PROCEDURA OCHRONY DANYCH OSOBOWYCH W PRACY ZDALNEJ

SPIS TREŚCI

1. CEL PROCEDURY

Niniejsza procedura została opracowana z związku z wejściem w życie w dniu 07 kwietnia 2023 r. przepisów rozdziału II c - Praca zdalna w ustawie z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2022 r. poz. 1510, 1700 i 2140).

Celem wprowadzenia niniejszej procedury jest zapewnienie bezpiecznego procesu przetwarzania danych osobowych w trakcie pracy zdalnej, zgodnie z rozporządzeniem 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) – dalej „RODO" oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

Niniejsze zasady bezpiecznego przetwarzania danych osobowych mają zastosowanie zarówno do wykonywania pracy zdalnej w formie stałej jak i okazjonalnej.

2. POSTANOWIENIA OGÓLNE

1. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
2. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.
3. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
4. Pracownik, w ramach pracy zdalnej zobowiązany jest do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulującymi pracę w zakładzie pracy zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych.

3. BEZPIECZEŃSTWO OBSZARU PRZETWARZANIA

1. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
2. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie nakładki na ekran tzw. filtru /folii prywatyzującej.
3. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
4. Pracownik zobowiązany jest po zakończeniu pracy na sprzęcie elektronicznym każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.

4. Bezpieczeństwo pracy z dokumentacją papierową

1. Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum. Pracodawca zezwala pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą zakładu pracy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Zabrania się drukowania dokumentów służbowych w zewnętrznych/publicznych punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
4. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w teczce wykonanej z nieprzezroczystego materiału.
5. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w formie papierowej w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.
6. W przypadku korzystania przez pracownika z oryginałów dokumentów (lub kopii dokumentów, przechowywanych w siedzibie pracodawcy), po zakończeniu pracy powinny zostać niezwłocznie zwrócone do siedziby pracodawcy.
7. W przypadku korzystania przez pracownika z oryginałów dokumentów, pracownik przed wydaniem dokumentów podpisuje oświadczenie, na podstawie którego przyjmuje na siebie odpowiedzialność za powierzone dokumenty, które stanowi załącznik nr 1.
8. W przypadku korzystania z kopii dokumentacji (utworzonej na potrzeby pracy zdalnej) powinny one zostać w całości zniszczone przez Pracownika. W przypadku nieposiadania niszczarki w miejscu pracy Pracownika powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
9. Po zakończeniu pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

5. Bezpieczeństwo nośników danych

1. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.
2. Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej musi być wspierany przez producenta i regularnie aktualizowany.
3. Sprzęt komputerowy i inne urządzenia mobilne wykorzystywane w celach służbowych, w tym laptop, telefon lub tablet powinny być zabezpieczone przed dostępem osób trzecich, na przykład za pomocą hasła i/lub dwustopniowego uwierzytelnienia.
4. Sprzęt komputerowy wykorzystywany w celach służbowych powinien dodatkowo posiadać szyfrowane dyski np. za pomocą BitLocker.

5. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być zabezpieczone przed dostępem osób trzecich, na przykład za pomocą hasła.
6. W przypadku braku konieczności stosowania zewnętrznych kart pamięci i innych nośników zewnętrznych, sprzęt komputerowy wykorzystywany w celach służbowych powinien mieć zablokowane fizyczne porty USB.

6. BEZPIECZEŃSTWO DOMOWEJ SIECI

1. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, prywatnej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w miejscu publicznym.
2. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.

7. PROCEDURA BEZPIECZNEGO LOGOWANIA

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła, na przykład poprzez ustawianie PIN-u lub innej formy uwierzytelnienia.
2. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.
3. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być zmieniane w cyklach co najmniej 6 miesięcznych. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach niegwarantujących ich poufności.
4. Zabronione jest domyślne zapamiętywanie hasła dostępu do programów, aplikacji wykorzystywanych w pracy zdalnej.
5. Zalecanym sposobem zabezpieczania danych logowania jest stosowanie klucza zabezpieczającego U2F (U2F security key).

8. PRACA Z DANYMI W OBIEGU ELEKTRONICZNYM

1. Instalowanie jakiegokolwiek oprogramowania na sprzęcie służbowym jest możliwe tylko przez pracowników działu informatycznego lub za ich zgodą i zgodnie z ich wytycznymi.
2. Na sprzęcie komputerowym nie może być instalowane żadne nielegalne lub darmowe oprogramowanie.
3. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu służbowego sprzętu.

4. Pracownik nie może przechowywać na laptopie ani telefonie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
5. Pracownik nie może łączyć się z firmowymi systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy.

9. KORZYSTNIE Z MAILA

1. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
2. Zalecanym sposobem zabezpieczania danych logowania jest stosowanie klucza zabezpieczającego U2F (U2F security key).
3. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
4. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
5. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników do wiadomości e-mail oraz hiperłączy znajdujących się w tekście.
6. Podczas wysyłania korespondencji zbiorczej pracownik zobowiązany jest do korzystania z opcji „kopia ukryta” (pole UDW – Ukryci Do Wiadomości lub pole BCC – Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.
7. Pracownik zobowiązany jest do szyfrowania wiadomości e-mailowych zawierających dane osobowe i przekazywania hasła zawsze inną formą, na przykład telefonicznie.
8. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mail.

W przypadku identyfikacji wirusa, nieaktualności oprogramowania antywirusowego lub jakichkolwiek podejrzanych aktywności na sprzęcie lub przetwarzanej dokumentacji (znikające pliki, załącznik, zmiany w treści, nieautoryzowana zmiana dokumentu), konieczne jest natychmiastowe skontaktowanie się z inspektorem Jerzym Wawerkiem (kock_info@kock.pl, tel. 81)8591004 wew. 38)

10. ZASADY BEZPIECZNEGO PROWADZENIA WIDEOKONFERENCJI

Etapy wideokonferencji	Wytyczne
Przed rozpoczęciem wideokonferencji	▪ Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.

	▪ Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store. ▪ Przed uruchomieniem spotkania upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu oraz nie będą słyszały prowadzonych rozmów (użyj słuchawek z mikrofonem). ▪ Logując się do aplikacji, korzystaj wyłącznie z zalecanych przez pracodawcę dostępów, loginów itp. ▪ Korzystaj z aplikacji webowych, nie desktopowych. ▪ Zabezpiecz sieć Wi-Fi silnym hasłem. ▪ Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli. ▪ Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów. ▪ Przeskanuj program do telekonferencji systemem antywirusowym.
W trakcie korzystania z wideokonferencji	▪ Ogranicz ilość podawania danych osobowych do niezbędnego minimum. ▪ Użyj innego hasła, niż używane przez Ciebie w innych usługach. ▪ Nie udostępniaj linków do konferencji poza zamknięte grupy upoważnionych użytkowników. ▪ Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line. ▪ Nie udostępniaj niezabezpieczonych plików. ▪ Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia). ▪ Korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji. ▪ Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne).
Po skorzystaniu z wideokonferencji	▪ Wyłącz mikrofon i kamerę. ▪ Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację. ▪ Sprawdź, czy program do telekonferencji nie działa w tle.

Załącznik nr 1 – zobowiązanie pracownika w związku z wydaniem dokumentacji papierowej

W związku z koniecznością korzystania z dokumentów w formie papierowej w trakcie wykonywania pracy zdalnej, ja niżej podpisany/a jako pracownik/~~współpracownik~~ Urzędu Miejskiego w Kocku przyjmuję na siebie odpowieialność za powierzoną mi dokumentację Pracodawcy, oraz zobowiązuje się do jej zwrotu, w zabezpieczony sposób zgodnie z Procedurą Ochrony Danych Osobowych w Pracy Zdalnej, bezzwłocznie po zakończeniu wykonywania pracy na dokumentach lub z chwilą zakończenia wykonywania pracy w sposób zdalny, w zależności które z nich nastąpi jako pierwsze.

W związku z udostępnioną mi dokumentacją Pracodawcy zobowiązuję się również do zachowania w poufności jej treści, nieudostępniania osobom postronnym oraz zabezpieczenia przed nieuprawnionym zapoznaniem się z jej treścią lub zgubieniem/kradzieżą.

……..……

(data oraz imię i nazwisko)

Załącznik nr 2 – oświadczenie o zapoznaniu się z procedurą i odbyciu szkolenia z procedury

Ja niżej podpisany/a pracownik/~~współpracownik~~ Urzędu Miejskiego w Kocku oświadczam, że zapoznałem/am się z Procedurą Ochrony Danych Osobowych w Pracy Zdalnej oraz, że w pełni rozumiem i akceptuję jej treść. Ponadto oświadczam, że odbyłem szkolenie z zasad przetwarzania danych osobowych w trakcie wykonywania pracy zdalnej i tym samym zobowiązuję się do ich przestrzegania.

……..……

(data oraz imię i nazwisko)