PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Wszelkie informacje (zarówno w formie papierowej, jak i elektronicznej) pozwalające na identyfikację konkretnej osoby stanowią dane osobowe podlegające ochronie.
2. Każdy pracownik może mieć dostęp do danych osobowych wyłącznie w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.
3. Każdy pracownik posiadający dostęp do danych osobowych jest zobowiązany do dołożenia szczególnej staranności do zabezpieczenia danych osobowych przed ich zniszczeniem lub udostępnieniem osobom nieuprawnionym.
4. Każdy pracownik, który w ramach swoich obowiązków służbowych posługuje się dokumentami zawierającymi dane osobowe musi przechowywać je w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym – musi stosować tzw. „Politykę czystego biurka", która polega na zabezpieczaniu dokumentów oraz nośników np. w zamykanych szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas nieobecności osób upoważnionych w trakcie godzin pracy.
5. Upoważnieni pracownicy zobowiązani są do bezpiecznego niszczenia dokumentów i wydruków (po upływie ich przydatności) przy użyciu niszczarek.
6. W przypadku, gdy pracownik przetwarzający dane osobowe korzysta ze sprzętu IT (komputery, monitory, drukarki, skanery, kserokopiarki, służbowe tablety i smartfony) zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem.
7. Każdy pracownik posiadający dostęp do danych osobowych w formie elektronicznej musi posiadać swój własny login oraz hasło, składające się z co najmniej 8 znaków, których nie może ujawnić.
8. W celu zminimalizowania ryzyka zainstalowania złośliwego oprogramowania, pracownik nie może na stanowisku komputerowym instalować oprogramowania bez zgody przełożonego.
9. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
10. Pracownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorze lub wyświetlaczu urządzenia mobilnego.
11. Pracownik zobowiązany jest do korzystania z Internetu Administratora wyłącznie w celach służbowych.
12. Pracownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
13. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
14. Pracownik jest zobowiązany do usuwania plików z nośników oraz dysków/folderów, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików.
15. Przed czasowym opuszczeniem stanowiska pracy, pracownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (**+ L**) lub wylogować się z systemu bądź z programu.
16. Po zakończeniu pracy, pracownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy i zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki, na których znajdują się dane osobowe.
17. Dokumentów lub nośników zawierających dane osobowe nie wolno wynosić poza teren siedziby Administratora z kopiować bez zgody przełożonego.
18. Naruszenie procedur zabezpieczenia danych osobowych może skutkować odpowiedzialnością karną, a także nałożeniem na Administratora wysokich kar pieniężnych, co dla pracownika może skutkować odpowiedzialnością dyscyplinarną.
19. Każdy **pracownik jest zobowiązany do zgłaszania naruszeń ochrony danych niezwłocznie** do swojego bezpośredniego przełożonego lub **Inspektora Ochrony Danych** Pana **Łukasza Więckowskiego** – tel. **534-971-975, e-mail: odo@cuw.dg.pl**
20. Naruszeniem ochrony danych może być np. zabranie, zgubienie, zniszczenie, kradzież dokumentu zawierającego dane osobowe, a także wykrycie na komputerze złośliwego oprogramowania (np. wirus, trojan, ransomware), uszkodzenie komputera (lub innego urządzenia służącego do pracy na danych osobowych), podobnie jak zgubienie urządzenia, na którym przetwarzane są dane osobowe (np. służbowego smartfona, laptopa, pendrive).
21. Każde naruszenie ochrony danych musi być odnotowane w wewnętrznej dokumentacji Administratora, a część z nich, dla których prawdopodobne jest naruszenie praw i wolności osób fizycznych musi być zgłoszona do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki 2).
22. Obowiązek niezwłocznego powiadamiania o fakcie naruszenia ochrony danych jest związany z obowiązkiem powiadamiania przez administratora danych Prezesa Urzędu Ochrony Danych Osobowych w ciągu maksymalnie 72 godzin po stwierdzeniu naruszenia. Niedopełnienie tego obowiązku może skutkować nałożeniem na Administratora wysokich kar pieniężnych.
23. Przestrzeganie zasad ochrony danych podlega cyklicznym sprawdzeniom. Każdy pracownik ma obowiązek umożliwić osobie sprawdzającej wyznaczonej przez administratora danych dokonanie niezbędnej weryfikacji.
24. Lekceważenie wyżej przywołanych zasad, zwłaszcza w zakresie zgłaszania potencjalnych naruszeń ochrony danych, współpracy przy sprawdzeniach przestrzegania procedur lub odpowiedniego zabezpieczania danych osobowych na swoim stanowisku pracy będzie postrzegane jako przewinienie dyscyplinarne.