RODO - praktyczne zastosowanie przepisów

Rozporządzenie o Ochronie Danych Osobowych (RODO) to nie tylko formalność, ale realna ochrona danych osobowych w codziennej praktyce. Właściwe przestrzeganie przepisów pomaga chronić klientów, pracowników oraz wizerunek organizacji.

W tej prezentacji przedstawimy najczęstsze błędy związane z przetwarzaniem danych osobowych oraz prawidłowe sposoby postępowania zgodne z wymogami RODO. Pamiętajmy, że najczęściej to nie technologia zawodzi, ale człowiek - dlatego tak ważna jest wiedza i ostrożność.

Komunikacja mailowa a ochrona danych

Błąd

Wysłanie wiadomości do kilkunastu klientów z widocznymi adresami e-mail w polu „Do" lub „DW", co prowadzi do ujawnienia danych kontaktowych wszystkim odbiorcom.

Zgodnie z RODO

Adresy e-mail powinny być ukryte w polu „UDW" (ukryte do wiadomości), by nie ujawniać danych innym odbiorcom i chronić prywatność każdego adresata.

Konsekwencje

Ujawnienie adresów e-mail może prowadzić do naruszenia prywatności, a w niektórych przypadkach skutkować skargą do UODO i karami finansowymi.

Bezpieczeństwo nośników danych

Problem

Pendrive bez hasła i szyfrowania zgubiony w komunikacji miejskiej zawiera imiona, nazwiska i numery telefonów pacjentów lub klientów.

Takie zdarzenie stanowi poważne naruszenie ochrony danych osobowych i wymaga natychmiastowej reakcji.

Rozwiązanie

Nośniki muszą być zabezpieczone hasłem i szyfrowaniem. Każdy incydent powinien zostać zgłoszony jako naruszenie danych osobowych do administratora danych i – w razie potrzeby – do UODO.

Warto rozważyć również stosowanie nośników z fizycznym zabezpieczeniem lub rozwiązań chmurowych z dwuskładnikowym uwierzytelnianiem.

Dokumenty papierowe i wydruki

Nieprawidłowe postępowanie

Wydrukowanie danych pracowników (listy płac, CV) i pozostawienie dokumentu przez kilka godzin w ogólnodostępnej drukarce.

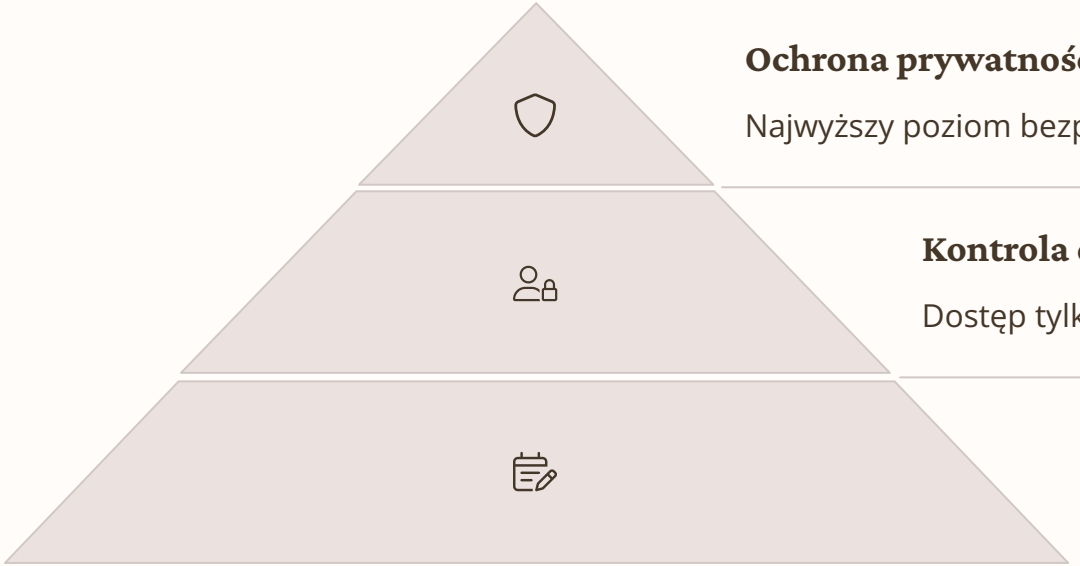
Prawidłowe zabezpieczenie

Dokumenty zawierające dane osobowe należy natychmiast odbierać z drukarki lub korzystać z funkcji „druk poufny" (wydruk wymaga PIN-u).

Utylizacja dokumentów

Niepotrzebne dokumenty z danymi osobowymi powinny być niszczone w niszczarkach, a nie wyrzucane do zwykłego kosza.

Zasada minimalizacji dostępu do danych



Ochrona prywatności

Najwyższy poziom bezpieczeństwa

Kontrola dostępu

Dostęp tylko dla uprawnionych osób

Minimalizacja danych

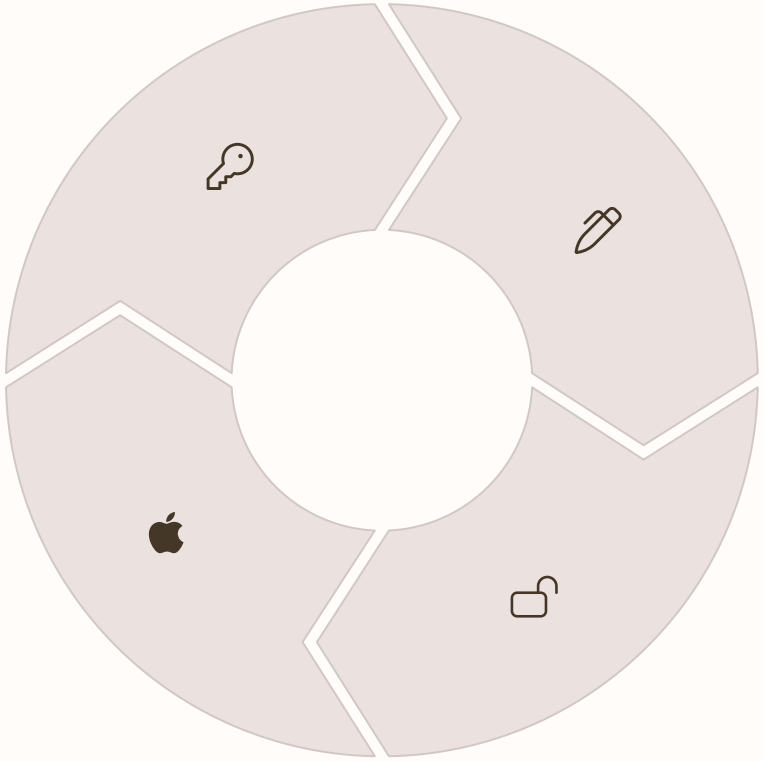
Podstawa bezpieczeństwa informacji

Błędem jest sytuacja, gdy pracownicy działu technicznego mają dostęp do dokumentacji HR lub danych klientów, mimo że nie jest im to potrzebne do pracy. Zgodnie z RODO obowiązuje zasada „minimalizacji danych" – dostęp ma tylko osoba, która realnie potrzebuje informacji do wykonania obowiązków służbowych.

Urządzenia prywatne w środowisku pracy

Silne hasła/PIN

Podstawowe zabezpieczenie dostępu do urządzenia



Aktualne oprogramowanie

Regularne aktualizacje systemów i aplikacji

Autoryzowane aplikacje

Korzystanie tylko z bezpiecznych programów

Szyfrowanie danych

Ochrona przed nieautoryzowanym dostępem

Błędem jest edytowanie plików z danymi osobowymi na prywatnym laptopie lub tablecie bez odpowiednich zabezpieczeń. Zgodnie z RODO, urządzenia, na których przetwarzane są dane osobowe, muszą być odpowiednio zabezpieczone według powyższych zasad.

Weryfikacja tożsamości i udostępnianie danych

Kontakt

Prośba o dane przez telefon

Weryfikacja

Potwierdzenie tożsamości

Decyzja

Udostępnienie lub odmowa

Dokumentacja

Rejestracja zdarzenia

Błędem jest udzielanie informacji o kliencie przez telefon osobie, która tylko twierdzi, że jest jego współmałżonkiem. Zgodnie z RODO, zanim przekażesz jakiekolwiek dane, musisz mieć pewność, że rozmawiasz z osobą uprawnioną. Najlepiej zweryfikować tożsamość lub skierować sprawę do przełożonego.

Pamiętaj, że w przypadku przekazywania danych osobowych podmiotom zewnętrznym konieczne jest zawarcie umowy powierzenia przetwarzania danych, która określa zakres i cel przetwarzania oraz gwarantuje odpowiedni poziom bezpieczeństwa.

Dobre praktyki zgodne z RODO

Bezpieczeństwo techniczne

- Szyfruj dane na nośnikach i w urządzeniach
- Regularnie aktualizuj oprogramowanie zabezpieczające
- Korzystaj z bezpiecznych systemów uwierzytelniania

Bezpieczeństwo fizyczne

- Zabezpieczaj dokumenty papierowe – zamykaj je w szafkach
- Nie zabieraj danych osobowych do domu bez zgody pracodawcy
- Stosuj politykę czystego biurka i ekranu

Procedury i zasady

- Zgłaszaj incydenty (zgubiony laptop, otwarty e-mail do złej osoby)
- Nie przechowuj danych dłużej niż to konieczne
- Zbieraj tylko dane niezbędne do realizacji celu
- Zawsze weryfikuj czy istnieje umowa powierzenia przetwarzania danych przed udostępnieniem danych firmom zewnętrznym