



POLITYKA OCHRONY DANYCH

Glass System Technologies S.A.

POLITYKA OCHRONY DANYCH

W Glass System Technologies S.A. ochrona informacji, danych osobowych oraz poufnych zasobów organizacji jest wysoce istotnym aspektem odpowiedzialnego i zgodnego z prawem działania. W dobie cyfryzacji, rosnącej roli danych oraz ryzyka związanego z ich nieuprawnionym wykorzystaniem, każdy pracownik i współpracownik firmy ma obowiązek zachowania najwyższej staranności w ich przetwarzaniu. Informacje strategiczne, dane kontrahentów, klientów oraz współpracowników są dobrem, które musi być bezwzględnie chronione – nie tylko ze względu na przepisy prawa, ale przede wszystkim ze względu na etykę zawodową, reputację firmy i zaufanie interesariuszy. Ten rozdział Kodeksu definiuje zasady obchodzenia się z informacjami poufnymi i danymi osobowymi, przypomina o obowiązkach wynikających z RODO oraz wyjaśnia, jak postępować, by unikać ryzyk naruszenia poufności w praktyce.



§1. Zasady ogólne

1. Pracownicy, współpracownicy, członkowie zarządu oraz wszystkie osoby działające w imieniu Glass System są zobowiązane do przestrzegania zasad poufności oraz do ochrony danych osobowych i informacji wrażliwych, do których mają dostęp w związku z wykonywaną pracą.
2. Obowiązek zachowania poufności dotyczy zarówno informacji uzyskanych w czasie trwania stosunku pracy/współpracy, jak i po jego zakończeniu.
3. Informacje poufne to wszelkie dane, których ujawnienie mogłoby narazić Spółkę, jej kontrahentów, klientów lub pracowników na szkodę, w szczególności:
 - a) dane finansowe i handlowe,
 - b) dane technologiczne i projektowe,
 - c) dane osobowe,
 - d) strategie biznesowe,
 - e) oferty handlowe, umowy, analizy, plany inwestycyjne,
 - f) dane klientów i dostawców,
 - g) dane logowania i informacje systemowe.

§2. Ochrona danych osobowych (RODO)

1. Spółka działa zgodnie z obowiązującym Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz ustawą o ochronie danych osobowych.
2. Dane osobowe przetwarzane są wyłącznie:
 - a) w zakresie niezbędnym do realizacji celów służbowych,
 - b) na podstawie odpowiednich podstaw prawnych,
 - c) w sposób przejrzysty, bezpieczny i zgodny z zasadą minimalizacji.
3. Każdy pracownik przetwarzający dane osobowe jest zobowiązany do:
 - a) zachowania tajemnicy danych,
 - b) nieprzekazywania ich osobom trzecim bez upoważnienia,
 - c) korzystania wyłącznie z autoryzowanych narzędzi i systemów,
 - d) nieprzechowywania danych w miejscach niechronionych (np. prywatnych urządzeniach, niezaszyfrowanych pendrive'ach).
4. Naruszenie zasad ochrony danych osobowych może skutkować:
 - a) odpowiedzialnością dyscyplinarną,

- b) odpowiedzialnością cywilną i karną,
- c) szkodą dla reputacji Spółki oraz utratą zaufania interesariuszy.

§3. Zasady postępowania z informacjami poufnymi

1. Informacje poufne mogą być przekazywane wyłącznie:
 - a) osobom uprawnionym,
 - b) w zakresie niezbędnym do realizacji obowiązków,
 - c) zgodnie z wewnętrznymi procedurami bezpieczeństwa.
2. Zabrania się:
 - a) kopiowania, udostępniania lub rozpowszechniania informacji bez zgody,
 - b) omawiania tematów poufnych w miejscach publicznych,
 - c) przesyłania danych w sposób niezabezpieczony (np. publiczne e-maile, niezabezpieczone komunikatory),
 - d) wnoszenia dokumentów lub plików poza firmę bez upoważnienia.
3. W przypadku wątpliwości co do charakteru informacji, należy traktować je jako poufne i skonsultować się z przełożonym lub osobą odpowiedzialną za ochronę danych.

§4. Środki bezpieczeństwa i prewencja

1. Spółka wdraża techniczne i organizacyjne środki ochrony danych, m.in.:
 - a) systemy kontroli dostępu,
 - b) szyfrowanie danych,
 - c) audyty bezpieczeństwa IT,
 - d) szkolenia z zakresu ochrony informacji i danych osobowych.
2. Każdy pracownik ma obowiązek:
 - a) przestrzegać zasad logowania, blokowania ekranów i haseł,
 - b) chronić urządzenia służbowe przed dostępem osób nieuprawnionych,
 - c) zgłaszać każdą sytuację naruszenia poufności lub podejrzenia wycieku informacji

§5. Odpowiedzialność i konsekwencje

1. Naruszenie zasad opisanych w niniejszym rozdziale jest traktowane jako poważne wykroczenie przeciwko obowiązkom służbowym i może skutkować:
 - a) upomnieniem,
 - b) rozwiązaniem umowy,
 - c) zawiadomieniem odpowiednich organów w przypadku podejrzenia przestępstwa.
2. Spółka nie ponosi odpowiedzialności za działania pracowników naruszających świadomie politykę poufności, zwłaszcza jeśli działania te były sprzeczne z niniejszym Kodeksem i pisemnymi wytycznymi oraz nie wynikały z charakteru wykonywanych obowiązków służbowych.

