ZARZĄDZENIE NR 120.9.2023
BURMISTRZA GMINY I MIASTA NOWE MIASTECZKO

z dnia 17 maja 2023 r.

w sprawie wprowadzenia Procedury ochrony danych osobowych w Urzędzie Miejskim w Nowym Miasteczku

Na podstawie art. 67^{26} §1 ustawy z dnia 26 czerwca 1974 r. - kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510 zpóźn. zm.) zarządzam, co następuje:

§ 1. Wprowadzam Procedurę ochrony danych osobowych, która ma zastosowanie do wykonywania pracy zdalnej wykonywanej okazjonalnie.

§ 2. Procedura stanowi załącznik do niniejszego zarządzenia.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Danuta Wojtasik

PROCEDURA OCHRONY DANYCH OSOBOWYCH

§ 1

1. Ilekroć w niniejszej Procedurze mowa jest o:
   a) Pracodawcy – oznacza to Urząd Miejski w Nowym Miasteczku.
   b) Pracowniku – oznacza to osobę, zatrudnioną na podstawie stosunku pracy u Pracodawcy;
2. Podczas wykonywania pracy zdalnej okazjonalnej Pracownika obowiązują zasady bezpieczeństwa i ochrony informacji oraz danych osobowych, określone w Polityce Bezpieczeństwa Informacji oraz Procedurze ochrony danych osobowych.
3. Przed rozpoczęciem wykonywania okazjonalnej pracy zdalnej Pracownik zobowiązany jest do zapoznania się z niniejszą Procedurą oraz złożenia oświadczenia o zobowiązaniu się do bezpiecznego przetwarzania danych osobowych oraz informacji, na dowód czego podpisuje oświadczenie o treści określonej w załączniku nr 1.
4. W zakresie, dotyczącym urządzeń, wykorzystywanych do okazjonalnej pracy zdalnej, ustanawia się następujące, minimalne wymagania w zakresie bezpieczeństwa urządzenia:
   a) zainstalowane zostało legalne i aktualne oprogramowanie;
   b) włączone zostały automatyczne aktualizacje systemowe;
   c) włączona została zapora systemowa;
   d) zainstalowano aktualny oraz legalny program antywirusowy;
   e) wprowadzono mechanizm logowania do systemu operacyjnego wymagający uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
   f) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
   g) zainstalowano program, umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
   h) ustawiono automatyczne blokowanie urządzenia po dłuższym braku aktywności lub wygaszacz ekranu;
   i) zaszyfrowano dysk wewnętrzny urządzenia;
   j) osoby trzecie, w tym domownicy Pracownika nie mają wglądu w pracę, wykonywaną z wykorzystaniem narzędzi i urządzeń, w szczególności poprzez właściwe ustawienie ekranu urządzenia przez Pracownika podczas jego wykorzystywania do okazjonalnej pracy zdalnej.
5. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do okazjonalnej pracy zdalnej zawierało inne zabezpieczenia, takie, jak:
   a) wyłączone porty pamięci zewnętrznych,
   b) ograniczone uprawnienia administracyjne użytkownika urządzenia;
   c) ustanowione połączenie VPN;
   d) wykorzystywanie oprogramowania służącego monitorowaniu wykonywania pracy przez Pracownika, które będzie wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.
6. Pracownik zobowiązany jest do posługiwania się przekazanymi przez Pracodawcę danymi dostępowymi (w tym loginami, hasłami) do systemów informatycznych i poczty elektronicznej i zapewnia ochronę tych danych, a także przetwarzanych w ramach takiego dostępu danych osobowych i informacji, w szczególności przed dostępem osób nieuprawnionych, ich zniszczeniem i utratą.

7. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać Administratorowi Systemów Informatycznych (informatykowi).
8. Naruszenia oraz incydenty bezpieczeństwa związane z nieprawidłowościami w zakresie przetwarzanych danych osobowych lub informacji służbowych Pracownik niezwłocznie zgłasza Administratorowi Danych (Pracodawcy) lub innym osobom odpowiedzialnym za ochronę danych osobowych i bezpieczeństwo informacji u Pracodawcy, w szczególności Administratorowi Systemów Informatycznych (informatykowi) lub Inspektorowi Ochrony Danych, w celu podjęcia działań wymaganych regulacjami wewnętrznymi oraz prawem.
9. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych przez Pracownika odbywa się w sposób, zapewniający poufność informacji przekazywanych w trakcie spotkania/rozmowy.
10. Jeżeli Pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik korzysta z tych urządzeń do połączeń z Internetem. Korzystanie z domowej sieci internetowej odbywa się za zgodą i wiedzą Pracodawcy.
11. W przypadku konieczności wykorzystywania przez Pracownika do wykonywania okazjonalnej pracy zdalnej domowej sieci internetowej (WiFi), należy upewnić się, że została ona skonfigurowana przed przystąpieniem Pracownika do pracy zdalnej w sposób, minimalizujący ryzyko włamania, w szczególności:
    a) korzystanie z Internetu wymaga uwierzytelnienia, np. poprzez hasło,
    b) hasło dostępu do sieci internetowej składa się z co najmniej ośmiu znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
    c) zmieniono login do panelu administracyjnego routera (jeśli to możliwe),
    d) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń, znajdujących się w sieci domowej,
    e) zmieniono domyślny adres routera na inny.
12. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby okazjonalnej pracy zdalnej udziela Administrator Systemów Informatycznych (informatyk).
13. Jeżeli w związku z wykonywaniem przez Pracownika okazjonalnej pracy zdalnej niezbędne jest przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, ustanawia się następujące, minimalne wymagania w zakresie bezpieczeństwa:
    a) dane należy zabezpieczyć hasłem;
    b) jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, należy przesyłać je w załączniku, zabezpieczonym hasłem;
    c) hasło do załącznika:
        - powinno zostać przekazane odbiorcy inną drogą komunikacji, aniżeli poczta e-mail;
        - powinno być odpowiednio skomplikowane;
    d) każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
14. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.
15. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy:
    a) skorzystać z opcji „Ukrytej kopii",
    b) zastosować specjalne oprogramowanie, udostępnione w tym celu przez Pracodawcę.

16. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
17. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.
18. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet, jeżeli są to jedynie imiona, nazwiska czy adresy e-mail.
19. Jeżeli w związku z wykonywaniem przez Pracownika okazjonalnej pracy zdalnej niezbędne jest wykorzystywanie przez Pracownika dokumentów (oryginałów/kopii/odpisów) w formie papierowej, ustanawia się następujące, minimalne wymagania w zakresie bezpieczeństwa:
    a) zabrania się zabierania oryginałów dokumentów poza siedzibę Pracodawcy;
    b) podczas przewożenia dokumentów do miejsca realizowania okazjonalnej pracy zdalnej, należy zachować szczególną ostrożność;
    c) praca z dokumentami nie może być wykonywana w miejscu publicznym;
    d) Pracownik zapewnia zabezpieczenie dokumentów w miejscu wykonywania okazjonalnej pracy zdalnej, poprzez przechowywanie w szafie zamykanej na klucz, do której tylko on ma dostęp.
20. W zakresie, dotyczącym ochrony danych osobowych, wykorzystywanych przez Pracownika do okazjonalnej pracy zdalnej Pracodawca przeprowadza niezbędne szkolenie Pracownika w zakresie ochrony danych osobowych w związku z wykonywaniem okazjonalnej pracy zdalnej przed przystąpieniem przez Pracownika do wykonywania tej pracy.
21. W zakresie zapewnienia bezpieczeństwa danych osobowych podczas okazjonalnej pracy zdalnej zastosowanie mają przepisy Rozporządzenia PEiR (UE) nr 2016/679 z 27.04.2016 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. UE z 2016 r. 119, s. 1 ze zm.) („RODO").
22. Podczas wykonywania okazjonalnej pracy zdalnej przez Pracownika niedozwolone jest:
    - udostępnianie innym osobom danych, służących do uwierzytelnienia do systemów i/lub usług;
    - przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
    - przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
    - korzystanie z urządzeń, które nie zostały zatwierdzone przez Pracodawcę;
    - odmowa dokonania przeglądu urządzeń przez Pracodawcę;
    - niszczenie dokumentów w domu;
    - udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
    - dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
    - logowanie się na konto innego użytkownika;
    - zabranie dokumentów z zakładu pracy bez uprzedniego poinformowania Pracodawcy na piśmie lub w formie mailowej;
    - zabranie z zakładu pracy oryginałów dokumentów;

- niezwrócenie dokumentów;
- niepotwierdzenie zakresu zwróconych danych,
- podejmowanie okazjonalnej pracy zdalnej w miejscach publicznych (m.in. kawiarnie, restauracje, galerie handlowe), w których osoby postronne mogłyby uzyskać jakiekolwiek informacje dot. wykonywanej pracy,
- wykorzystywanie danych osobowych, przetwarzanych przez Pracownika w ramach okazjonalnej pracy zdalnej w innym celu, niż wykonywanie obowiązków służbowych.

§ 2

1. Pracownik oświadcza, że zapoznał się z zasadami poufności i ochrony danych w warunkach okazjonalnej pracy zdalnej, obowiązującymi u Pracodawcy, jak również zasadami bezpiecznego i higienicznego wykonywania pracy zdalnej i zobowiązuje się do ich przestrzegania.
2. Złamanie zasad wykonywania okazjonalnej pracy zdalnej, określonych w niniejszej Procedurze lub rażące niestosowanie się do postanowień Procedury może stanowić naruszenie obowiązków pracowniczych.
3. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do Pracodawcy/Inspektora ochrony danych.
4. Obowiązek stosowania się do zapisów niniejszej Procedury dotyczy każdego Pracownika wykonującego okazjonalną pracę zdalną.
5. Niniejsza Procedura wchodzi w życie z dniem ogłoszenia.

Załącznik nr 1

....., dnia ..... r.

.....
(imię i nazwisko pracownika)

.....
(stanowisko, komórka organizacyjna)

OŚWIADCZENIE PRACOWNIKA

Ja, niżej podpisany/-a ..... niniejszym oświadczam, że zapoznałem/-łam się z Procedurą ochrony danych osobowych oraz zobowiązuję się do jej przestrzegania podczas wykonywania okazjonalnej pracy zdalnej.
Oświadczam, iż zobowiązuję do przestrzegania przepisów w zakresie ochrony danych osobowych, wynikających z 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), ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku oraz Polityki Bezpieczeństwa Informacji u Pracodawcy, która określa zasady związane z bezpiecznym przetwarzaniem informacji służbowych oraz danych osobowych, a także zobowiązuję się do zachowania w tajemnicy danych osobowych oraz informacji pozyskanych w trakcie wykonywania pracy .

Realizując zadania w ramach okazjonalnej pracy zdalnej, z wykorzystaniem urządzeń na których przetwarzane są informacje służbowe lub dane osobowe, zobowiązuję się do przestrzegania obowiązków w zakresie bezpieczeństwa i ochrony informacji oraz danych osobowych w pracy zdalnej, które zostały określone w Procedurze ochrony danych osobowych.

Równocześnie potwierdzam, iż w przypadku naruszenia bezpieczeństwa przetwarzanych danych osobowych lub informacji służbowych, niezwłocznie poinformuję Administratora Danych, Administratora Systemów Informatycznych lub Inspektora Ochrony Danych, w celu podjęcia działań wymaganych prawem.

.....