ZARZĄDZENIE NR 60/23
BURMISTRZA BIERUTOWA

z dnia 20 czerwca 2023 r.

w sprawie zmiany zarządzenia w sprawie Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, oraz Wytycznych do analizy i szacowania ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Bierutowie

Na podstawie 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. Urz. EU L 119/1) – dalej: RODO, zarządzam co następuje:

§ 1. W załączniku Nr 2 pn.: „Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych" do Zarządzenia Nr 37/18 Burmistrza Bierutowa z dnia 22 maja 2018 r. w sprawie Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, oraz Wytycznych do analizy i szacowania ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Bierutowie, po Rozdziale 6 Zasady pracy na komputerze **dodaje się Rozdział 6a** w brzmieniu określonym w załączniku do niniejszego zarządzenia.

§ 2. Zobowiązuję kierowników referatów, upoważnionych pracowników przetwarzających dane osobowe, a także osoby zatrudnione na samodzielnych stanowiskach pracy w tut. Urzędzie, do sprawowania nadzoru nad ochroną przetwarzanych danych osobowych oraz do współpracy z Administratorem Danych Osobowych (dalej: Administratorem) w tym zakresie, Inspektorem Ochrony Danych Osobowych (dalej: IODO) oraz z Administratorem Systemu Informatycznego (dalej: ASI).

§ 3. Zobowiązuje się pracowników Urzędu Miejskiego w Bierutowie przetwarzających dane osobowe przy okazjonalnej pracy zdalnej, do przestrzegania przepisów o których mowa w § 1.

§ 4. Nadzór nad wykonaniem zarządzenia sprawuję osobiście.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Bierutowa

Piotr Sawicki

Załącznik do Zarządzenia Nr 60/23 z dnia 20 czerwca 2023 r.

Rozdział 6a Procedura ochrony danych osobowych w okazjonalnej pracy zdalnej.

1. Zasady bezpieczeństwa w miejscach świadczenia pracy zdalnej.

1. Pracując w miejscu pracy zdalnej, należy zapewnić, aby osoby nieuprawnione nie posiadały wglądu/dostępu do treści danych służbowych na nośnikach, komputerach, laptopach i w dokumentacji papierowej.
2. W miejscu wykonywania okazjonalnej pracy zdalnej należy zabezpieczać się przed dostępem osób nieupoważnionych.
3. Nie należy pozostawiać bez nadzoru dokumentów, nośników i sprzętu.

2. Warunki okazjonalnej pracy zdalnej.

1. Pracodawca zapewnia pracownikowi wsparcie w ustanowieniu bezpiecznego dostępu do infrastruktury IT organizacji poprzez np. użycie zdalnego pulpitu/VPN/innych aplikacji.
2. Do okazjonalnej pracy zdalnej, pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
3. Pracodawca zastrzega możliwość stosowania oprogramowania służącego do monitorowania wykonywania pracy przez pracownika.
4. Zgodnie z ustaleniami między pracodawcą a pracownikiem, pracodawca zapewnia pracownikowi służbowe urządzenia, jak komputer stacjonarny, laptop, smartfon, tablet, inne.
5. Urządzenia służbowe posiadają włączone automatyczne aktualizacje, zapory systemowe (firewall), program antywirusowy oraz tryb automatycznego blokowania urządzenia po dłuższym braku aktywności oraz blokadę portów USB.
6. Logowanie do systemu operacyjnego urządzeń wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika.
7. W sytuacji gdy urządzenia zawierają na nośnikach dane osobowe, powinny być przechowywane na zaszyfrowanym dysku/partycji.
8. W przypadku przesyłania plików zawierających dane osobowe lub dane operacyjne organizacji, należy korzystać z narzędzi/aplikacji zapewnionych przez pracodawcę lub za wyrażeniem zgody na użycie aplikacji zewnętrznych (np. serwer sieciowy, FTP, weTransfer, Google Drive, DropBoX, inne), zabezpieczonych co najmniej hasłem. Rekomendowane jest zastosowanie w tych przypadkach mechanizmu podwójnego uwierzytelnienia.
9. W aplikacjach użytych do pracy zdalnej w przeglądarce internetowej należy wyłączyć autouzupełnianie i zapamiętywanie hasła.
10. Pracownik w ramach uzgodnień z pracodawcą może być zobowiązany do wykonywania kopii bezpieczeństwa, którą powinien przechowywać na odrębnym nośniku danych, za którego zabezpieczenie odpowiada.
11. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy zgłaszać niezwłocznie informatykowi.

3. Zasady postępowania z dokumentami w formie papierowej.

1. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich zabrania do domu na czas wykonywania pracy zdalnej lub wykonania niezbędnych kopii.
2. Podczas przewożenia dokumentów do miejsca wykonywania okazjonalnej pracy zdalnej należy zachować szczególną ostrożność, aby nie doszło do ich zagubienia lub kradzieży. Trzeba zapewnić bezpieczne przewożenie dokumentacji papierowej np. w teczkach, aktówkach, plecakach.
3. Dokumentacja w miejscu wykonywania pracy zdalnej powinna być zabezpieczona przed dostępem nieupoważnionych osób tam przebywających, np. w szafie, biurku zamykanym na klucz.
4. **Zabrania się** poza miejscem wykonywania pracy zdalnej, pozostawiania dokumentów w miejscach dostępnych dla osób nieupoważnionych.
5. Po zakończeniu pracy dokumenty zawierającej dane osobowe jak i inne należy zwrócić do Urzędu do właściwych teczek, utworzonych zgodnie z obowiązującym JRWA.

4. Zasady korzystania z poczty elektronicznej.

1. Komunikacja powinna odbywać się za pomocą elektronicznej poczty służbowej.
2. Pliki zawierające dane osobowe przed wysłaniem ich do odbiorców, powinny być zabezpieczone hasłem, które należy przekazać odbiorcy telefonicznie, SMS lub inną drogą komunikacji.
3. W przypadku zabezpieczenia plików hasłem, należy stosować się do obowiązującej zasady silnych haseł, tj. hasło powinno składać się z minimum (np. 12) znaków: duże i małe litery i cyfry oraz znaki specjalne.
4. Przy wysyłaniu wiadomości należy upewnić się, że jest ona kierowana do odpowiedniego odbiorcy.
5. Nie należy otwierać załączników poczty pochodzącej z nieznanych, nietypowych źródeł lub podszywających się pod rzeczywistych nadawców.
6. Zakazane jest otwieranie hiper-linków, gdyż grozi to zainfekowaniem komputera.
7. Nie wolno wprowadzać loginów i haseł do formularzy zawartych w poczcie.
8. Należy zgłaszać informatykowi wszystkie przypadki podejrzanych e-maili, plików w e-mailach, prób wyłudzeń haseł dostępowych, kontaktów podejrzanych osób o próby uzyskania nieuprawnionego dostępu do danych.

9. W przypadku wysyłania informacji do odbiorców, z zastrzeżeniem ich poufności lub gdy ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy należy wpisać w ww. pole.

5. Obowiązek zachowania poufności i ochrony danych osobowych przez pracownika.

1. Pracownik wykonujący okazjonalną pracę zdalną jest zobowiązany do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Pracownik jest zobowiązany do zachowania w tajemnicy danych osobowych, do których ma dostęp.
3. Pracownik jest zobowiązany do niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań.
4. Pracownik jest zobowiązany do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
5. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.
6. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych. W przypadkach wątpliwych należy skontaktować się z bezpośrednim przełożonym lub Inspektorem Ochrony Danych.

6. Postępowanie w przypadku naruszenia ochrony danych osobowych.

1. Każdy pracownik zobowiązany jest do powiadomienia pracodawcy lub bezpośredniego przełożonego, informatyka lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia należą:
   a) zdarzenia losowe zewnętrzne (utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata/zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
   d) telefoniczne próby wyłudzenia danych osobowych,
   e) kradzież, zagubienie komputerów, dysków przenośnych, pendrive z danymi osobowymi,
   f) e-maile zachęcające do ujawnienia identyfikatora oraz hasła.
3. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji należy niezwłocznie zgłosić zdarzenie do pracodawcy, informatykowi oraz Inspektorowi Ochrony Danych.