ZARZĄDZENIE NR 198/2020

Burmistrza Miasta i Gminy Ostrzeszów

z dnia 3 listopada 2020 r.

w sprawie zmiany Zarządzenia nr 60/2018 z dnia 25 maja 2020 r. w sprawie wprowadzenia Polityki ochrony danych, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, instrukcji regulującej postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych.

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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), oraz na podstawie rozdziału IIb kodeksu pracy, w związku z art. 3 ustawy z dnia 2 marca 2020 o szczególnych rozwiązanych związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t. j. Dz. U. z 2020 r. poz. 374), w związku z art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2020 r. poz. 713) oraz art. 3^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320), zarządzam co następuje:

§ 1 W Zarządzeniu nr 60/2018 z dnia 25 maja 2018 r. w sprawie w sprawie wprowadzenia Polityki ochrony danych, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, instrukcji regulującej postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych wprowadza się następujące zmiany:

1) §10 otrzymuje brzmienie:

„§10 1. Do przetwarzania danych osobowych Pracodawcy są dopuszczone wyłącznie upoważnione osoby.

2. *Każda osoba podejmująca pracę zdalną, jest zobowiązana do podpisania:*
   - zobowiązania do pracy zdalnej – Załącznik nr 5,
   - oświadczenie – praca zdalna – Załącznik nr 6.
3. *Zabrania się dopuszczania osób postronnych do komputera, telefonu i innych nośników przekazanych przez Pracodawcę oraz informacji w nich zawartych.*
4. *Wszelkie dane przekazane przez Pracodawcę muszą zostać zachowane w tajemnicy. Wszelkie notatki będą przechowywane i zabezpieczone, tak by osoby trzecie nie miały do nich dostępu.*
5. *Zabrania się kopiować/zapisywać dane służbowe na niezabezpieczonych lub prywatnych pendriv'ach oraz innych nośnikach zewnętrznych.*

6. *Komputer, telefon i inne nośniki przekazane przez Pracodawcę służą wyłącznie do pracy służbowej – nie wolno instalować dodatkowego oprogramowania bez nadzoru działu IT, nie można korzystać ze służbowego sprzętu w innych celach niż związanych z pracą.*
7. *Należy przestrzegać zasad korzystania z komputera, telefonu i innych nośników przekazanych przez Pracodawcę zgodnie z obowiązującymi w tym zakresie procedurami, w tym w szczególności zgodnie z wytycznymi i regulaminami IT.*
8. *Należy zwrócić powierzone nośniki wraz z kompletnymi danymi na każde żądanie Pracodawcy.*
9. *Wszelkie dokumenty zawierające dane osobowe nie mogą znajdować się poza siedzibą Pracodawcy przez czas dłuższy niż 5 dni roboczych. W uzasadnionych przypadkach czas ten może ulec wydłużeniu do 15 dni roboczych – po wcześniejszym uzgodnieniu z Pracodawcą.*
10. *Wszelkie materiały zabrane z siedziby pracodawcy na potrzeby pracy zdalnej (oryginały oraz kserokopie), po ich wykorzystaniu należy zwrócić. Niedopuszczalne jest ich niszczenie poza siedzibą administratora.*
11. *Na potrzeby pracy zdalnej powinny być zabierane tylko kopie dokumentów.*
12. *Datę pobrania i zwrotu powyższych dokumentów należy wpisywać w ewidencję pobranych kopii dokumentów zawierających dane osobowe, (załącznik nr 4).*
13. *Ogranicza się liczbę dokumentów wynoszonych z siedziby administratora do tego, co niezbędne w stosunku do celu przetwarzania danych osobowych w ramach pracy zdalnej.*
14. *Odpowiednio zabezpiecza się dane osobowe podczas wynoszenia dokumentacji (np. wynoszenie dokumentów w zabezpieczonej aktówce, przenoszenie dokumentów np. w taki sposób, aby były niewidocznie dla osób trzecich).*
15. *Odpowiednio zabezpiecza się dane w miejscu wykonywania pracy zdalnej (np. przechowywanie dokumentów w zamykanych na klucz szufladach biurka lub szafach, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób, m.in. członków rodziny).*
16. *Wykorzystuje się pozyskane dane osobowe wyłącznie w tym celu, w jakim byłyby wykorzystywane w siedzibie zakładu pracy.*
17. *Bezwzględnie zgłasza się pracodawcy każdy incydent bezpieczeństwa zgodnie z procedurą postępowania w sprawie naruszeń ochrony danych (Instrukcja postępowania w przypadku naruszenia ochrony danych), tak aby administrator mógł się wywiązać z obowiązku nałożonego na mocy art. 33 ust. 1 RODO.*
18. *W przypadku korzystania z prywatnych urządzeń, zgłasza się ten fakt administratorowi, a ponadto upewnia się, że wszystkie urządzenia z których się korzysta mają niezbędne aktualizacje systemu operacyjnego oraz aktualne oprogramowanie antywirusowe.*
19. *Przed przystąpieniem do pracy, należy wydzielić odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, które wykorzystywane są do pracy.*
20. *Należy utworzyć osobny profil w systemie operacyjnym, zabezpieczony silnym hasłem dostępu. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.*
21. *Odchodząc od stanowiska pracy każdorazowo blokuje się urządzenie.*
22. *Należy podjąć szczególne środki, aby urządzenia z których korzysta się podczas pracy szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione – używamy szyfrowanych i zabezpieczonych hasłem urządzeń.*
23. *Do pracy zdalnej używa się przede wszystkim służbowych kont email. Jeśli podczas pracy przetwarza się dane osobowe i wymaga to użycia prywatnego konta email należy upewnić się że treść i załączniki są właściwie szyfrowane.*
24. *Należy unikać używania danych osobowych lub poufnych informacji w temacie wiadomości.*
25. *Przed wysłaniem maila należy upewnić się że wysyłany jest go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane szczególnych kategorii.*
26. *W przypadku wysyłania tej samej wiadomości do szerszej liczby adresatów przy ich wprowadzaniu należy korzystać z pola UDW.*
27. *Zabrania się otwierania wiadomości od nieznanych adresatów, a zwłaszcza nie otwierania załączników oraz uruchamiania linków w nich zawartych.*
28. *Zabrania się przesyłania mailem informacji zaszyfrowanej razem z hasłem - nawet w osobnej wiadomości. Hasło należy przekazać w innej formie.*

2) Po §10 dodaje się §11 o następującym brzmieniu:

„§11 1. Do zapoznania się i stosowania niniejszego dokumentu zobowiązani są wszyscy pracownicy zakładu."

3) Dodaje się załącznik nr 4,5,6 według numeracji jak w załączniku do niniejszego wydarzenia.

§ 2 1. Wykonanie Zarządzenia powierza się pracownikom Urzędu Miasta i Gminy w Ostrzeszowie.

2. Skuteczne powiadomienie o zapisach niniejszego Zarządzenia powierzam Sekretarzowi Miasta i Gminy Ostrzeszów

§ 3 Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Patryk Jędrowiak