POLITYKA OCHRONY DANYCH OSOBOWYCH

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

1. DEFINICJE

RODO (rozporządzenie, nazywane również ogólnym rozporządzeniem o ochronie danych) to akt prawny, który już 25 maja 2018 r. zastąpi aktualnie obowiązującą ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych.

DANE OSOBOWE Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Oznacza to, że są to informacje, które:

- **pozwalają na ustalenie tożsamości** (np. imię, nazwisko, adres, numer PESEL, numer dowodu osobistego);
- **dotyczą konkretnej, zidentyfikowanej już, osoby fizycznej** (np. jej stan cywilny, wiek, stan zdrowia, wykształcenie, wyznanie, itd.).

PRZETWARZANIE DANYCH OSOBOWYCH: wszelkie operacje wykonywane na danych osobowych, zarówno te:

- zautomatyzowane (np. wykonywane w systemie informatycznym), jak i te niezautomatyzowane (manualne);
- dynamiczne (np. modyfikowanie, aktualizowanie, przesyłanie), jak i statyczne (np. przechowywanie, wgląd).

Przykładowe operacje przetwarzania:
zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

ADMINISTRATOR: podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. To podmiot, który określa zakres pozyskiwanych danych, czas ich przechowywania, sposoby zabezpieczenia, a także podejmuje szereg innych decyzji dotyczących przetwarzanych danych osobowych.

PODMIOT PRZETWARZAJĄCY: podmiot, który przetwarza dane osobowe w imieniu administratora, na podstawie tzw. umowy powierzenia przetwarzania danych osobowych.

NARUSZENIE OCHRONY DANYCH: zdarzenie, którego skutkiem jest przypadkowe lub niezgodne z prawem zniszczenie, utrata, zmiana, ujawnienie lub udostępnienie danych osobowych osobom trzecim.

Przykłady zdarzeń stanowiących naruszenie ochrony danych osobowych:

- umożliwienie wglądu w dokumentację dotyczącą klienta osobom nieupoważnionym (np. innemu klientowi),
- wprowadzenie do systemu informatycznego nieprawidłowych danych,
- ujawnienie osobom nieupoważnionym swojego indywidualnego loginu i hasła i, tym samym, umożliwienie im wykonywania operacji na danych osobowych,
- nieprawidłowe usuwanie dokumentacji zawierającej dane osobowe (np. poprzez wyrzucenie dokumentów do kosza),
- pozostawienie po zakończonym dniu pracy niezabezpieczonych dokumentów zawierających dane osobowe w miejscu dostępnym dla osób trzecich (np. pozostawienie ich na drukarce/ biurku),
- przesłanie informacji dotyczących danego klienta na niewłaściwy adres poczty elektronicznej,
- przesłanie mailem danych osobowych bez zastosowania dodatkowych zabezpieczeń,
- ujawnienie w rozmowie telefonicznej informacji dotyczących danego klienta osobie nieupoważnionej,
- wykonywanie nieuprawnionych kopii danych osobowych (zarówno w formie elektronicznej, jak i papierowej),
- kradzież nośników danych osobowych (np. dokumentacji, sprzętu służącego do przetwarzania danych),
- naruszenie zasad ochrony pomieszczeń, w których przetwarzane są dane (np. poprzez pozostawienie otwartego biura po zakończonym dniu pracy).

2.ZASADY OCHRONY DANYCH

Dane przetwarzane są z zachowaniem następujących zasad:

1. LEGALIZM - w oparciu o podstawę prawną i zgodnie z prawem
2. RZETELNOŚĆ - rzetelnie i uczciwie
3. TRANSPARENTNOŚĆ - w sposób przejrzysty dla osoby, której dane dotyczą
4. MINIMALIZACJA - w konkretnych celach i nie „na zapas”

5. ADEKWATNOŚĆ - nie więcej niż potrzeba
6. PRAWIDŁOWOŚĆ - z dbałością o prawidłowość danych
7. CZASOWOŚĆ - nie dłużej niż potrzeba
8. BEZPIECZEŃSTWO - zapewniając odpowiednie bezpieczeństwo danych

3.ORGANIZACYJNE I TECHNICZNE SPOSOBY ZABEZPIECZENIA DANYCH

1. Ustawienie ekranu monitora komputera w taki sposób, by uniemożliwić osobom postronnym wgląd w widoczne na nim dane osobowe;
2. Hasła, które umożliwiaą zalogowanie się do systemu informatycznego nie mogą być zapisywane w systemie.
3. Przy podejrzeniu, że mogło dojść do ujawnienia hasła dostępu– niezwłocznie jest zmieniane;
4. Pracownicy nie tworzą nieautoryzowanych kopii danych osobowych powierzonych przez Pracodawcę; nie kopiują danych osobowych na zewnętrzne nośniki danych (np. pendrive, płyta CD itp.);
5. Każdy pracownik odchodzący w czasie pracy od stanowiska pracy, ma obowiązek zablokowania komputera ;
6. Pracownicy korzystają wyłącznie z legalnego oprogramowania komputerowego;
7. Wszystkie komputery udostępnione do pracy są wyposażone w aktualne oprogramowanie antywirusowe;
8. Dostęp do komputera, jest zabezpieczyony hasłem;
9. W Firmie stosujemy zasadę czystego biurka/ czystej drukarki/kopiarki
10. Po zakończonym dniu pracy dokumenty umieszcza się w zamkniętych na klucz szafach/ szufladach. Klucze są pozostawiane w miejscu niedostępnym dla osób postronnych;
11. W razie konieczności zniszczenia dokumentu zawierającego dane osobowe, dokumenty są niszczone w sposób bezpiecczny – wyłącznie w niszczarce. Nie wyrzucamy dokumentów do kosza;
12. Wszyscy pracownicy zostali przeszkoleni i zapoznani z przepisami o ochronie danych osobowych – ich świadomość jest kluc zem do bezpieczeństwa tych danych;
13. Pracownicy przestrzegają przepisów prawa o ochronie danych osobowych i stosują się do wytycznych Pracodawcy w tym zakresie.
14. Dyski komputerów i dyski zewnętrzne, na których tworzone są autoryzowane kopie zapasowe danych są szyfrowane.