

## **ZASADY OCHRONY DANYCH, W TYM DANYCH OSOBOWYCH, W PRACY ZDALNEJ**

### **I. OBOWIĄZKI DOTYCZĄCE UŻYTKOWANIA SPRZĘTU, NARZĘDZI PRACY, SIECI I SYSTEMÓW INFORMATYCZNYCH ZGODNIE Z WYMOGAMI W ZAKRESIE BEZPIECZEŃSTWA I OCHRONY INFORMACJI**

1. Pracownik jest zobowiązany do:
  - a. adekwatnego zabezpieczenia i ochrony przed uszkodzeniem, kradzieżą, zniszczeniem lub nieuprawnionym użyciem/dostępem powierzonego sprzętu i dokumentów;
  - b. wykorzystywania powierzonego sprzętu, oprogramowania i środków łączności wyłącznie do celów służbowych;
  - c. zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi;
  - d. niekorzystania ze sprzętu służbowego w miejscach publicznych;
  - e. zachowania zasad BHP.
  
2. Praca zdalna z danymi w obiegu elektronicznym odbywa się zgodnie z poniższymi zasadami:
  - a. do pracy możliwe jest wykorzystanie sprzętu służbowego będącego własnością Urzędu, który został zatwierdzony do użytku poza siedzibą Urzędu przez Dyrektora Generalnego;
  - b. zabronione jest używanie prywatnego sprzętu, jeśli nie umożliwia to poszanowania i ochrony informacji poufnych, innych tajemnic prawnie chronionych, danych osobowych oraz informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
  - c. zabronione jest używanie prywatnych kont pocztowych do przetwarzania informacji;
  - d. instalowanie jakiegokolwiek oprogramowania lub aplikacji na laptopie, telefonie służbowym jest możliwe tylko przez pracowników Oddziału Informatyki;
  - e. pracownik nie może przechowywać żadnych informacji na innych nośnikach niż udostępnione mu przez pracodawcę;
  - f. sprzęt służbowy chroniony jest hasłem, a laptopy muszą być szyfrowane;
  - g. połączanie się z zasobami sieciowymi Urzędu możliwe jest wyłącznie za pomocą sieci VPN;
  - h. hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową;
  - i. przy wysyłaniu wiadomości e-mail pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów jej adresatów;

- j. w przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z Oddziałem Informatyk;
  - k. w przypadku awarii lub uszkodzenia powierzonego sprzętu, należy niezwłocznie przekazać go Oddziału Informatyki.
3. Praca zdalna z dokumentami papierowymi odbywa się zgodnie z poniższymi zasadami:
- a. wnoszenie dokumentacji papierowej z siedziby Urzędu jest zabronione;
  - b. w przypadku konieczności korzystania z dokumentacji których oryginalna wersja jest papierowa, należy dokonać odwzorowania cyfrowego z zachowaniem zasady, o której mowa w pkt. 2 lit. e.
  - c. pliki elektroniczne będące cyfrowym odwzorowaniem dokumentacji papierowej (skan, zdjęcie) można sporządzać i przechowywać wyłącznie za pośrednictwem i z pomocą sprzętu i systemów będących własnością pracodawcy.

## **II. ZASADY OCHRONY DANYCH OSOBOWYCH**

1. Pracodawca przeprowadza, w miarę potrzeb, instruktaż i szkolenie w zakresie ochrony danych osobowych dla pracowników wykonujących pracę zdalną.
2. Do przetwarzania danych osobowych dopuszczeni mogą być jedynie pracownicy poddający stosowane upoważnienie, którzy odbyli szkolenie z zasad przetwarzania i ochrony danych osobowych w warunkach pracy zdalnej oraz złożyli oświadczenie o zachowaniu w poufności danych osobowych oraz środków ich ochrony.
3. Pracownicy mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność, w tym zapewnić dedykowane pomieszczenie do wykonywania pracy zdalnej, do którego dostęp osób trzecich jest ograniczony.
5. Pracownik zobowiązany jest zapewnić bezpieczne połączenie z siecią Internet w przypadku, gdy nie wykorzystuje środków łączności dostarczonych przez Urząd.
6. Pracownik zobowiązany jest natychmiastowo powiadomić inspektora ochrony danych oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z naruszeniem bezpieczeństwa danych.
7. Nieprzestrzeganie zasad ochrony danych może być kwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

## **III. WYMOGI W ZAKRESIE KOMUNIKACJI**

1. Komunikacja odbywa się:
  - a) telefonicznie, pracownik ma obowiązek przekierować połączenia przychodzące na służbowy numer telefonu, na numer telefonu użytkowany w miejscu świadczenia pracy zdalnej,
  - b) za pośrednictwem systemu pracy grupowej Zimbra (służbowej poczty elektronicznej, komunikatora, kalendarza),
  - c) zapewnionej przez pracodawcę platformy wideokonferencji Zoom,
  - d) dekretacji w systemie EZD PUW