ZARZĄDZENIE NR V/42/23
BURMISTRZA SOLCA KUJAWSKIEGO
Z DNIA 17 KWIETNIA 2023 ROKU

w sprawie wprowadzenia Procedury ochrony danych osobowych dotyczącej wykonywania pracy zdalnej w Urzędzie Miejskim w Solcu Kujawskim

Na podstawie art. 33 ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40)[1] oraz art. 67^{26} ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2022 r. poz. 1510)[2]

ZARZĄDZAM, CO NASTĘPUJE:

§ 1

Wprowadzam Procedurę ochrony danych osobowych dotyczącą wykonywania pracy zdalnej w Urzędzie Miejskim w Solcu Kujawskim, zwaną dalej Procedurą, w brzmieniu określonym w załączniku do zarządzenia.

§ 2

Zobowiązuję pracowników Urzędu Miejskiego w Solcu Kujawskim do stosowania postanowień Procedury.

§ 3

Wykonanie zarządzenia powierzam Sekretarzowi Gminy Solec Kujawski.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Teresa Substyk
Burmistrz Solca Kujawskiego

[1] Zmiany: Dz.U.2023.572
[2] Zmiany: Dz.U.2022.1700, Dz.U.2022.2140, Dz.U.2023.240
Zatwierdziła: Magdalena Rudna-Plewa, Sekretarz Gminy
Sporządziły: Genowefa Nasierowska, Zastępca Inspektora Ochrony Danych Osobowych
Katarzyna Paliwoda-Kozak, inspektor ds. kadr,

Załącznik do zarządzenia Nr V/42/2023
Burmistrza Solca Kujawskiego
z 17 kwietnia 2023 r.

Procedura ochrony danych osobowych dotycząca wykonywania pracy zdalnej w Urzędzie Miejskim w Solcu Kujawskim

1. Wstęp

Procedura ochrony danych osobowych dotycząca wykonywania pracy zdalnej w Urzędzie Miejskim w Solcu Kujawskim, zwana dalej Procedurą, określa zasady ochrony danych osobowych oraz związane z tym prawa i obowiązki Urzędu Miejskiego w Solcu Kujawskim (dalej jako Pracodawca) i pracowników w związku z wykonywaniem pracy zdalnej.
Procedura jest aktem wewnętrznego stosowania i stanowi element Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miejskim w Solcu Kujawskim.
Celem niniejszej Procedury jest zapewnienie bezpiecznego procesu przetwarzania informacji, w tym danych osobowych podczas wykonywania pracy zdalnej, w tym pracy zdalnej okazjonalnej.

2. Podstawy prawne

Niniejsza Procedura opracowana została na podstawie:
1) 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) – dalej „RODO”;
2) ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy;
3) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
4) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

3. Definicje i skróty

Ilekroć w niniejszej Procedurze jest mowa o:
1) **Pracodawcy** lub **Urzędzie** – oznacza to Urząd Miejski w Solcu Kujawskim w rozumieniu przepisów Kodeksu pracy;
2) **Administratorze** - oznacza to Burmistrza Solca Kujawskiego;
3) **BIiRSI** – oznacza to Biuro Informatyzacji i Rozwoju Systemów Informatycznych w Urzędzie Miejskim w Solcu Kujawskim;

4) **Inspektorze Ochrony Danych (IOD) -** oznacza to osobę wyznaczoną przez Administratora, nadzorującą przestrzeganie zasad ochrony danych osobowych w Urzędzie Miejskim w Solcu Kujawskim;
5) **pracowniku** – oznacza to osobę zatrudnioną w Urzędzie Miejskim w Solcu Kujawskim na podstawie o umowę o pracę;
6) **pracy zdalnej** – oznacza to wykonywanie pracy całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość, jeżeli wykonywanie pracy poza miejscem jej stałego wykonywania jest możliwe ze względu na organizację pracy lub rodzaj wykonywanej pracy przez pracownika;
7) **pracy zdalnej okazjonalnej –** oznacza to pracę w rozumieniu art. 67^{33} ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy, zgodnie z którym pracownik może świadczyć pracę zdalną okazjonalnie w wymiarze nieprzekraczającym 24 dni w roku kalendarzowym;
8) **danych osobowych** – oznacza to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
9) **przetwarzaniu** - oznacza to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; w szczególności, w odniesieniu do niniejszego regulaminu: rejestrowanie, przechowywanie, udostępnianie;
10) **nośnikach danych osobowych** – oznacza to zewnętrzny nośnik danych osobowych to mobilny przedmiot fizyczny, na którym możliwe jest zapisanie informacji zawierającej dane osobowe i z którego możliwe jest późniejsze odtworzenie tej informacji; w praktyce najpopularniejszymi nośnikami danych osobowych są: papier, dyski twarde, karty pamięci, pamięć USB, laptop, płyty CD/DVD, telefony komórkowe, karty magnetyczne i chipowe;
11) **sprzęcie służbowym –** oznacza to wszelkie urządzenia otrzymane przez pracownika od Pracodawcy do celów służbowych (np.: laptop, telefon, pendrive) wraz z całą infrastrukturą telekomunikacyjną i oprogramowaniem.

4. Zakres stosowania

Zasady określone w Procedurze mają zastosowanie do:
1) wszystkich rodzajów nośników danych osobowych, w tym papierowych, które zawierają lub mogą zawierać dane osobowe;
2) wskazanego przez pracownika miejsca zamieszkania lub innych miejsc uzgodnionych z Pracodawcą, w których są lub mogą być przetwarzane dane osobowe.

Wykonywanie pracy zdalnej nie zwalnia pracownika z obowiązku przestrzegania innych regulacji wewnętrznych obowiązującymi w Urzędzie, zwłaszcza Polityki Bezpieczeństwa Informacji oraz Polityki Ochrony Danych Osobowych wraz z dokumentami powiązanymi.

Do zapoznania się z treścią Procedury i stosowania jej zapisów zobowiązani są wszyscy pracownicy wykonujący pracę zdalną w Urzędzie (bez względu na tryb nawiązania stosunku pracy, zajmowanego stanowiska, wymiaru czasu pracy). Złamanie zasad określonych w Procedurze lub niedostosowanie się do jej postanowień stanowi naruszenie obowiązków pracowniczych.

5. Rozpoczęcie pracy zdalnej

Przed przystąpieniem do wykonywania pracy zdalnej:
1) Stanowisko ds. kadr:
   a) przekazują Inspektorowi Ochrony Danych informację o potrzebie przeprowadzenia szkolenia wobec pracownika mającego świadczyć pracę zdalną;
   b) przechowują w aktach osobowych oświadczenie, o którym mowa w pkt 2 lit. a przez okres niezbędny do prowadzenia akt dla danego pracownika, przewidziany przepisami prawa,
   c) prowadzą listę pracowników wykonujących pracę zdalną;
2) pracownik:
   a) zapoznaje się z treścią Procedury, co potwierdza pisemnym lub w elektronicznej postaci oświadczeniem i zobowiązaniem do przestrzegania postanowień w niej zawartych;
   b) odbywa szkolenie, zgodnie z rozdziałem 6 Procedury.

6. Szkolenie

1. Na potrzeby wykonywania pracy zdalnej Pracodawca przeprowadza, w miarę potrzeby instruktaż i szkolenie w tym zakresie.
2. Szkolenie może zostać przeprowadzone w formie e-learningu, szkolenia stacjonarnego, szkolenia zdalnego lub zapoznania z przygotowaną lub udostępnioną dokumentacją obejmującą wymagany zakres szkolenia.
3. Szkolenie w zakresie ochrony danych osobowych w pracy zdalnej przeprowadza IOD.

4. Zapoznanie pracownika z zasadami postępowania określonymi w Procedurze jest tożsame z ich akceptacją i stanowi przeszkolenie w tym zakresie.
5. Odbycie szkolenia pracownik potwierdza składając stosowne oświadczenie, które przechowywane jest na Stanowisku ds. kadr.

7. Bezpieczeństwo stanowiska pracy

1. Pracownik jest odpowiedzialny za zapewnienie odpowiednich warunków lokalowych i technicznych niezbędnych do świadczenia pracy zdalnej oraz właściwe zabezpieczenie dostępu do sprzętu służbowego oraz posiadanych danych i informacji przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
2. Pracownik zobowiązany jest do:
   1) wykonywania pracy w miejscu, które gwarantuje zachowanie poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji;
   2) przechowywania komputerów i nośników informacji, w tym zawierających dane osobowe w szafkach/pomieszczeniach, uniemożliwiających dostęp do nich przez osoby postronne (zasada chronionego pomieszczenia);
   3) niepozostawiania nośników zawierających dane osobowe (zarówno sprzętu, jak i nośników papierowych) bez nadzoru - zarówno w trakcie wykonywania pracy zdalnej, jak i po jej zakończeniu (zasada czystego biurka);
   4) ustawienia monitora komputera w sposób uniemożliwiający osobom postronnym wgląd i dostęp do wyświetlanych na ekranie informacji np. poprzez odpowiednie ustawienie ekranu lub zastosowanie nakładki na ekran tzw. filtru /folii prywatyzującej;
   5) blokowania komputera przed każdorazowym opuszczeniem stanowiska do wykonywania pracy zdalnej oraz poprawnego wyłączenia sprzętu służbowego po zakończeniu pracy (zasada czystego ekranu);
   6) zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (zasada czystej drukarki);
   7) trwałego niszczenia nieprzydatnych brudnopisów w sposób uniemożliwiający odtworzenie zawartych w nich informacji (zasada czystego kosza).

8. Praca z dokumentami papierowymi

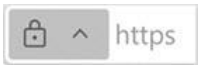
1. W celu zminimalizowania ryzyka naruszenia integralności danych oraz utraty ich dostępności nie dopuszcza się wynoszenia poza siedzibę Urzędu oryginałów dokumentów w formie papierowej.
2. Pracownik podczas pracy zdalnej, jeżeli jest to niezbędne do realizacji obowiązków pracowniczych, powinien pracować na kopiach dokumentów papierowych i chronić je tak samo jak dokumentację oryginalną.
3. Na kopii dokumentów zawierających dane osobowe należy dokonać w miarę możliwości anonimizacji danych.

4. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą Urzędu pracownik zgłasza taką potrzebę do bezpośredniego przełożonego.
5. Po uzyskaniu pisemnej zgody bezpośredniego przełożonego na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów, w godzinach pracy Urzędu.
6. Pracownik zobowiązany jest do bezpiecznego transportu oraz zabezpieczania dokumentacji po zakończonym dniu pracy przed dostępem osób nieuprawnionych poprzez przechowywanie dokumentacji w zamykanych na klucz szafach/ pomieszczeniach.
7. Podczas pracy zdalnej pracownik zobowiązany jest przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania pracy zdalnej (zasada ograniczenia przetwarzania).
8. Po zakończeniu pracy zdalnej, pracownik ma obowiązek zwrotu wszystkie kopie dokumentów do siedziby Urzędu.
9. Po analizie, kopie dokumentów podlegają archiwizacji zgodnie z obowiązującymi przepisami w tym zakresie lub zniszczeniu (za pomocą niszczarki).
10. Zabrania się drukowania lub kopiowania dokumentów służbowych w ogólnodostępnych punktach ksero lub z pomocą innych podmiotów czy osób trzecich.

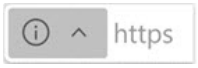
9. Praca z danymi w obiegu elektronicznym

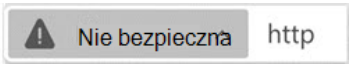
1. Na sprzęcie służbowym nie może być instalowane żadne nielegalne oprogramowanie.
2. Instalowanie jakiegokolwiek oprogramowania na sprzęcie służbowym jest możliwe tylko przez pracowników BIiRSI.
3. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności dorosłych domowników i dzieci.
4. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnionych mu przez Pracodawcę.
5. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu sprzętu służbowego.
6. Pracownik nie może przechowywać na sprzęcie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
7. Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, nie może korzystać z laptopa służbowego w miejscach publicznych jak np.: restauracje, bary, parki, centra handlowe, biblioteki itp.
8. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych (np. Dysk Google), komunikatorach (np. Messenger lub WhatsApp) lub innych usługach dostępnych w sieci.
9. Sprzęty służbowe chronione są hasłem.

10. Pracownik nie może łączyć się z systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy. Łącząc się z zasobami sieciowymi Urzędu, pracownik jest zobowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN.
11. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
12. Przy wysyłaniu wiadomości e-mail pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
13. Podczas wysyłania korespondencji zbiorczej pracownik zobowiązany jest do korzystania z opcji „kopia ukryta" (pole UDW– Ukryci Do Wiadomości lub BCC– Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.
14. W przypadku korzystania z przeglądarki internetowej należy sprawdzić informacje o jej zabezpieczeniach, zgodnie z tabelą poniżej. W tym celu należy kliknąć na symbol stanu bezpieczeństwa na lewo od adresu internetowego gdzie wyświetli się informacja o stopniu prywatności połączenia.

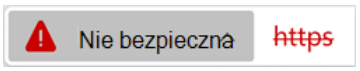


Bezpieczne połączenie (prawidłowy certyfikat),

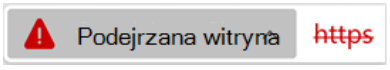


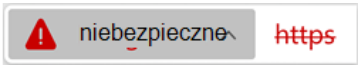


Nie w pełni bezpieczny (brak prawidłowego certyfikatu)



Nieaktualna konfiguracja zabezpieczeń (nieprawidłowe, wygasłe, z podpisem własnym).





Podejrzana lub niebezpieczna witryna internetowa (wyłudzanie informacji lub złośliwe oprogramowanie)

15. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
16. W przypadku wiadomości zawierających informacje poufne lub dane osobowe konieczne jest zabezpieczanie plików hasłem dostępu i przekazywanie tego hasła innym kanałem komunikacyjnym.
17. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z BIiRSI.
18. Pracownik nie ma prawa korzystać ze sprzętu służbowego w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralny, niestosownym, mając na uwadze powszechnie obowiązujące zasady postępowania.
19. Zasady bezpiecznego odbywania wideokonferencji określa rozdział 10 Procedury.

10. Zasady bezpiecznego prowadzenia wideokonferencji

Zasady bezpiecznego prowadzenia wideokonferencji[3]	
Etapy wideokonferencji	**Wytyczne**
Przed rozpoczęciem wideokonferencji	1. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać. 2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane. 3. Zweryfikuj, do jakich celów będą wykorzystywane Twoje dane osobowe. 4. Sprawdź, o jakie uprawnienia do danych jesteś proszony - lista kontaktów, lokalizacja itp. 5. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu. 6. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie. 7. Korzystaj z aplikacji webowych, nie desktopowych. 8. Zabezpiecz sieć Wi-Fi silnym hasłem. 9. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli. 10. Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów. 11. Przeskanuj program do telekonferencji systemem antywirusowym.
W trakcie korzystania z wideokonferencji	1. Ogranicz ilość podawania danych osobowych - użyj pseudonimu i służbowego adresu e-mail. 2. Użyj innego hasła, niż używane przez Ciebie w innych usługach. 3. Nie udostępniaj linków do konferencji w mediach społecznościowych. 4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line. 5. Zarządzaj opcjami udostępniania ekranu. 6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN. 7. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny. 8. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych). 9. Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia). 10. Korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji; unikniesz przypadkowych lub niechcianych osób. 11. Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne).
Po skorzystaniu z wideokonferencji	1. Wyłącz mikrofon i kamerę. 2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację. 3. Sprawdź, czy program do telekonferencji nie działa w tle. 4.

[3] Opracowano na podstawie: https://uodo.gov.pl/pl/138/1525.

11. Zarządzanie narzędziami pracy zdalnej

1) BIiRSI:
   a) prowadzi wykaz sprzętu służbowego wydanego pracownikowi pracującemu zdalnie;
   b) zapewnia, aby sprzęt służbowy wydawany pracownikowi został wcześniej odpowiednio skonfigurowany, w szczególności zabezpieczony przed ujawnieniem lub utratą oraz posiadał aktualną ochroną antywirusową,
   c) określa zasady dotyczące instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonego pracownikowi sprzętu służbowego,
   d) zapewnia wsparcie techniczne ze strony Pracodawcy.
2) Pracownik jest zobowiązany:
   a) przed rozpoczęciem pracy zdalnej zweryfikować z pracownikiem BIiRSI prawidłowość działania sprzętu służbowego, konfiguracji kanału VPN,
   b) właściwie eksploatować i dbać o powierzony mu służbowy sprzęt oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego,
   c) stosować zasady, o których mowa w pkt 1 lit. c.
3) Zabrania się samodzielnego przekazywania sprzętu służbowego do serwisu. W przypadku awarii narzędzi pracy zdalnej należy niezwłocznie skontaktować się z BIiRS. Zakazane jest kontynuowanie pracy na sprzęcie służbowym, który został uszkodzony, zużyty lub zachodzi potrzeba jego wymiany.

12. Naruszenie ochrony danych osobowych

Pracownik zobowiązany jest do niezwłocznego zgłaszania wystąpienia lub podejrzenia wystąpienia wszelkich zdarzeń (incydentów) naruszających lub mogących skutkować naruszeniem bezpieczeństwa informacji, cyberbezpieczeństwa, czy też ochrony danych osobowych w sposób określony w wewnętrznych regulacjach obowiązujących w Urzędzie.

13. Postanowienia końcowe

1. Pracownik jest zobowiązany informować, gdy warunki pracy zdalnej (np. warunki lokalowe) mogą naruszać wymogi (w tym bezpieczeństwa fizycznego) zawarte w niniejszej Procedurze.
2. W sprawach nieuregulowanych Procedurą zastosowanie znajdą wewnętrzne regulacje obowiązujące u Pracodawcy oraz przepisy prawa powszechnie obowiązującego.