

Regulamin Ochrony Danych Osobowych

1. Regulamin przetwarzania danych osobowych przez Zakład Usług Technicznych Piotr Sparczyński, os. Stare Sady 6/25, 98-300 Wieluń jest dostępny w wersji papierowej w siedzibie firmy i na stronie internetowej pod adresem <http://zut.aspercz.pl> w dziale Dokumenty.
2. ADO jest to Administrator Danych Osobowych - Zakład Usług Technicznych Piotr Sparczyński, os. Stare Sady 6/25, 98-300 Wieluń, Nip 8322066517, Regon 365241376.
3. IODO jest to Inspektor Ochrony Danych Osobowych – Andrzej Sparczyński, który odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym zakładu, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
4. ADO i IODO prowadzi rejestr przekazywania i udostępniania danych osobowych firmom upoważnionym do tego. Takie przetwarzanie danych jest dopuszczalne, jeżeli odbywa się w prawnie usprawiedliwionych celach oraz nie narusza praw i wolności osób, których dane dotyczą:
 1. ADO zbiera dane osobowe klientów w celu wystawiania faktur, rachunków dla klientów i dostawców oraz sprawozdawczości finansowej.
 2. ADO zbiera dane osobowe pracowników w zakresie list płac, zawartości teczek osobowych pracowników, kartotek i wszelkich wykazów pracowników.
 3. ADO zbiera dane od osób świadczących usługi na podstawie umów cywilnoprawnych, w zakresie jaki jest konieczny dla zawarcia i realizacji umowy.
5. Osoby lub firmy muszą wyrazić zgodę na wykorzystanie ich danych w celach marketingowych lub reklamowych.
6. Każdy, kogo dane osobowe zostały wprowadzone do Zbioru Danych Osobowych ma prawo dostępu do ich treści oraz ich poprawienia i aktualizacji. Zgoda ta może być anulowana.
7. ADO stosuje środki techniczne i organizacyjne zapewniające odpowiednią do zagrożeń i kategorii ochronę danych. Dotyczy to sposobu zabezpieczenia danych przed ich udostępnieniem, utratą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.
8. Dane muszą być technicznie i administracyjnie zabezpieczone w sposób uniemożliwiający dostęp do nich osobom trzecim, np.:
 1. Zamknięte pomieszczenia.
 2. Właściwe hasła i ich okresowa zmiana.
 3. Przenoszenie danych na szyfrowanych dyskach lub pendrivach.
 4. Skuteczne skasowanie danych przed zezłomowaniem dysków.
9. Postanowienia Regulaminu odnoszą się zarówno do danych osobowych klientów jak i pracowników.
10. Regulamin obowiązuje od dnia 1 września 2016 roku.