

**Procedura ochrony danych osobowych w ramach wykonywania pracy zdalnej
w Uniwersytecie Warmińsko-Mazurskim w Olsztynie**

§ 1 Postanowienia ogólne

1. Niniejsza Procedura określa zasady ochrony danych osobowych oraz bezpieczeństwa informacji w ramach wykonywania pracy zdalnej.
2. Inspektor Ochrony Danych przeprowadza, w miarę potrzeb – na podstawie zgłoszonego wcześniej przez kierowników jednostek organizacyjnych zapotrzebowania, instruktaż i szkolenie w zakresie ochrony danych osobowych dla pracowników wykonujących pracę zdalną.
3. Pracownik podczas pracy zdalnej może przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik jest zobowiązany niezwłocznie poinformować swojego bezpośredniego przełożonego w sytuacji, gdy warunki pracy zdalnej mogą naruszać wymogi zawarte w niniejszej Procedurze.
5. Praca zdalna może być wykonywana przez pracownika posiadającego dostęp do służbowego przenośnego sprzętu komputerowego wyposażonego w adekwatne narzędzia umożliwiające zabezpieczenie danych osobowych/danych poufnych pracodawcy oraz możliwie najnowsze (skuteczne) oprogramowanie chroniące przed cyberatakiem.
6. Praca zdalna wykonywana przez pracownika administracyjnego powinna być świadczona w godzinach pracy Centrum Informatycznego, co zapewni mu pomoc techniczną – niezwłoczną reakcję np. na utratę dostępu do wirtualnej skrzynki uniwersyteckiej pracownika.

§ 2 Rozpoczęcie pracy zdalnej

1. Pracę zdalną może wykonywać wyłącznie pracownik, który odbył szkolenie z zakresu ochrony danych osobowych, uzyskał upoważnienie do ich przetwarzania oraz złożył oświadczenie o zachowaniu w tajemnicy danych osobowych i informacji oraz sposobów ich zabezpieczenia, zgodnie z regulacjami zawartymi w Polityce Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, stanowiącej załącznik do Zarządzenia Nr 36/2018 Rektora Uniwersytetu Warmińsko-Mazurskiego w Olsztynie z dnia 28 maja 2018 roku w sprawie Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie (z późn. zm.).
2. Przed przystąpieniem do wykonywania pracy zdalnej pracownik jest zobowiązany do zapoznania się z niniejszą Procedurą, co potwierdza składając stosowne oświadczenie.
3. Oświadczenie, o którym mowa w ust. 2, jest przechowywane w aktach osobowych pracownika, przez okres prowadzenia jego akt przewidziany przepisami prawa pracy.
4. Bezpośredni przełożony prowadzi ewidencję pracowników wykonujących pracę zdalną.

§ 3 Bezpieczeństwo pracy zdalnej

1. Pracownik jest zobowiązany do zabezpieczenia sprzętu służbowego wykorzystywanego w świadczonej pracy zdalnej oraz informacji, w tym danych osobowych zawartych w jego pamięci, systemach informatycznych, jak i na nośnikach zewnętrznych, w szczególności poprzez:
 - 1) niepozostawianie sprzętu służbowego bez nadzoru;
 - 2) niezapisywanie loginu i hasła logowania do systemów teleinformatycznych (dotyczy to zarówno zapisywania fizycznego - np. na kartkach, zapisywania w pamięci przeglądarki) oraz nieudostępnianie ich osobom trzecim;

- 3) regularną aktualizację oprogramowania na udostępnionych urządzeniach elektronicznych a także systematyczne skanowanie urządzeń służbowych programem antywirusowym;
- 4) wykorzystywanie w pracy zabezpieczonej, domowej sieci WiFi (urządzenie sieciowe powinno posiadać aktualne oprogramowanie);
- 5) niekorzystanie w trakcie pracy zdalnej z publicznych sieci bezprzewodowych;
- 6) nieudostępnianie osobom trzecim przekazanego przez Uniwersytet sprzętu służbowego oraz wykorzystywanie go wyłącznie do celów służbowych;
- 7) zabezpieczenie przekazanego sprzętu hasłem, a w przypadku laptopów służbowych, także szyfrowanie dysku;
- 8) łączenie się z uniwersyteckimi systemami informatycznymi oraz dyskami sieciowymi, wyłącznie za pośrednictwem sprzętu służbowego i korzystanie z bezpiecznego połączenia za pomocą sieci VPN;
- 9) każdorazowe upewnienie się, podczas wysyłania wiadomości e-mail, co do poprawności wpisywanych adresów mailowych, a w przypadku przesyłania załączników zawierających dane osobowe lub inne informacje istotne dla funkcjonowania Uniwersytetu, zabezpieczenie ich hasłem.
2. Pracownik jest zobowiązany właściwie eksploatować powierzony mu sprzęt oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
3. Niedozwolone jest gromadzenie, instalowanie i użytkowanie oprogramowania, plików oraz innych informacji pochodzących z nielegalnego lub niewiadomego źródła, jak również niezwiązanych z wykonywaniem obowiązków służbowych pracownika.
4. Pracownik korzystający ze sprzętu służbowego nie może samodzielnie – bez konsultacji z Centrum Informatycznym - przekazać go do serwisu zewnętrznego.

§ 4 Incydenty

1. Naruszenie ochrony danych osobowych jest to zdarzenie prowadzące do:
 - 1) przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych;
 - 2) nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych.
2. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, każdy pracownik ma obowiązek niezwłocznie zgłosić ten fakt swojemu bezpośredniemu przełożonemu oraz poinformować Inspektora Ochrony Danych Osobowych i Centrum Informatyczne.
3. 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 osobowych lub bezpieczeństwa informacji.

§ 5 Monitoring korzystania ze sprzętu służbowego

1. Uniwersytet ma prawo monitorować sposób korzystania przez pracownika ze sprzętu służbowego, z zastrzeżeniem poszanowania jego dóbr osobistych i przepisów o ochronie danych osobowych, w tym zawartych w Kodeksie pracy oraz innych powszechnie obowiązujących przepisach prawa.
2. 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.

3. Pracownik jest informowany o celach, zakresie oraz sposobie zastosowania monitoringu korzystania ze sprzętu służbowego przed dopuszczeniem go do pracy (jeżeli taki monitoring może być/będzie stosowany).

§ 6 Bezpieczeństwo stanowiska pracy

1. Pracownik powinien przestrzegać następujących zasad przy wykonywaniu pracy zdalnej:
 - 1) przechowywania nośników zawierających dane osobowe w szafkach/pomieszczeniach zamykanych na klucz, uniemożliwiających dostęp do nich przez osoby postronne, m. in. członków rodziny;
 - 2) niepozostawiania nośników zawierających dane osobowe (sprzętu, jak i nośników papierowych) bez nadzoru – zarówno w trakcie wykonywania pracy zdalnej, jak i po jej zakończeniu;
 - 3) blokowania komputera przed każdorazowym opuszczeniem stanowiska do wykonywania pracy zdalnej oraz poprawnego wyłączenia i zabezpieczenia sprzętu po zakończeniu pracy;
 - 4) zabierania dokumentów z drukarek zaraz po ich wydrukowaniu;
 - 5) trwałego niszczenia nieprzydatnych dokumentów, brudnopisów oraz zbędnych kopii, tj. w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych. Dotyczy to również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Jeżeli pracownik nie posiada w domu niszczarki, powinien dokumenty oraz inne nośniki danych np. płyty CD/DVD przechowywać w bezpieczny sposób – uniemożliwiający dostęp do nich przez osoby postronne, a po zakończeniu pracy zdalnej zniszczyć je w Uniwersytecie;
2. Pracownik powinien korzystać z dokumentów papierowych zawierających dane osobowe podczas pracy zdalnej jedynie wyjątkowo, tj. gdy:
 - 1) nie jest możliwe wykonywanie obowiązków wskazanych w inny sposób, np. poprzez bezpieczny dostęp do dokumentów zawierających dane osobowe w formie elektronicznej;
 - 2) nie jest możliwe skorzystanie z dokumentów zanonimizowanych.
3. W celu zminimalizowania ryzyka naruszenia integralności danych oraz utraty ich dostępności, pracownik podczas pracy zdalnej powinien pracować na kopiach dokumentów papierowych zawierających dane osobowe. Powyższe nie oznacza, że pracownikowi wolno samowolnie wchodzić w posiadanie ww. kopii, 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. Pracownik na wyraźne polecenie bezpośredniego przełożonego wykonuje kopie dokumentów niezbędnych do wykonywania czynności służbowych. Po wykonaniu kopii dokumentów pracownik przygotowuje zestawienie określające jakie dokumenty, w jakiej liczbie zostały skopiowane, następnie przekazuje je bezpośredniemu przełożonemu.
5. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce w taki sposób, aby były niewidoczne dla osób trzecich.
6. Po zakończeniu wykonywania pracy zdalnej pracownik jest zobowiązany do uporządkowania swojego stanowiska pracy oraz wykonania czynności zabezpieczających, adekwatnych do warunków technicznych i lokalowych, polegających na:
 - 1) zabezpieczeniu dokumentacji i pieczętek służbowych;
 - 2) zabezpieczeniu komputerów i nośników informacji;
 - 3) zamknięciu okien i drzwi na klucz.

