- 3) jednorazowa zgoda udzielona przez Prezydenta Miasta Starogard Gdański na wyjście służbowe określonych pracowników z dokumentami, jak też środkami służącymi do przetwarzania informacji (np. komputerami przenośnymi),
- 4) upoważnienie do odbioru, nadawania i doręczania korespondencji i innych materiałów.

§ 3. Dokumenty i materiały, o których mowa w § 1, podlegające z przyczyn uzasadnionych potrzebami służbowymi konieczności okresowego wyniesienia poza obszar pomieszczeń biurowych Urzędu, muszą być przenoszone (przechowywane) w teczce (pojemniku) zabezpieczonej w sposób uniemożliwiający dostęp osobom nieupoważnionym do danych określonych w § 1.

1 Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1000.

§ 4. 1. Jeżeli zachodzi konieczność wyniesienia poza obszar pomieszczeń biurowych Urzędu informacji, o których mowa w § 1, utrwalonych na nośnikach informatycznych, należy umieścić nośnik w zaklejonej kopercie służącej do przesyłania nośników (koperta „bąbelkowa”), opatrzonej pieczęcią nagłówkową.

2. Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 9 ust. 1 RODO, przekazywane poza obszar pomieszczeń biurowych Urzędu **zabezpiecza się w sposób zapewniający poufność i integralność tych danych.**

3. Do danych osobowych szczególnej kategorii, o których mowa w art. 9 ust. 1 RODO należą: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

§ 5. Wprowadza się następujące zasady dotyczące wykorzystywania komputerów przenośnych:

- 1) osoba użytkująca komputer przenośny, zawierający dane osobowe lub inne informacje podlegające ochronie, ma obowiązek zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem pomieszczeń biurowych Urzędu;
- 2) wykorzystywać należy m. in. środki ochrony kryptograficznej danych osobowych. Osoba sprawująca obowiązki Administratora Systemu Informatycznego Urzędu Miasta zainstaluje w służbowych komputerach przenośnych odpowiednie programy kryptograficzne zabezpieczające dane osobowe i inne informacje podlegające ustawowej ochronie;
- 3) użytkownik służbowego komputera przenośnego winien stosować zabezpieczenie tego urządzenia mechanizmami kontroli dostępu do danych (hasło);
- 4) Administrator Systemu Informatycznego zainstaluje w służbowych komputerach przenośnych oprogramowanie chroniące przed złośliwym oprogramowaniem;
- 5) użytkownicy służbowych komputerów przenośnych wykonywać winni kopie zapasowe danych, które powinny być we właściwy sposób chronione przed kradzieżą lub utratą informacji. Sposób sporządzania i przechowywania tych kopii określi Administrator Systemu Informatycznego,
- 6) obowiązuje zakaz niekontrolowanego pozostawiania komputerów służbowych w samochodach i innych środkach transportu, pokojach hotelowych, centrach konferencyjnych itp.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.