

OCHRONA DANYCH OSOBOWYCH

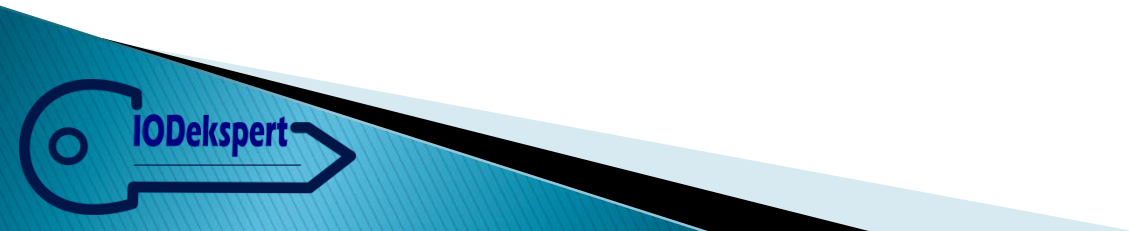
Przygotował
Grzegorz Dżuga



Na podstawie:

Polityki Ochrony Danych

przyjętej w jednostce



Wszelkie informacje, zarówno w
formie papierowej,
jak i elektronicznej - pozwalające
na identyfikację konkretnej osoby
stanowią dane osobowe
podlegające ochronie.

Każdy posiadający dostęp do danych osobowych jest zobowiązany do zabezpieczenia danych osobowych przed ich zniszczeniem lub udostępnieniem osobom nieuprawnionym.

Każdy, kto w ramach swoich obowiązków służbowych posługuje się dokumentami zawierającymi dane osobowe musi przechowywać je w szafach zamykanych na klucz, stosować zasadę czystego biurka i czystego ekranu.

Zgodnie z postanowieniami Polityki Ochrony Danych:

- zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie ochrony przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu,
- każdy Użytkownik jest zobowiązany do zapoznania się z instrukcją obsługi systemu informatycznego.

Zgodnie z postanowieniami Polityki Ochrony Danych:

- w celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.

Zgodnie z postanowieniami Polityki Ochrony Danych:

- zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika,
- użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora,

Zgodnie z postanowieniami Polityki Ochrony Danych:

- użytkownik zobowiązany jest do przestrzegania zasady czystego biurka, w szczególności przed opuszczeniem swego stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym systemem oraz informatyczne nośniki danych (płyty CD, DVD, pamięci przenośne, zawierające dane osobowe)

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników systemu informatycznego:

- rozpoczęcie pracy następuje po uruchomieniu komputera,
- uruchomienie systemu następuje po wybraniu przez Użytkownika odpowiedniego profilu użytkownika (spośród dostępnych na ekranie logowania).
- w celu chwilowego zawieszenia pracy należy zablokować system lub włączyć wygaszacz ekranu zabezpieczony hasłem. Jeśli komputer Użytkownika nie pozwala na zablokowanie hasłem, należy wylogować się z systemu,
- po zakończeniu pracy należy wylogować się z systemu.

Każdy pracownik zobowiązany jest do zgłaszania naruszeń i incydentów związanych z ochroną danych. Naruszeniem ochrony danych może być np.:

- zabranie, zgubienie, zniszczenie, kradzież dokumentu zawierającego dane osobowe,
- wykrycie na komputerze złośliwego oprogramowania (wirusa, trojana),
- uszkodzenie komputera lub innego urządzenia służącego do pracy na danych osobowych,
- zgubienie np.: smartfonu, laptopa, pendrive'a.

Każdy pracownik realizując zadania określone w zakresie czynności zobowiązany jest do ciągłej oceny, w szczególności:

- czy sposób, w jaki realizowane jest zadanie odpowiednio zabezpiecza przetwarzane dane, przed ich utratą, nieuprawnionym dostępem, zmianą,
- czy udostępnienie danych innym osobom (w tym współpracownikom) i podmiotom jest zgodne z prawem, a przede wszystkim czy sam sposób udostępniania nie narusza prawa i przyjętych procedur.
- czy zakres przetwarzanych danych jest zgodny z prawem i czy stosowana jest zasada minimalizacji danych,
- czy dane są przetwarzane i przechowywane przez właściwy okres i czy stosowane metody pracy umożliwiają kontrolę tych okresów.

Pracownicy zobowiązani są do spełniania obowiązku informacyjnego w stosunku do osób, których dane przetwarzają wykonując zadania określone w zakresach czynności służbowych oraz do realizacji innych ich praw określonych w RODO.

Klauzula informacyjna (wzór do uzupełnienia)

- Administratorem Państwa danych osobowych jest
- Możecie się Państwo kontaktować również z wyznaczonym przez Administratora inspektorem ochrony danych pod telefonem adresem email *- tu podajemy telefon i email do jednostki.*
- Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu wyłącznie w celu
proszę wpisać cel dla którego gromadzimy i wykorzystujemy dane na podstawie jeśli wcześniej nie podano a istnieje proszę podać podstawę prawną
- Odbiorcami Państwa danych osobowych będą organy uprawnione na podstawie przepisów prawa.
..... *-tu proszę wpisać ewentualnie komu dane zostaną przekazane*
- Będziemy przetwarzać podane dane osobowe przez – *proszę podać po jakim czasie dane zostaną usunięte*
- Zgodnie z RODO przysługuje Państwu:
 - prawo dostępu do swoich danych oraz otrzymania ich kopii;
 - prawo do sprostowania (poprawiania) swoich danych;
 - prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub prawnie uzasadnionych interesów administratora,
 - prawo do ograniczenia przetwarzania danych;
 - prawo do wniesienia skargi do Prezesa UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)
- Podanie przez Państwa danych osobowych w niniejszym formularzu, jest dobrowolne jednak niezbędne aby
.....
- Administrator nie ma zamiaru przekazywania danych osobowych do państwa trzeciego lub do organizacji międzynarodowej. W trakcie przetwarzania danych osobowych żadne decyzje dotyczące Państwa nie będą zapadać automatycznie oraz nie będą tworzone żadne profile, co oznacza, że nie będą podejmowane działania, o których mowa w art. 22 ust. 1 i 4 RODO¹.

Praktyczne porady przetwarzania danych osobowych.

Zasada czystego ekranu

Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd),
Monitory komputerów wyposażone są w wygaszacze ekranu, (...).
Wznowienie wyświetlenia następuje po wprowadzeniu odpowiedniego hasła przez użytkownika.

Zablokowanie lokalnego komputera

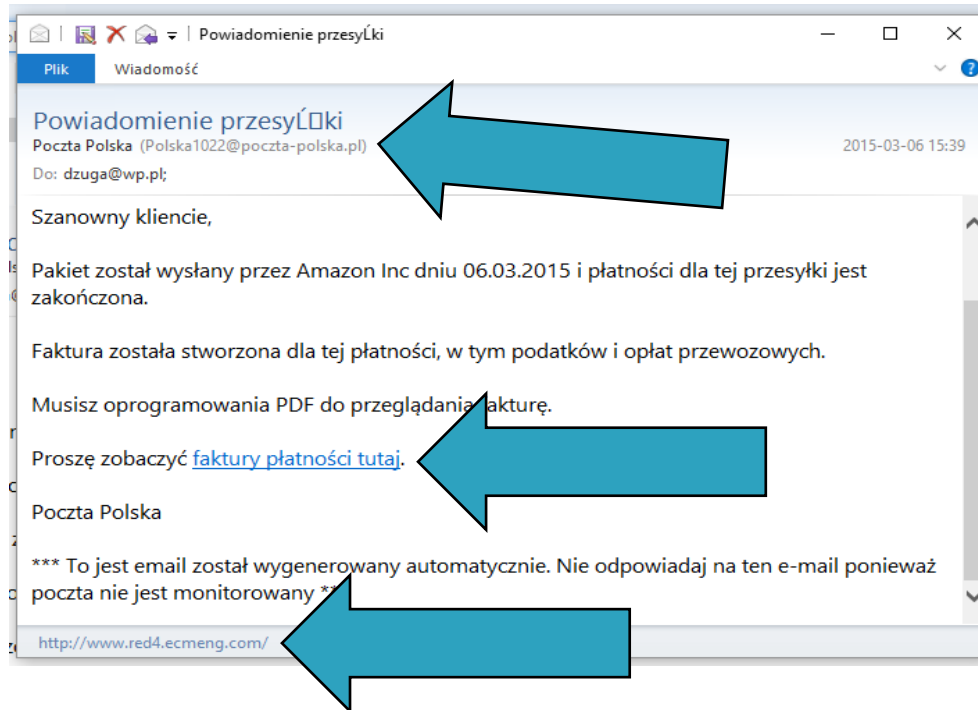
Metod blokowania lokalnego komputera jest kilka:

- wybranie odpowiedniej opcji z menu start
- wybranie z listy po wciśnięciu Ctr+Alt+Del
- użycie skrótu klawiszowego Win+L



Lock Computer (WIN-L)

Fałszywe email'e



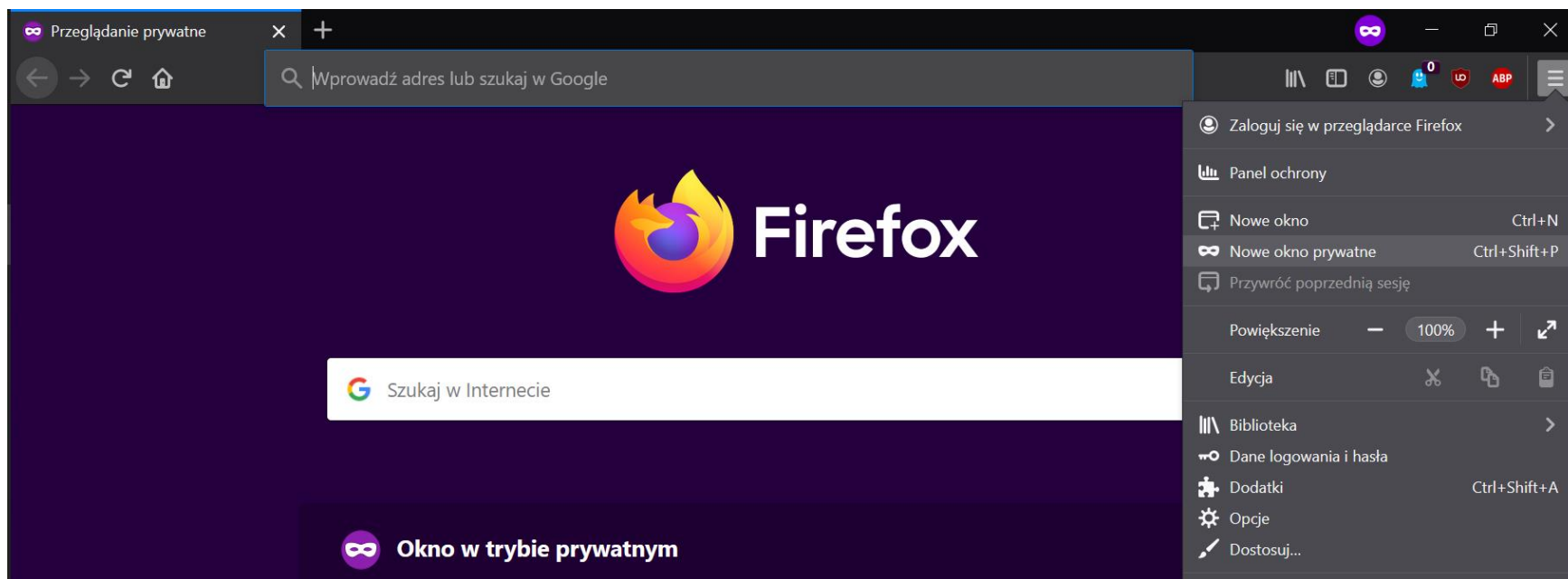
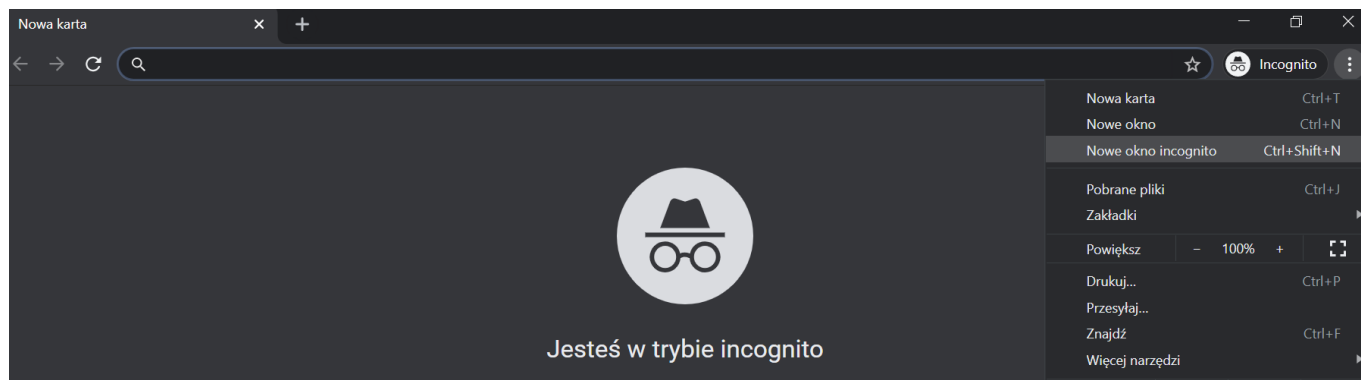
- Brak Twojego adresu w polu TO:/DO:
- Nieprawidłowa nazwa nadawcy w adresie mailowym
- Błędy w treści lub temacie wiadomości
- Brak logo i zdjęć w treści wiadomości
- Fałszywy adres URL
- Fałszywe załączniki
- Zachęcanie do podania osobistych danych

Sprawdź się na stronie:

<https://phishingquiz.withgoogle.com/>

Konfiguracja przeglądark:

- Tryb prywatny, incognito



Przykłady incydentów

- Korespondencja elektroniczna:
 - niewłaściwie zaadresowana poczta elektroniczna,
 - nie wykorzystywanie opcji „kopii ukrytej”.
- Utrata (zagubienie, kradzież) telefonu, laptopa, pamięci przenośnej.
- Wyłudzenie informacji z wykorzystaniem różnego rodzaju socjotechnik.
- Nieodpowiednie techniki usuwania danych.

W wypadku pytań proszę o kontakt

Grzegorz Dżuga
iod@techbig.pl

