

Centrum Usług Wspólnych w Okonku


ul. Leśna 46, 64-965 Okonek,
☎ (67) 266 91 45

ZARZĄDZENIE Nr 14/2023 Dyrektora Centrum Usług Wspólnych w Okonku z dnia 17 maja 2023 r.

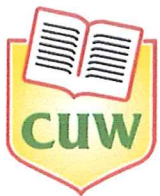
w sprawie wprowadzenia „Procedury ochrony danych osobowych w ramach pracy zdalnej w Centrum Usług Wspólnych w Okonku”

Na podstawie art. 67²⁶ § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2022 roku poz. 1510 z późn. zm.), zarządza się, co następuje:

- § 1. Wprowadza się „Procedurę ochrony danych osobowych w ramach pracy zdalnej w Centrum Usług Wspólnych w Okonku” stanowiącą załącznik do niniejszego zarządzenia.
- § 2. Wykonanie zarządzenia powierza się inspektorowi ds. kadr.
- § 3. Zarządzenie wchodzi w życie po 14 dniach od dnia ogłoszenia i podlega publikacji w Biuletynie Informacji Publicznej Centrum Usług Wspólnych w Okonku.


DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

edw.

Procedura ochrony danych osobowych w ramach pracy zdalnej w Centrum Usług Wspólnych w Okonku

§ 1. Zakres i cel procedury

1. Procedura ochrony danych osobowych w ramach pracy zdalnej, zwana dalej *Procedurą*, określa zasady postępowania z danymi osobowymi, zasady ich zabezpieczenia i ochrony podczas wykonywania pracy zdalnej.
2. Ilekroć w Procedurze mowa jest o:
 - 1) Pracodawcy, administratorze – należy przez to rozumieć pracodawcę pracownika wykonującego pracę zdalną.
 - 2) Dane osobowe – należy przez to rozumieć dane osobowe w rozumieniu art. 4 pkt 1) RODO, czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takiej osobie, 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.
 - 3) IOD – należy przez to rozumieć Inspektora Ochrony Danych, powoływanego przez Administratora zgodnie z art. 37 RODO.
 - 4) Przetwarzaniu – należy przez to rozumieć operację lub zestaw operacji określonych w art. 4 pkt 2) RODO, takie 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.
 - 5) RODO – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. Nr 119, s. 1 ze zm.).
3. Przed rozpoczęciem pracy zdalnej pracownik:
 - 1) potwierdza zapoznanie się z treścią niniejszej Procedury i składa oświadczenie, o którym mowa w załączniku Nr 1 do Procedury;

- 2) potwierdza zapoznanie się z informacją dotyczącą przetwarzania jego danych osobowych w toku pracy zdalnej stosownie do treści załącznika Nr 2 Procedury;
4. Oświadczenie przechowywane jest w aktach osobowych, przez okres prowadzenia akt dla danego pracownika przewidziany przepisami prawa pracy.
5. Obowiązek stosowania *Procedury* dotyczy każdego pracownika wykonującego pracę zdalną bez względu na tryb jej uruchomienia.

§ 4. Dokumentacja ochrony danych osobowych

1. Dokumentację ochrony danych osobowych u pracodawcy stanowią:
 - 1) polityka ochrony danych/polityka bezpieczeństwa informacji;
 - 2) instrukcja zgłaszania naruszeń;
 - 3) instrukcja postępowania z wnioskami dotyczącymi ochrony danych osobowych;
 - 4) instrukcja zarządzania systemem informatycznym;
 - 5) niniejsza procedura.
2. Pracownik zobowiązany jest do stosowania zasad ochrony danych osobowych, w tym zasad uzyskiwania dostępu, przesyłania, przechowywania i wykonywania obowiązków związanych z przetwarzaniem danych osobowych.
3. W przypadku wątpliwości co do dopuszczalnego postępowania z danymi osobowymi, pracownik, po sprawdzeniu, czy dokumentacja ochrony danych osobowych nie reguluje takiego obszaru, kontaktuje się z wyznaczoną u pracodawcy osobą, tj. IOD lub osobą odpowiedzialną za nadzór nad przetwarzaniem danych osobowych.

§ 5. Dostęp do danych osobowych i praca z danymi osobowymi

1. Pracownik wykonujący pracę zdalną, uzyskuje dostęp do danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków pracowniczych. Dostęp do danych osobowych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania i trwa do momentu ustania zatrudnienia.
2. Niedozwolone jest gromadzenie, instalowanie i użytkowanie oprogramowania, plików oraz innych informacji pochodzących z nielegalnego lub niewiadomego źródła oraz będących w sprzeczności z przepisami prawa, przyjętymi u Pracodawcy procedurami oraz niezwiązanymi z wykonywaniem obowiązków pracownika.
3. Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków służbowych.
4. Pracownik utrzymuje w tajemnicy otrzymane od pracodawcy dane dostępowe, w tym loginy i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników. Szczegółowe zasady dotyczące zmiany hasła, jego budowy i przechowywania pracodawca może określić w dokumentacji ochrony danych osobowych.
5. Pracownik jest zobowiązany do pracy w ramach przydzielonego mu konta w systemie informatycznym. Nie jest dopuszczalne udostępnianie konta, loginu, hasła osobom

nieuprawnionym, w tym innym pracownikom lub domownikom, ani też korzystanie z konta, loginu, hasła innego pracownika.

6. Dostęp do danych osobowych odbywa się w sposób zdalny i następuje poprzez:
 - 1) dostęp do skrzynki pocztowej pracownika w domenie pracodawcy;
 - 2) dostęp do systemu informatycznego przetwarzającego dane osobowe (w tym: imię i nazwisko, PESEL, adres zamieszkania);
 - 3) dostęp do określonych zasobów w infrastrukturze pracodawcy przy użyciu szyfrowanego połączenia zdalnego (np. VPN).
7. Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych, wyłącznie poprzez wskazane przez pracodawcę narzędzia i połączenia. Jeżeli pracownik przesyła załączniki zawierające dane osobowe muszą być one zaszyfrowane odpowiednim programem (np. zip). Nie należy przysyłać plików z danymi osobowymi (np. w celu pracy z danymi osobowymi), jeżeli możliwy jest dostęp do danych w systemie informatycznym.
8. Pracodawca odbiera pracownikowi wydany sprzęt służbowy, w szczególności gdy:
 - 1) nie jest już niezbędny do wykonywania obowiązków służbowych w ramach pracy zdalnej;
 - 2) pracownik używa wydany sprzęt w sposób niezgodny z niniejszą Procedurą oraz innymi dokumentami dotyczącymi bezpieczeństwa korzystania ze sprzętu, zasadami współżycia społecznego lub przepisami prawa;
 - 3) sprzęt został uszkodzony, zużyty lub zachodzi potrzeba jego wymiany;
 - 4) pracownik zakończy współpracę z Pracodawcą (niezależnie od podstawy nawiązania lub zakończenia współpracy).

§ 6. Przechowywanie danych osobowych i nośników

1. Pracownik odpowiada za bezpieczne przechowywanie danych osobowych, sprzętu i nośników służących do ich przetwarzania.
2. Nośniki oraz dokumentacja zawierająca dane osobowe nie powinna być pozostawiana bez nadzoru. Po zakończeniu pracy nośniki i dokumentacja powinny być schowane w miejscu zabezpieczonym przed osobami nieuprawnionymi (np. w szafce, szufladzie).

§ 7. Transport sprzętu i nośników danych

1. Pracownik odpowiada za bezpieczeństwo powierzonego mu sprzętu, nośników i dokumentacji podczas ich transportu. W szczególności nie jest dozwolone pozostawianie ich bez nadzoru (np. w środku transportu – samochodzie, komunikacji publicznej).
2. Przewożenie dokumentacji zawierającej dane osobowe powinno odbywać się w sposób zabezpieczający ją przed dostępem osób nieuprawnionych. W tym celu pracownik umieszcza dokumentację w teczce lub skoroszycie uniemożliwiającym zapoznanie się z treścią danych osobowych, a następnie w plecaku lub torbie.

§ 8. Szkolenia

1. Pracownik uczestniczy we wszystkich szkoleniach, warsztatach, instruktażach dotyczących ochrony danych osobowych i bezpieczeństwa informacji, w tym w ramach pracy zdalnej.
2. Udział pracownika w wyżej wskazanych formach doształcania ma charakter obowiązkowy oraz aktywny.

§ 9. Zgłaszanie incydentów


1. Pracownik zgłasza incydenty ochrony danych oraz ich podejrzenia osobom odpowiedzialnym w zakładzie pracy za ochronę danych osobowych (IOD lub inna osoba wskazana przez pracodawcę).
2. W przypadku zauważenia nieprawidłowości w funkcjonowaniu systemów informatycznych pracownik podejmuje możliwe działania zabezpieczające jednocześnie z powiadomieniem właściwych osób, zgodnie z § 9 pkt 1 Procedury.
3. Szczegółowy sposób postępowania w przypadku zauważenia incydentu ochrony danych określa dokumentacja ochrony danych osobowych obowiązująca w zakładzie pracy.

§ 10. Stosowanie zabezpieczeń przez pracowników

1. Pracownik zobowiązany jest do dbałości o bezpieczeństwo danych osobowych przetwarzanych w ramach wykonywania obowiązków służbowych.
2. W celu dbałości o bezpieczeństwo danych osobowych, podczas codziennej pracy pracownik:
 - 1) ogranicza do niezbędnego minimum drukowanie plików zawierających dane osobowe i do sytuacji, gdy jest to konieczne;
 - 2) niszczy robocze wydruki zawierające dane osobowe po ustaniu ich przydatności dla bieżącej pracy; nie można wyrzucać dokumentów zawierających dane osobowe do kosza, zniszczenie musi mieć charakter nieodwracalny, np. przy użyciu niszczarki lub nożyczek;
 - 3) cyklicznie usuwa niepotrzebne pliki zawierające dane osobowe, pobrane w celu pracy z nimi;
 - 4) przechowuje dokumentację zawierającą dane osobowe w sposób bezpieczny, zamkniętą w teczce, skoroszytcie lub segregatorze, w miejscu niedostępnym dla osób postronnych (szafka, szuflada);
 - 5) wylogowuje się z systemów informatycznych po zakończeniu pracy w nich;
 - 6) zabezpiecza ekran przed dostępem innych osób, w tym domowników, poprzez stosowanie wygaszaczy ekranów lub każdorazowe wylogowanie się przed odejściem od ekranu;
 - 7) nie korzysta i nie uruchamia programów i aplikacji pochodzących od nieznanych nadawców;
 - 8) nie udostępnia domownikom komputerów przenośnych przeznaczonych do pracy, jeżeli komputer stanowi własność pracownika, praca odbywa się wyłącznie na wydzielonych kontach systemowych. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
- 9) Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny one zostać zabezpieczone hasłem.

A

- 10) Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
- 11) Hasła, o których mowa w § 9 pkt. 9 i 10, nadawca przekazuje odbiorcy inną drogą komunikacji bądź odrębnym mailem. Dopuszczalne jest ustalenie stałego hasła z jednym odbiorcą.
- 12) Każda wiadomość powinna być wysyłana z należyłą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
- 13) W przypadku wykonywania masowych wysyłek wiadomości e-mail należy realizować je poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.


DYREKTOR
Centrum Usług Wspólnych
w Olkuszku
Renata Kubrocka



**Załącznik nr 1 do
Procedury ochrony danych osobowych w ramach pracy zdalnej
w Centrum Usług Wspólnych w Okonku**

**Oświadczenie o zapoznaniu się z procedurami ochrony danych
osobowych przetwarzanych w ramach pracy zdalnej**

Oświadczam, że – w związku z wykonywaniem przeze mnie pracy zdalnej na rzecz Centrum Usług Wspólnych w Okonku zostałem/zostałam przeszkolony/przeszkolona w dziedzinie ochrony i przetwarzania danych osobowych w zakresie niezbędnym do realizacji moich obowiązków w sposób zdalny, a także zapoznałem/zapoznałam się ze stosownymi przepisami i przyjętymi u pracodawcy procedurami dotyczącymi ochrony danych osobowych przetwarzanych w sposób zdalny i zobowiązuję się do ich przestrzegania.

.....
(data, podpis pracownika)

4

KLAUZULA INFORMACYJNA
dla pracownika wykonującego pracę zdalną w
CENTRUM USŁUG WSPÓLNYCH W OKONKU

Ilekróć zebranie od Państwa i/lub Państwa pracodawców danych osobowych Państwa dotyczących będzie niezbędne i/lub konieczne do wypełnienia zadań statutowych realizowanych przez Centrum Usług Wspólnych w Okonku, należytego wykonania zawartych umów i wykonania innych zadań Centrum Usług Wspólnych w Okonku, zgodnie z art. 13 i art. 14 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), Centrum Usług Wspólnych w Okonku informuje, że :

1. Administratorem Pana/Pani danych osobowych jest Centrum Usług Wspólnych w Okonku, z siedzibą w Okonku przy ul. Leśna 43, 64-965 Okonek, reprezentowane przed Dyrektora Centrum Usług Wspólnych w Okonku.
2. Inspektorem ochrony danych osobowych w Centrum Usług Wspólnych w Okonku jest Anna Frąk, adres e-mail: iod@adwokat-pila.com.pl lub pisemnie na adres Admiratora z dopiskiem Inspektor Ochrony Danych.
3. Pani/Pana dane osobowe będą przetwarzane w celach i na podstawach prawnych wskazanych poniżej.

Cel	Podstawa prawna
Ukształtowanie i realizacja pracy zdalnej na zasadach określonych w przepisach prawa, w ramach: 1) uzgodnienia między pracodawcą a pracownikiem lub 2) polecenia wykonywania pracy zdalnej.	<i>Ad 1. Art. 6 ust. 1 lit. b RODO (wykonanie umowy, podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy).</i> <i>Ad 2. Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora) w zw. z art. 6 ust. 1 lit. c RODO (obowiązek administratora), np. w zakresie obowiązku podania i uzgodnienia miejsca wykonywania pracy zdalnej, rozpatrzenia wniosku pracownika.</i>
Obowiązek pracodawcy uwzględnienia wniosku pracownika o wykonywanie pracy zdalnej (w warunkach art. 67 ¹⁹ § 6 KP).	<i>Art. 6 ust. 1 lit. c RODO w zw. z art. 67¹⁹ § 6 KP, art. 9 ust. 2 lit. b RODO w zw. z art. 67¹⁹ § 6 KP (realizacja obowiązku ciążącego na administratorze).</i>
Realizacja obowiązku pracodawcy rozpatrzenia wniosku pracownika o zaprzestanie wykonywania pracy zdalnej i przywrócenie poprzednich warunków wykonywania pracy.	<i>Art. 6 ust. 1 lit. c RODO w zw. z art. 67²² KP, art. 9 ust. 2 lit. b RODO w zw. z art. 67²² § 1 KP (realizacja obowiązku ciążącego na administratorze).</i>
Realizacja obowiązków pracodawcy związanych z organizacją pracy zdalnej.	<i>Art. 6 ust. 1 lit. c RODO w zw. z art. 67²⁴ KP (realizacja obowiązku ciążącego na administratorze).</i>
Przeprowadzenie kontroli pracy zdalnej.	<i>Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora).</i>
Obowiązek reakcji w przypadku zidentyfikowanych nieprawidłowości w toku kontroli.	<i>Art. 6 ust. 1 lit. c RODO w zw. z art. 67²⁸ KP (realizacja obowiązku ciążącego na administratorze).</i>
Obsługa wypadku przy pracy zdalnej stosownie do wymogów szczególnych zawartych w art. 67 ³¹ § 9 KP.	<i>Art. 6 ust. 1 lit. c RODO w zw. z art. 67³¹ § 9 KP (realizacja obowiązku ciążącego na administratorze).</i>
Zapewnienie organizacji pracy	<i>Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes</i>

Cel	Podstawa prawna
umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy (monitoring).	administratora).
Zapewnienie przestrzegania przepisów o ochronie danych osobowych (np. monitorowanie bezpieczeństwa).	Art. 6 ust. 1 lit. c RODO w zw. z art. 32 RODO i art. 67 ²⁶ KP (realizacja obowiązku ciężącego na administratorze).

4. Dane osobowe zostaną usunięte po upływie okresów ich przechowywania przewidzianych przepisami prawa, np. w przypadku umowy o pracę, której częścią są uzgodnienia lub polecenie pracy zdalnej – po upływie okresu zatrudnienia pracownika, a także 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygaś (ewentualnie 50 lat liczone od daty ustania stosunku pracy dla pracowników, z którymi stosunki pracy zostały nawiązane przed 1.1.2019 r.). Pozostałe dane osobowe zostaną usunięte maksymalnie po upływie okresu przedawnienia potencjalnych roszczeń związanych z zawarciem lub realizacją umowy, w tym zobowiązań publicznoprawnych, lub krócej, jeżeli zgłosicie Państwo skuteczny sprzeciw. Podanie danych wynikających z przepisów prawa jest obowiązkowe. Podanie pozostałych danych jest dobrowolne, ale niezbędne do realizacji ww. celów.
5. Pani/Pana dane osobowe będą mogły być przez nas przekazywane naszym partnerom, z którymi mamy zawarte umowy na współpracę przy wykonywaniu naszym zadań statutowych i innych obowiązków prawnych, w tym umownych, podmiotom świadczących na naszą rzecz pomoc prawną, usługi doradcze, konsultacyjne, dostawcy usług informatycznych, poczty elektronicznej, systemów kadrowych, systemów monitorowania i ewidencji czasu pracy) oraz innym podmiotom działającym na nasze zlecenie, a świadczącym nam usługi niezbędne do realizacji naszych zadań statutowych i wykonania innych obowiązków prawnych, w tym umownych
6. Podanie danych jest dobrowolne, ale niezbędne do realizacji ww. celów (jest to wymóg prawny w przypadku podstawy przetwarzania danych z art. 6 ust. 1 lit. c RODO lub umowny w przypadku podstawy przetwarzania danych z art. 6 ust. 1 lit. b RODO lub związany z uzasadnionym interesem Administratora w przypadku podstawy przetwarzania danych z art. 6 ust. 1 lit. f RODO)
7. Zgodnie z RODO, przysługują Pani/Panu :
 - a. prawo żądania od nas dostępu do danych osobowych dotyczących Pani/ Pana,
 - b. prawo sprostowania Pani/Pana danych osobowych,
 - c. prawo żądania usunięcia lub ograniczenia przetwarzania Pani/Pana danych osobowych
 - d. prawo sprzeciwu wobec przetwarzania danych na podstawie art. 21 RODO, w przypadku gdy łącznie spełnione są następujące przesłanki:
 - zaistnieją przyczyny związane z Pani/Pana szczególną sytuacją, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez Administratora,
 - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.
 - e. prawo przenoszenia Pani/Pana danych;
 - f. prawo do cofnięcia zgody w dowolnym momencie, w przypadku gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO). Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

- g. prawo wniesienia skargi do organu nadzorczego na niezgodne z prawem przetwarzanie Pani/Pana danych osobowych przez Administratora. Organem właściwym do wniesienia skargi jest Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
8. Pani/Pana dane nie będą profilowane i nie będą udostępniane ani przekazywane na rzecz Państwa trzeciego i/lub organizacji międzynarodowej.

ADMINISTRATOR

AK