ZARZĄDZENIE NR ..4..../2023

Kierownika Zarządu Dróg Powiatowych w Turku

z dnia 10.08.2023 roku

w sprawie procedury ochrony danych osobowych podczas pracy zdalnej w Zarządzie Dróg Powiatowych w Turku

Na podstawie art. 3^1 i art. 67^{26} § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2023 r. poz. 1465) oraz art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (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 L z 2016 r. 119 ze zm.)

§ 1

Wprowadza się procedurę ochrony danych osobowych podczas wykonywania pracy zdalnej w Zarządzie Dróg Powiatowych w Turku w brzmieniu określonym załącznikiem do niniejszego zarządzenia.

§ 2

Zobowiązuję Panią Magdalenę Ignatowicz-Kowalską do podania zarządzenia do wiadomości pracowników poprzez wywieszenie jego treści na tablicy ogłoszeń w siedzibie Zarządu Dróg Powiatowych w Turku.

§ 3

Zarządzenie wchodzi w życie z chwilą podpisania.

Roman Kacprzak
Kierownik
Zarządu Dróg Powiatowych w Turku

RADCA PRAWNY
Mateusz Jastrzębski
KN-2839

ZARZĄD DRÓG POWIATOWYCH
w Turku
ul. Kolska Szosa 64, 62-700 Turek
tel. (0-63) 222 31 10, fax (0-63) 222 31 18
REGON 311080366 NIP 668-17-19-792

Załącznik

do zarządzenia nr 4/2023

Kierownika Zarządu Dróg Powiatowych w Turku

z dnia 10.08.2023r.

PROCEDURA OCHRONY DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ W ZARZĄDZIE DRÓG POWIATOWYCH W TURKU

§ 1. Postanowienia wstępne.

1. Niniejsza procedura określa zasady ochrony danych osobowych podczas pracy zdalnej i jest wprowadzana w związku z przepisami rozporządzenia Parlamentu Europejskiego i Rady (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 L z 2016 r. 119, s. 1 ze zm.) – dalej RODO oraz ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510 z późn. zm.).
2. Ilekroć w procedurze mowa o:
   1) pracy zdalnej – należy przez to rozumieć pracę zdalną w rozumieniu art. 67^{18} ustawy Kodeks pracy,
   2) pracowniku – należy przez to rozumieć osobę zatrudnioną w Zarządzie Dróg Powiatowych w Turku na podstawie umowy o pracę albo świadczącą na rzecz Zarządu Dróg Powiatowych w Turku prace na podstawie innego stosunku prawnego, w szczególności umowy cywilnoprawnej,
   3) danych osobowych – należy przez to rozumieć dane osobowe w rozumieniu RODO.
3. Pracownik zobowiązany jest przetwarzać dane osobowe w ramach pracy zdalnej wyłącznie przy zachowaniu wymogów określonych niniejszą procedurą.
4. Jeżeli pracownik nie ma możliwości zachowania wymogów określonych niniejszą procedurą, w szczególności ze względu na siłę wyższą (w tym brak prądu lub dostępu do sieci Internet), zobowiązany jest do zaprzestania przetwarzania danych osobowych oraz do poinformowania o tym pracodawcy.

§ 2. Miejsce świadczenia pracy zdalnej.

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Pracownik wykonuje pracę zdalną wyłącznie pod adresem, który wskazał pracodawcy. Niedozwolone jest wykonywanie pracy zdalnej w miejscach publicznych, takich jak kawiarnie, restauracje, galerie handlowe.

3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane.
6. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający ochronę danych osobowych, przekazywanych w trakcie spotkania lub rozmowy.

§ 3. Urządzenia służące do pracy zdalnej.

1. Pracownik wykonuje pracę zdalną wyłącznie z wykorzystaniem urządzeń i oprogramowania udostępnionych przez pracodawcę.
2. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, w tym domownikom.
3. Pracodawca udostępnia urządzenia spełniające następujące wymagania:
   1) oprogramowanie, w tym system operacyjny zainstalowane na urządzeniu, pochodzą z legalnego źródła,
   2) zostały włączone automatyczne aktualizacje,
   3) została włączona zapora systemowa,
   4) został zainstalowany i działa w tle program antywirusowy,
   5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika spełniające wymagania co do złożoności min. 12 znaków, małe i duże litery, znaki specjalne,
   6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
   7) został zainstalowany program umożliwiający tworzenie plików zabezpieczonych hasłem,
   8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności
   9) zainstalowane zostało oraz działa oprogramowanie szyfrujące dyski, partycje, kontenery.
4. Pracownik w miarę możliwości powinien wykonywać pracę zdalną na koncie z ograniczonymi uprawnieniami.
5. Pracownikowi nie wolno samodzielnie zmieniać ustawień urządzenia, w szczególności mających wpływ na spełnienie wymienionych w ust. 3.
6. Jeżeli pracownik stwierdzi, że udostępnione przez pracodawcę nie spełnia wymagań określonych w ust. 3, zobowiązany jest niezwłocznie zawiadomić o tym pracodawcę.

§ 4. Internet i sieć lokalna.

1. Niedozwolone jest wykonywanie pracy zdalnej z nieznanych, obcych lub otwartych sieciach.
2. Jeżeli pracodawca udostępnia pracownikowi modem Internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik powinien korzystać w pierwszej kolejności z tych urządzeń po uzgodnieniu z Pracodawcą limitu danych komórkowych do wykorzystania.

3. W przypadku korzystania z domowej sieci WiFi, sieć ta winna być skonfigurowana w sposób minimalizujący ryzyko nieautoryzowanego dostępu do urządzenia, a w szczególności:
   1) korzystanie z Internetu powinno wymagać uwierzytelnienia, w szczególności poprzez hasło składające się z co najmniej 12 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
   2) jeśli to możliwe, należy zmienić login i hasło do panelu administracyjnego routera na własne,
   3) dostęp do panelu administracyjnego routera powinien być możliwy wyłącznie z urządzeń znajdujących się w sieci lokalnej (domowej).

§ 5. Zabezpieczanie informacji zawierających dane osobowe.

1. Jeżeli niezbędne jest udostępnienie informacji zawierających dane osobowe podmiotom uprawnionym do ich pozyskania, dostęp do tych danych powinien zostać zabezpieczony hasłem. W przypadku udostępniania informacji pocztą elektroniczną, dane te powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
2. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
3. Hasło powinno zawierać 12 znaków, małe i duże litery, znaki specjalne,
4. Dozwolone jest ustalenie stałego hasła do celów komunikacji z jednym odbiorcą.
5. Zabezpieczania hasłem może polegać w szczególności na nadaniu hasła do pliku, w którym znajdują się dane osobowe oraz zabezpieczenie pliku poprzez kompresję z zaszyfrowaniem archiwum wynikowego hasłem.
6. Każda wiadomość zawierająca dane osobowe powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
7. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji ukrytej kopii (UDW/BCC).
8. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych, o ile zapewniają one szyfrowaną komunikację.

§ 6. Zasady korzystania z materiałów w postaci nieelektronicznej.

1. Wszelkie materiały zawierające dane osobowe powinny być przechowywane w szafach, szufladach na klucz, chronionych zamkami patentowymi w siedzibie pracodawcy.
2. Pracownikowi nie wolno wynosić materiałów lub ich kopii poza siedzibę pracodawcy.

§ 7. Szczególne sytuacje.

1. Pracownik jest zobowiązany niezwłocznie zgłaszać pracodawcy problemy z działaniem udostępnionych urządzeń lub oprogramowania.

2. W przypadku zgubienia lub kradzieży urządzeń lub nośników informacji zawierających dane osobowe lub stwierdzenia, że dostęp do danych osobowych uzyskały osoby nieuprawnione, pracownik jest zobowiązany niezwłocznie zawiadomić o tym pracodawcę oraz inspektora danych osobowych.

§ 8. Zakazy.

Pracownikowi nie wolno:

1) udostępniać innym osobom danych umożliwiających dostęp do danych osobowych, w szczególności loginów oraz haseł służących do uwierzytelnienia w systemach lub usługach,
2) przekazywać informacji zawierających dane osobowe bez zabezpieczenia hasłem i szyfrowania, w szczególności w treści wiadomości e-mail;
3) przekazywać hasła do zabezpieczonych informacji zawierających dane osobowe tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
4) korzystać przy wykonywaniu pracy zdalnej z urządzeń i oprogramowania innych, niż udostępnione przez pracodawcę;
5) uniemożliwiać pracodawcy lub osobie przez niego wyznaczonej przeprowadzenia kontroli urządzenia udostępnionego pracownikowi w celu wykonywania pracy zdalnej;
6) udostępniać innym osobom urządzeń i oprogramowania udostępnionych przez pracodawcę w celu wykonywania pracy zdalnej;
7) udostępniać innym osobom danych osobowych, do których pracownik ma dostęp w związku z wykonywaniem pracy zdalnej,
8) uzyskiwać dostępu do urządzeń, systemów i usług przy pomocy danych autoryzacyjnych (login, hasło) przypisanych innym użytkownikom.

Roman Kasprzak
Kierownik
Zarządu Dróg Powiatowych w Turku

ZARZĄD DRÓG POWIATOWYCH
w Turku
ul. Kolska Szosa 64, 62-700 Turek
tel. (0-63) 222 31 10, fax (0-63) 222 31 18
REGON 311080366 NIP 668-17-19-792