

ZARZĄDZENIE Nr 54/2025
Burmistrz Miasta i Gminy Drobin
z dnia 01 kwietnia 2025 roku

w sprawie: wprowadzenia procedury bezpieczeństwa informacji i ochrony danych osobowych podczas pracy zdalnej

Na podstawie art. 67²⁶ ustawy z dnia 26 czerwca 1974 roku Kodeks Pracy (Dz. U. z 2025 r., poz. 277) zarządzam, co następuje:

§ 1

Wprowadza się Procedurę bezpieczeństwa informacji i ochrony danych osobowych podczas pracy zdalnej, zwany dalej „procedurą”, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się Sekretarza Miasta i Gminy do przekazania treści Regulaminu Pracy pracownikom Urzędu Miasta i Gminy w Drobinie, wykonującym pracę zdalną.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta i Gminy Drobin

Grzegorz Szykowski



Załącznik Nr 1

do Zarządzenia Nr 54/2025
Burmistrza Miasta i Gminy Drobin
z dnia 01 kwietnia 2025 r.

PROCEDURA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

§ 1. Wprowadzenie

1. Na potrzeby wykonywania pracy zdalnej pracodawca określa niniejsze procedury ochrony danych osobowych, które wynikają z art. 67²⁶ § 1 kodeksu pracy.
2. Postanowienia zawarte w tym dokumencie dotyczą wszystkich pracowników bez względu na zajmowane stanowisko i rodzaj wykonywanej pracy, a także rodzaj umowy o pracę.
3. Ilekroć w regulaminie pracy jest mowa o:
 - a) procedurze – należy przez to rozumieć Procedurę bezpieczeństwa informacji i ochrony danych osobowych podczas pracy zdalnej,
 - b) pracodawcy, zakładzie pracy, urzędzie – należy przez to rozumieć Urząd Miasta i Gminy Drobin, w imieniu którego występuje Burmistrz lub inna upoważniona do tego osoba,
 - c) pracownikowi – należy przez to rozumieć osoby zatrudnione na podstawie, wyboru, powołania i umowy o pracę (bez względu na rodzaj i wymiar czasu pracy),
 - d) osobie prowadzącej sprawy kadrowe – należy przez to rozumieć pracownika zatrudnionego na stanowisku inspektora ds. kadr i płac,
 - e) ADO – należy przez to rozumieć Administratora Danych Osobowych,
 - f) ASI – należy przez to rozumieć Administratora Systemu Informatycznego.
4. Za przegląd i aktualizację niniejszej Procedury odpowiada ADO oraz ASI. Przeglądu Procedury dokonuje się co najmniej raz w roku kalendarzowym. W przypadku aktualizacji Procedury należy uzyskać potwierdzenie zapoznania się z nową wersją Procedury zgodnie z § 2 ust. 1 lit. a Procedury. Za komunikację nowej wersji Procedury odpowiada osoba prowadząca sprawy kadrowe. Nowa wersja Procedury wchodzi w życie po upływie 7 dni od jej zatwierdzenia przez Burmistrza Miasta i Gminy Drobin. Następnie należy zapoznać pracowników pracujących zdalnie oraz uzyskać od nich oświadczenie, o którym mowa w § 2 ust. 1 lit. a maksymalnie w ciągu 15 dni.
5. Treść niniejszej Procedury jest konsultowana z inspektorem ochrony danych.
6. Pracownik obowiązany jest do niezwłocznego poinformowania Pracodawcy lub ASI, IOD o wszelkich stwierdzonych nieprawidłowościach lub gdy warunki pracy zdalnej mogą naruszać wymogi (w tym bezpieczeństwa fizycznego) zawarte w niniejszej Procedurze.

§ 2. Rozpoczęcie pracy zdalnej

1. Przed rozpoczęciem pracy zdalnej pracownik:
 - a) potwierdza zapoznanie się z treścią niniejszej Procedury i składa oświadczenie, o którym mowa w załączniku Nr 1 do Procedury;
 - b) uzyskuje upoważnienie do przetwarzania danych osobowych zgodnie z odrębną procedurą;
 - c) składa oświadczenie o zachowaniu poufności, którego wzór znajduje się w załączniku nr 1 do Procedury;

- d) zapoznaje się z informacją dotyczącą przetwarzania jego danych osobowych w toku pracy zdalnej stosownie do treści załącznika Nr 2 Procedury;
 - e) w miarę potrzeby odbywa szkolenie w zakresie pracy zdalnej zgodnie z § 3 Procedury, które jest dokumentowane w sposób wskazany w § 3 Procedury.
2. Osoba prowadzącą sprawy kadrowe prowadzi listę pracowników pracujących zdalnie.
 3. Osoba prowadzącą sprawy kadrowe przekazuje informację o potrzebie przeprowadzenia szkolenia wstępnego inspektorowi ochrony danych.

§ 3. Szkolenia

1. Szkolenie dotyczące ochrony danych osobowych w zakresie pracy zdalnej przeprowadza IOD lub inna osoba wyznaczona przez ADO.
2. O konieczności przeprowadzenia szkolenia wstępnego (przed rozpoczęciem pracy zdalnej) osoba prowadzącą sprawy kadrowe informuje inspektora ochrony danych.
3. Szkolenie przeprowadza inspektor ochrony danych.
4. Szkolenie jest dokumentowane w formie listy obecności, która przechowywana jest w kadrach.

§ 4. Zarządzanie narzędziami pracy zdalnej

1. ASI prowadzi wykaz sprzętu [*np. laptopy, smartfony*] wydanego pracownikom pracującym zdalnie.
2. ASI zapewnia, żeby sprzęt wydawany pracownikowi został wcześniej odpowiednio skonfigurowany, w szczególności sprzęt ten powinien zostać zabezpieczony przed ujawnieniem lub utratą zgodnie z zasadami bezpieczeństwa sprzętu przyjętymi w urzędzie.
3. Przed przekazaniem pracownikowi narzędzi pracy, w tym urządzeń technicznych, które wykorzystywane będą w pracy zdalnej ADO zabezpiecza je za pomocą adekwatnych środków technicznych, w szczególności sprzęt powinien:
 - a) posiadać legalne oprogramowanie,
 - b) posiadać legalne oprogramowanie antywirusowe,
 - c) wykonywane są aktualizacje,
 - d) dostęp do komputera odbywa się poprzez podanie loginu i hasła.
4. ASI przygotowuje dla pracowników pracujących zdalnie instrukcję dotyczącą instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych.
5. Pracownik jest zobowiązany stosować się do zakomunikowanych zasad dotyczących instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych.
6. Urząd udostępnia pracownikom listę osób uprawnionych do wsparcia pracownika (w zakresie instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych) w sposób minimalizujący ryzyko

podszycia się pod te osoby. Pracownik może się komunikować wyłącznie ze wskazanymi osobami.

§ 5. Zabezpieczenie zdalnego dostępu

1. Wszystkie zdalne połączenia wykorzystywane w związku z pracą zdalną przed rozpoczęciem jej wykonywania ADO odpowiednio zabezpiecza.
2. Komunikację pomiędzy podmiotami dopuszcza się jedynie z wykorzystaniem szyfrowanego tunelu VPN.

§ 6. Kopie bezpieczeństwa przetwarzanych danych

ADO określa potrzebę a w przypadku jej stwierdzenia także zasoby danych, które podlegać mają procedurze tworzenia kopii zapasowych, w związku z wykonywaniem przez pracownika pracy zdalnej, a następnie w miarę potrzeby przeprowadza stosowny instruktaż oraz szkolenie w zakresie korzystania z ww. funkcjonalności.

§ 7. Bezpieczeństwo narzędzi pracy zdalnej

1. Pracownicy są zobowiązani do zapewnienia bezpieczeństwa sprzętu służbowego, danych do logowania (login i hasło) oraz przechowywanych na nim informacji, w tym danych osobowych, w szczególności poprzez:
 - a) niepozostawianie wydanego sprzętu służbowego bez nadzoru;
 - b) niezapisywanie nigdzie danych do logowania się (loginu i hasła);
 - c) korzystanie ze sprzętu w sposób bezpieczny, w szczególności niedozwolone jest korzystanie z publicznych sieci bezprzewodowych;
 - d) korzystania wyłącznie z szyfrowanych pendrive'ów, wydanych im zgodnie z § 4 ust. 1 powyżej;
 - e) nieudostępniania sprzętu osobom postronnym do korzystania oraz niekorzystania ze sprzętu do celów prywatnych.
2. Pracownik jest zobowiązany właściwie eksploatować i dbać o powierzony mu sprzęt oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części (np. monitorów, drukarek, myszy).
3. 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 w urzędzie procedurami oraz niezwiązanymi z wykonywaniem obowiązków pracownika w urzędzie.
4. Zakazane jest drukowanie dokumentów zawierających dane osobowe lub tajemnice urzędu, z wyłączeniem sytuacji, gdy odbywa się to na polecenie ADO.
5. Wszystkie dane służbowe (pliki, dokumenty, notatki wytworzone, modyfikowane lub otrzymane w związku z wykonywanymi zadaniami służbowymi) powinny być umieszczane i przechowywane na zasobach udostępnionych przez urząd.

6. W przypadku awarii lub braku dostępu do zasobów sieciowych urzędu dopuszczalne jest czasowe zapisanie danych służbowych na dysku twardym komputera służbowego. W takim wypadku pracownik jest zobowiązany do przeniesienia zapisanych danych służbowych na właściwie miejsce w zasobach sieciowych niezwłocznie po odzyskaniu dostępu do tych zasobów, a następnie usunięcia tych danych ze swego komputera.
7. Pracodawca odbiera pracownikowi wydany sprzęt służbowy, w szczególności gdy:
 - a) nie jest już niezbędny do wykonywania obowiązków służbowych w ramach pracy zdalnej;
 - b) pracownik używa wydany sprzęt w sposób niezgodny z niniejszą Procedurą oraz innymi dokumentami dotyczącymi bezpieczeństwa korzystania ze sprzętu przyjętymi w urzędzie, zasadami współżycia społecznego lub przepisami prawa;
 - c) sprzęt został uszkodzony, zużyty lub zachodzi potrzeba jego wymiany;
 - d) pracownik zakończy współpracę z urzędem (niezależnie od podstawy nawiązania lub zakończenia współpracy).
8. W przypadku gdy podstawą odebrania sprzętu jest zakończenie współpracy z urzędem, osoba prowadząca sprawy kadrowe jest zobowiązana do niezwłocznego poinformowania ASI o zakończeniu współpracy z danym pracownikiem (ze wskazaniem jej daty), w celu uniemożliwienia takiemu pracownikowi dalszego dostępu do powierzonego sprzętu i systemów – najpóźniej z datą zakończenia współpracy z urzędem.
9. Zakazane jest samodzielne (bez konsultacji z działem IT) przekazywanie sprzętu do serwisu. W przypadku awarii narzędzi pracy zdalnej należy niezwłocznie skontaktować się z ASI. Zakazane jest kontynuowanie pracy na wadliwym sprzęcie.
10. Do komunikacji zdalnej (z innymi pracownikami, interesantami itd.) można wykorzystywać wyłącznie systemy urzędu.

§ 8. Praca z wykorzystaniem sieci Internet

1. W miarę potrzeby pracodawca zapewnia pracownikowi odpowiednie urządzenia modemowe, gwarantujące mu bezpieczny dostęp do sieci Internet.
2. Zabronione jest korzystanie z sieci Internet z wykorzystaniem łącza służbowego na urządzeniach, na których wykonywana jest praca zdalna, do innych celów niż służbowe.
3. Dopuszcza się korzystanie z sieci Internet z wykorzystaniem łącza prywatnego do pracy zdalnej, ale po odpowiednim ustawieniu routera, w szczególności zmianie ustawień domyślnych.
4. W sytuacji wykorzystania prywatnej sieci Internet do pracy zdalnej, pracownik zobowiązany jest do nieudostępniania własnej sieci Internetu np. z telefonu innym użytkownikom.
5. Pracownik zobowiązany jest nie korzystać z ogólnodostępnych sieci Internet.
6. Pracodawca zapewnia zdalne wsparcia informatyczne dla pracowników świadczących pracę zdalną.

§ 9. Zgłaszanie incydentów

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. O tym, że doszło do naruszenia ochrony danych osobowych, mogą świadczyć w szczególności:
 - a) kradzież lub zgubienie dokumentów zawierających dane osobowe;
 - b) kradzież lub zgubienie nośników zawierających dane osobowe (np. komputera służbowego);
 - c) nieuprawniona modyfikacja lub kopiowanie danych osobowych;
 - d) nieuprawnione niszczenie dokumentów lub usuwanie rekordów w systemie informatycznym w zakresie, w jakim zawierają dane osobowe;
 - e) nieuprawniony dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe, w szczególności atak hakerski;
 - f) utrata dostępu do danych osobowych, trwała lub czasowa, np. z powodu awarii serwera, awarii połączeń telefonicznych;
 - g) nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe, wgląd przez osobę nieuprawnioną w treść informacji (zawierającej dane osobowe) wyświetlanej na ekranie komputera lub zawartą w dokumencie papierowym;
 - h) przekazanie danych osobowych osobom nieuprawnionym (np. wysłanie przesyłki lub wiadomości e-mail na zły adres);
 - i) działanie wirusa komputerowego mającego wpływ na dane osobowe;
 - j) pozostawienie danych osobowych w ogólnodostępnym miejscu;
 - k) utrata klucza deszyfrującego lub danych do logowania do systemu, w którym są przetwarzane dane osobowe;
 - l) podszycie się pod cudze dane osobowe i np. wysłanie e-maila z podaniem się za inną osobę;
 - m) wydanie dokumentacji innej osobie niż uprawniona;
 - n) zdarzenie losowe, np. pożar w pomieszczeniu, w którym są przetwarzane dane osobowe, zalanie.
3. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych każdy pracownik ma obowiązek zgłosić natychmiast ten fakt w jeden z niżej wskazanych sposobów:
 - a) przez wykonanie połączenia telefonicznego pod numerem telefonu: 24 235 91 50 lub
 - b) za pośrednictwem e-maila przesłanego na adres: urząd@drobin.pl.
4. Pracownik jest zobowiązany powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia oraz podjąć działania stosownie do zaistniałej sytuacji lub udzielonych instrukcji, niezbędne do zapobieżenia dalszym zagrożeniom dla danych.
5. Zgłoszenie jest dokumentowane i procedowane zgodnie z przyjętą w urzędzie Procedurą zarządzania

naruszeniami ochrony danych osobowych.

§ 10. Monitorowanie korzystania ze sprzętu

1. Pracodawca ma prawo monitorować sposób korzystania przez pracowników ze sprzętu służbowego, z zastrzeżeniem poszanowania dóbr osobistych pracownika i przepisów o ochronie danych osobowych, w tym zawartych w Kodeksie pracy oraz innych powszechnie obowiązujących przepisach prawa.
2. Decyzję w zakresie wprowadzenia monitorowania podejmuje Burmistrz Miasta i Gminy Drobin po konsultacji z inspektorem ochrony danych oraz ASI i weryfikacji spełnienia kryteriów wskazanych w ust. 1 powyżej.
3. Monitoring korzystania ze sprzętu służbowego może być prowadzony, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.
4. Pracownik jest informowany o celach, zakresie oraz sposobie zastosowania monitoringu korzystania ze sprzętu służbowego przed dopuszczeniem go do pracy (jeżeli taki monitoring jest stosowany).
5. Należy weryfikować, czy zakres rejestracji aktywności pracownika (np. informacje z logów) nie prowadzi do przetwarzania danych szczególnych kategorii (np. poprzez ujawnienie informacji związanej z przeglądanyymi stronami www).

§ 11. Kontrola pracy zdalnej

1. Kontrola wykonywania pracy zdalnej w zakresie bezpieczeństwa i higieny pracy lub kontrola przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, odbywa się na zasadach ustalonych z pracownikiem.
2. Pracodawca ma prawo przeprowadzać kontrolę wykonywania pracy zdalnej przez pracownika, kontrolę w zakresie bezpieczeństwa i higieny pracy lub kontrolę przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, na zasadach określonych w niniejszym dokumencie.
3. Kontrolę przeprowadza się w porozumieniu z pracownikiem w miejscu wykonywania pracy zdalnej w godzinach pracy pracownika.
4. Pracodawca dostosowuje sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju.
5. Kontrola wykonywania pracy zdalnej może być przeprowadzona z wykorzystaniem środków komunikacji elektronicznej lub w miejscu wykonywania pracy zdalnej.
6. Pracownik, którego wykonywanie pracy zdalnej jest kontrolowane, zobowiązany jest do współpracy z personelem wykonującym czynności kontrolne.
7. Czynności kontrolne mogą być wykonywane tylko i wyłącznie przez upoważniony do tego personel.

8. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.
9. Kontrole wykonywanej pracy zdalnej prowadzone są według harmonogramu kontroli, jeśli został taki opracowany przez pracodawcę, bądź w sytuacji podjęcia takiej decyzji przez pracodawcę.
10. Jeżeli pracodawca w trakcie kontroli pracy zdalnej stwierdzi uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy lub w przestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych:
 - a) zobowiązuje pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie, albo
 - b) cofa zgodę na wykonywanie pracy zdalnej przez tego pracownika. W przypadku wycofania zgody na wykonywanie pracy zdalnej pracownik rozpoczyna pracę w dotychczasowym miejscu pracy w terminie określonym przez pracodawcę.

§ 12. Bezpieczeństwo stanowiska pracy

1. Pracownik powinien przestrzegać następujących zasad przy wykonywaniu pracy zdalnej:
 - a) przechowywania nośników zawierających dane osobowe w szafkach/pomieszczeniach zamykanych na klucz, uniemożliwiających dostęp do nich przez osoby postronne (zasada chronionego pomieszczenia);
 - b) 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);
 - c) blokowania komputera przed każdorazowym opuszczeniem stanowiska do wykonywania pracy zdalnej oraz poprawnego wyłączenia sprzętu po zakończeniu pracy (zasada czystego ekranu);
 - d) zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (zasada czystej drukarki);
 - e) trwałego niszczenia nieprzydatnych dokumentów, brudnopisów oraz zbędnych kopii, tj.: w sposób uniemożliwiający odtworzenie zawartych w nich informacji (zasada czystego kosza). Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD oraz innych nośników – powinny one zostać wcześniej zniszczone fizycznie;
 - f) niezamieszczania na tablicach (jeżeli takie są używane) informacji podlegających ochronie w sposób umożliwiający zapoznanie się z nimi osobom nieuprawnionym (zasada czystej tablicy);
 - g) nie prowadzenia rozmów poufnych w obecności osób trzecich, w tym również domowników oraz w miejscu ogólnodostępnym np. balkon, podwórko, winda, w kolejce w sklepie;
 - h) prowadzenia wymiany informacji z zachowaniem zasad bezpieczeństwa danych, w szczególności zobowiązany jest do stosowania szyfrowania wiadomości, załączników do

wiadomości, zabezpieczając je hasłem, które przekazywane powinno być bezpośrednio innym odrębnym kanałem przepływu do odbiorcy wiadomości.

2. Pracownik powinien korzystać z dokumentów papierowych zawierających dane osobowe podczas pracy zdalnej jedynie wyjątkowo, tj.: gdy:
 - a) nie jest możliwe wykonanie obowiązków wskazanych w ust. 1 powyżej w inny sposób, np. poprzez bezpieczny dostęp do dokumentów zawierających dane osobowe w formie elektronicznej;
 - b) nie jest możliwe skorzystanie z dokumentów zanonimizowanych (tak, by nie było możliwe ustalenie, jakiej osoby fizycznej dotyczy dany dokument).
3. W celu zminimalizowania ryzyka naruszenia integralności danych oraz utraty ich dostępności, jeżeli tylko pozwala to na zrealizowanie celu wskazanego w ust. 2 powyżej, pracownik podczas pracy zdalnej powinien pracować na kopiach dokumentów papierowych zawierających dane osobowe. Powyższe nie oznacza, że pracownikowi wolno samowolnie wchodzić w posiadanie kopii dokumentów zawierających dane osobowe, np. poprzez ich drukowanie, w szczególności zakazane jest samowolne drukowanie dokumentów zawierających dane osobowe w warunkach domowych. Pracownik musi chronić dane zawarte w kopiach dokumentach tak samo jak w dokumentacji oryginalnej.
4. Po zakończeniu wykonywania pracy zdalnej pracownicy są zobowiązani do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do warunków technicznych i lokalowych, polegających na:
 - a) zabezpieczeniu dokumentacji i pieczętek służbowych;
 - b) zabezpieczeniu komputerów i nośników informacji;
 - c) zamknięciu okien i drzwi na klucz.

§ 13. Zakończenie pracy zdalnej

1. W przypadku zakończenia pracy zdalnej osoba prowadząca sprawy kadrowe przekazuje tę informację do ASI.
2. ASI odbiera pracownikowi dostęp do wydanych urządzeń, zgodnie z postanowieniami § 4 powyżej.
3. Zakończenie pracy zdalnej oznacza m.in. obowiązek zakończenia prowadzenia działań kontrolnych względem pracownika pracującego zdalnie.
4. W sprawach nieuregulowanych zastosowanie mają odpowiednio przepisy wewnątrzzakładowe określające w szczególności zasady ochrony danych osobowych.

Burmistrz Miasta i Gminy Drobín

Grzegorz Szykowski

Załącznik Nr 1

do Procedury bezpieczeństwa informacji
i ochrony danych osobowych podczas pracy zdalnej

.....
imię i nazwisko pracownika

.....
miejscowość, data

**OŚWIADCZENIE O ZAPOZNANIU
Z PROCEDURAMI BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH
OSOBOWYCH
PODCZAS PRACY ZDALNEJ/ZACHOWANIE W TAJEMNICY**

(WZÓR)

Ja niżej podpisany/a, w związku z wykonywaniem przeze mnie pracy zdalnej zostałem/zostałam przeszkolony/a w dziedzinie ochrony i przetwarzania danych osobowych w zakresie niezbędnym do realizacji moich obowiązków w sposób zdalny, a także zapoznałem/am się ze odpowiednimi przepisami i przyjętymi w Jednostce procedurami dotyczącymi ochrony danych osobowych przetwarzanych w sposób zdalny, w tym Procedurą bezpieczeństwa informacji i ochrony danych osobowych podczas pracy zdalnej i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do bezterminowego zachowania w tajemnicy danych osobowych, a także sposobów ich zabezpieczenia, do których uzyskałem/am dostęp w związku z wykonywaniem pracy zdalnej.

.....
podpis pracownika

Załącznik Nr 2

do Procedury bezpieczeństwa informacji
i ochrony danych osobowych podczas pracy zdalnej

KLAUZULA INFORMACYJNYA

1. Administrator

Administratorem Państwa danych osobowych jest Urząd Miasta i Gminy Drobin, ul. Marszałka Piłsudskiego 12, 09-210 Drobin, adres e-mail: urząd@drobin.pl, nr tel. 24 235 91 68.

2. Inspektor Ochrony Danych

Kontakt z wyznaczonym Inspektorem Ochrony Danych w sprawach dotyczących przetwarzania Państwa danych osobowych oraz realizacji przysługujących Państwu praw związanych z ich przetwarzaniem możliwy jest pod adresem e-mail: iod@data-partners.pl.

3. Cel i podstawa prawna przetwarzania

Cel	Podstawa prawna
Ukształtowanie i realizacja pracy zdalnej na zasadach określonych w przepisach prawa.	<i>Ad 1.</i> Art. 6 ust. 1 lit. b RODO (wykonanie umowy, podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy). <i>Ad 2.</i> 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.
Obowiązek pracodawcy uwzględnienia wniosku pracownika o wykonywanie pracy zdalnej	Art. 6 ust. 1 lit. c RODO w zw. z KP, art. 9 ust. 2 lit. b RODO w zw. z KP (realizacja obowiązku ciążącego na administratorze).
Realizacja obowiązku pracodawcy rozpatrzenia wniosku pracownika o zaprzestanie wykonywania pracy zdalnej i przywrócenie poprzednich warunków wykonywania pracy.	Art. 6 ust. 1 lit. c RODO w zw. z KP, art. 9 ust. 2 lit. b RODO w zw. z art. KP (realizacja obowiązku ciążącego na administratorze).
Realizacja obowiązków pracodawcy związanych z organizacją pracy zdalnej.	Art. 6 ust. 1 lit. c RODO w zw. z KP (realizacja obowiązku ciążącego na administratorze).
Przeprowadzenie kontroli pracy zdalnej.	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora).
Obowiązek reakcji w przypadku zidentyfikowanych nieprawidłowości w toku kontroli.	Art. 6 ust. 1 lit. c RODO w zw. z art. KP (realizacja obowiązku ciążącego na administratorze).

Obsługa wypadku przy pracy zdalnej stosownie do wymogów szczególnych zawartych w art. 67 ³¹ § 9 KP.	Art. 6 ust. 1 lit. c RODO w zw. z art. 67 ³¹ § 9 KP (realizacja obowiązku ciążącego na administratorze).
Zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy (monitoring).	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes 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 ciążącego na administratorze).

4. Odbiorcy danych osobowych

Odbiorcami Państwa danych osobowych mogą być podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa, a także podmioty, które przetwarzają Państwa dane osobowe na podstawie zawartych umów powierzenia przetwarzania danych osobowych z Administratorem.

5. Okres przechowywania danych

Dane osobowe zostaną usunięte po upływie okresów ich przechowywania przewidzianych przepisami prawa, np. w przypadku umowy o pracę, której częścią są uzgodnienia 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 ewentualnych roszczeń związanych z zawarciem lub realizacją umowy, w tym zobowiązań publicznoprawnych, lub krócej, jeżeli zgłosicie Państwo skuteczny sprzeciw.

6. Prawa osób, których dane dotyczą

Posiadają Państwo prawo do żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, a także prawo wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie, ul. Stawki 2, 00-193 Warszawa.

7. Wymóg podania danych

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).

Jeżeli administrator będzie pytał o zgodę na przetwarzanie danych osobowych, to podanie danych i wyrażenie zgody będzie dobrowolne i nie wpływa na realizację pracy zdalnej.

8. Transfer danych

Nie dochodzi do transferu danych w przypadku korzystania z udostępnionych narzędzi do pracy zdalnej.