

INFORMATOR DLA OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

Pracownika / Użytkownika:

- opróżniaj regularnie folder „Kosz” w komputerze,
- nie przetrzymuj na pulpicie pojedynczych plików oraz folderów,
- nie przekazuj swojego loginu oraz hasła współpracownikom i innym osobom postronnym,
- zmieniaj hasło regularnie,
- w pracy używaj tylko służbowych nośników danych zabezpieczonych hasłem,
- nie używaj obcych nośników danych,
- dokumenty papierowe niszczone zawsze w niszczarkach,
- elektroniczne nośniki danych oddaj informatykowi do zniszczenia,
- regularnie twórz kopię zapasową swoich zasobów dyskowych,
- nie używaj nielegalnych publikacji, zdjęć oraz programów,
- nośniki danych sprawdzaj zawsze systemem antywirusowym,
- zbierając dane od klientów Jednostki, spełnij wobec nich „obowiązek informacyjny”,
- zbieraj tylko tyle danych, ile wymaga realizacja usługi, o którą wystąpił klient Jednostki, oraz ile dopuszcza prawo,
- gdy udostępniasz dane osobowe lub informacje, upewnij się, że przekazujesz je tylko ich właścicielom lub podmiotom upoważnionym na podstawie przepisów prawa,
- gdy udzielasz informacji telefonicznej, zweryfikuj tożsamość osoby, w celu sprawdzenia czy ma ona prawo do uzyskania tych informacji,
- gdy wysyłasz wiadomość e-mail z załącznikiem zawierającym dane osobowe klienta Jednostki, zahasłuj ten załącznik,
- gdy korzystasz z listy mailingowej, wysyłaj informacje do klientów Jednostki, używając pola „kopia ukryta” w wiadomości e-mail,
- gdy udostępniasz informację publiczną, trwale zanonimizuj informacje o kliencie Jednostki, aby nie naruszyć jego praw i wolności i żeby wnioskodawca nie mógł go zidentyfikować,
- jeżeli klientawnioskuje o realizację swoich praw wynikających z RODO, poinformuj o tym przypadku IOD,
- wykorzystuj służbową pocztę e-mail tylko do celów służbowych,
- nie otwieraj załączników z niewiadomego źródła,
- nie wykorzystuj opcji „autouzupelnianie” w wypełnianych formularzach,
- nie zapamiętuj swoich haseł w przeglądarkach,
- przy pracy na urządzeniu przenośnym upewnij się, że jest ono zabezpieczone przed dostępem osób trzecich,
- nie podłączaj służbowych urządzeń przenośnych do obcych sieci wi-fi,
- nie pozostawiaj w pomieszczeniach biurowych Jednostki osób postronnych bez asysty,
- gdy opuszczasz stanowisko pracy, zawsze blokuj stację roboczą,
- kończ pracę w systemach, zawsze wylogowując się z nich poprawnie,
- nie pozostawiaj niezamkniętych pomieszczeń biurowych oraz nie zostawiaj w drzwiach tych pomieszczeń kluczy,
- gdy kończysz pracę, zabezpiecz przed dostępem osób nieupoważnionych dokumenty papierowe oraz elektroniczne nośniki danych, a także wszystkie szafy, w których przechowywane są dokumenty,
- po zakończeniu pracy zabezpiecz wszystkie pomieszczenia, w których pracujesz,
- zadbaj o stosowne uprawnienia, gdy pozostajesz w pomieszczeniu biurowym po godzinach pracy,
- jeśli udostępniasz informacje dotyczące bezpieczeństwa informacji, skontaktuj się z IOD,
- jeśli przekazujesz dane osobowe podmiotom zewnętrznym, skonsultuj z IOD zasadność zawarcia umowy powierzenia,
- zgłoś do kierownika Jednostki i IOD potrzebę gromadzenia nowych danych osobowych lub aktualizację danych dotychczasowych,
- zgłaszaj wszystkie incydenty bezpieczeństwa lub ochrony danych do przełożonego, ASI oraz IOD,
- dbaj o otrzymany od pracodawcy sprzęt służbowy,
- zgłaszaj wszystkie awarie sprzętu do obsługi informatycznej.