ZARZĄDZANIE NR 14/2023
STAROSTY POWIATU SZTUMSKIEGO
z dnia 17 kwietnia 2023 roku

w sprawie: wprowadzenia Regulaminu ochrony danych osobowych podczas wykonywania pracy zdalnej w Starostwie Powiatowym w Sztumie.

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. 2022 r., poz. 1526 ze zm.) oraz art. 67^{26} ust. 1ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j. Dz. U. z 2022 r., poz. 1510 ze zm.) w związku z rozporządzeniem 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 L z 2016 r. 119, s. 1 ze zm.) zarządzam, co następuje:

§ 1

Wprowadza się do stosowania w Starostwie Powiatowym w Sztumie Regulaminu ochrony danych osobowych podczas wykonywania pracy zdalnej w Starostwie Powiatowym w Sztumie, stanowiący Załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się Naczelników Wydziałów oraz Samodzielne stanowiska do zapoznania podległych pracowników z Regulaminem ochrony danych osobowych podczas wykonywania pracy zdalnej w Starostwie Powiatowym w Sztumie wymienionym w § 1 niniejszego Zarządzenia.

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Powiatu Sztumskiego.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

Leszek Jan Sarnowski
Elektronicznie podpisany przez Leszek Jan Sarnowski
Data: 2023.06.30 11:16:37 +02'00'

Załącznik
do Zarządzenia Nr 14/2023
Starosty Powiatu Sztumskiego
z dnia 17 kwietnia 2023 r.

Regulamin ochrony danych osobowych podczas wykonywania pracy zdalnej

I. Wprowadzenie

1. Niniejszy regulamin określa zasady ochrony danych osobowych podczas pracy zdalnej i jest wprowadzany w związku z przepisami 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 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. W Regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

II. Warunki podjęcia pracy zdalnej

1. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady ochrony danych osobowych podczas pracy zdalnej określone w niniejszym Regulaminie.
2. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki techniczne oraz lokalowe, ochrony danych osobowych w miejscu wykonywania pracy zdalnej.
3. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
4. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

III. 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 pod adresem, który wskazał pracodawcy. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona.
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 lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

6. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania / rozmowy.

IV. Bezpieczeństwo pracy zdalnej

Internet

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
2. 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.
3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
   - Korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
   - Hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych.
   - Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny.
   - Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela Starszy informatyk.

Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna jest realizowana z wykorzystaniem służbowego sprzętu, jak komputera stacjonarny, laptop, smartfon, tablet, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
5. Urządzenie służbowe jest wydawane pracownikowi za potwierdzeniem.
6. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do Wydziału Organizacji, Promocji, Nadzoru i Kadr.
7. Wydziału Organizacji, Promocji, Nadzoru i Kadr odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
8. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie Starszego informatyka udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez Starszego informatyka narzędzia), w celu dokonania jego zdalnego przeglądu.
9. Minimalne wymagania w zakresie bezpieczeństwa:
   - Na urządzeniu jest legalne i aktualne oprogramowanie;
   - Zostały włączone automatyczne aktualizacje;
   - Została włączona zapora systemowa;
   - Został zainstalowany i działa w tle program antywirusowy;
   - Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN lub token;
   - Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;

- Został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
- Zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
- Jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami;

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik wykorzystuje tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, uprzednio należy je zabezpieczyć hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, należy przesyłać je w załączniku zabezpieczonym hasłem.
4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska czy adresy e-mail.
5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.
8. Rekomendowane metody zabezpieczania hasłem:
   1. Nadanie hasła do pliku, w którym są dane osobowe
   2. Zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
10. 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), tzn. adresy wpisać w to pole.
12. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.
13. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
14. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana pracodawcy.

8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.)
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.
11. Pracownik zapewnia zabezpieczenie dokumentów w miejscu wykonywania pracy zdalnej, poprzez przechowywanie w szafie zamykanej na klucz, do której tylko on ma dostęp.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Starszego informatyka.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, Wydziału Organizacji, Promocji, Nadzoru i Kadr, a także inspektora ochrony danych.

VI. Działania niedozwolone

1. 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;
   - Odmówienie Starszemu informatykowi przeglądu urządzenia;
   - 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;
   - Samodzielne zniszczenie dokumentów w domu;
   - Logowanie się na konto innego użytkownika;
   - Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
   - Zabranie oryginałów dokumentów;
   - Niezwrócenie dokumentów;
   - Niepotwierdzenie z pracodawcą zakresu zwróconych danych.