

OCHRONA DANYCH OSOBOWYCH **WYMAGANIA RODO**

PLAN SZKOLENIA

-
1. Pojęcia i definicje
 2. Zasady przetwarzania danych osobowych
 3. Prawa osób, których dane dotyczą
 4. Udostępnianie danych
 5. Powierzenie danych podmiotom zewnętrznym
 6. Obowiązki pracowników i sankcje
 7. Zabezpieczenie danych
 8. Zarządzanie incydentami
-

RODO

- ▶ Od 25 maja 2018r. obowiązuje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Podstawowe pojęcia



Podstawowe pojęcia

Dane osobowe

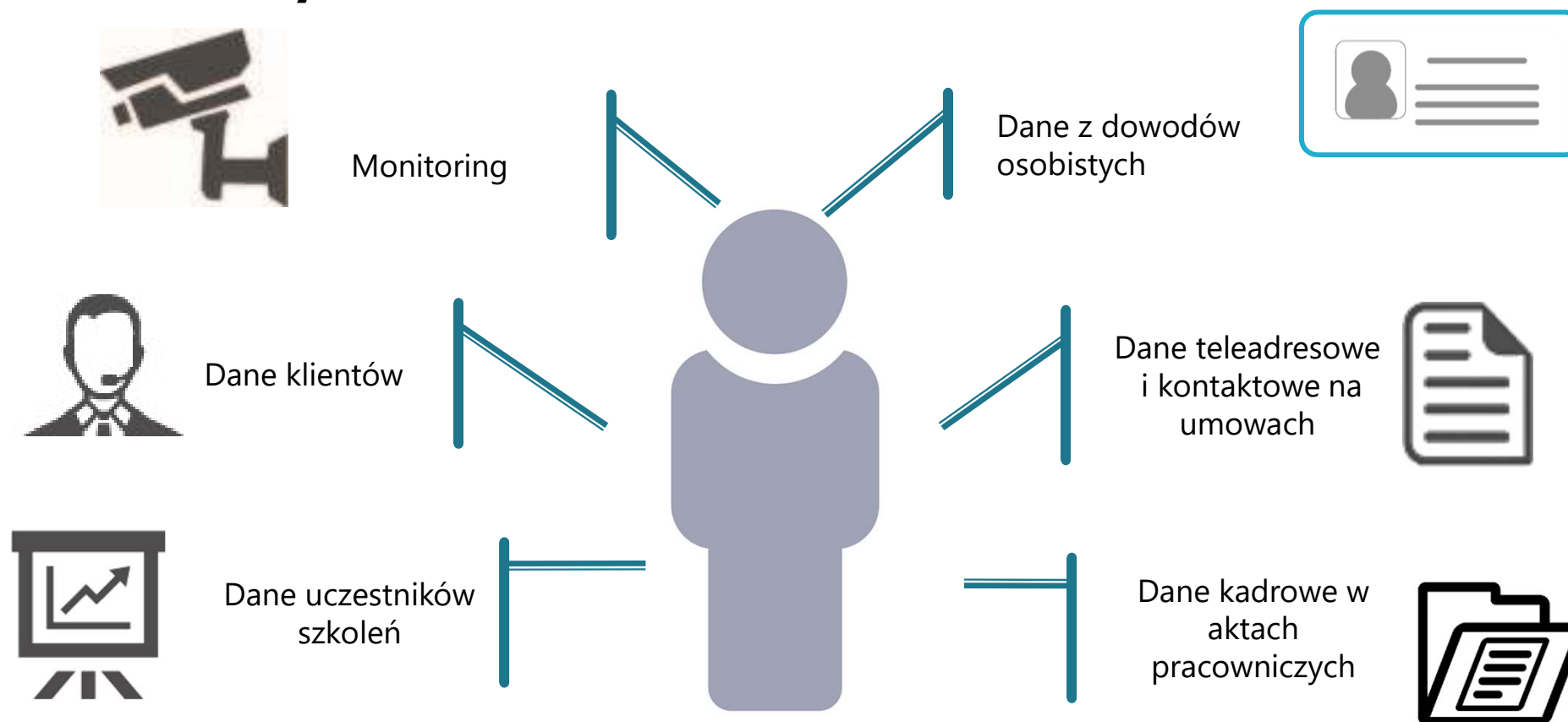
Są to wszelkie informacje, za pomocą których można zidentyfikować osobę fizyczną, chociaż nie jest ona wyraźnie wskazana.

Możliwą do zidentyfikowania jest taka osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne

1

Podstawowe pojęcia

Przykładowe kategorie przetwarzanych danych osobowych

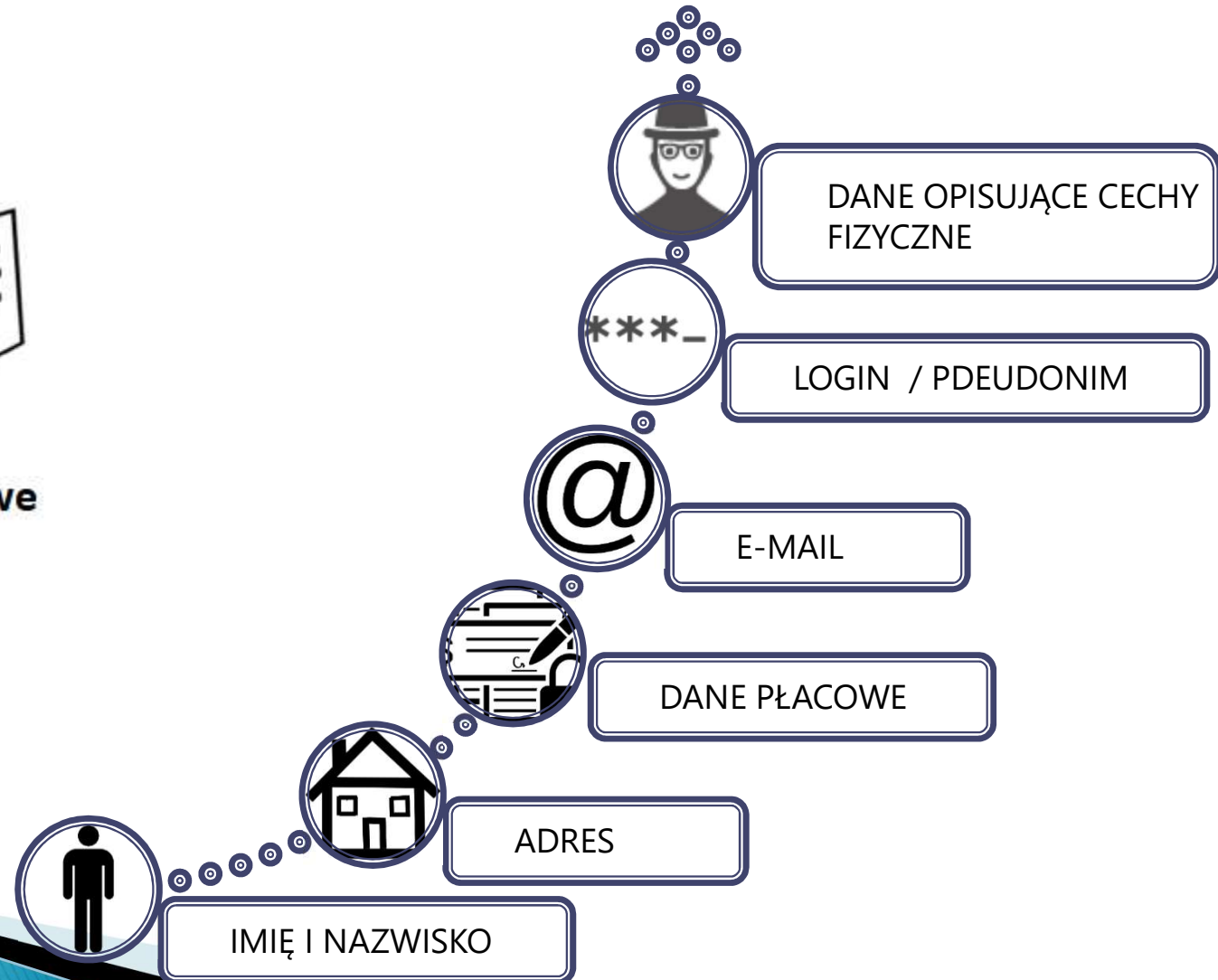


Podstawowe pojęcia

Jakie informacje mogą być danymi osobowymi



dane osobowe



Podstawowe pojęcia

Przetwarzanie

Jakiegolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Podstawowe pojęcia

Jakie operacje są przetwarzaniem danych?



WPROWADZNIENIE DANYCH
DO SYSTEMU
INFORMATYCZNEGO



KOPIOWANIE
DOKUMENTÓW NP.
TOŻSAMOŚCI



PRZESYŁANIE DANYCH
MAILEM



ROZMOWA TELEFONICZNA
W CALL CENTER



OPERACJE NA DANYCH –
ZESTAWIANIE,
PORÓWNYWANIE



NISZCZENIE DANYCH



PRZECHOWYWANIE
DANYCH PAPIEROWYCH
W SZAFACH

Podstawowe pojęcia

Administrator Danych (AD)

Organ, instytucja, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych (to on ma interes w przetwarzaniu).

AD Ponosi odpowiedzialność za dane i jest odpowiedzialny za ich zabezpieczenie.

Podstawowe pojęcia

INSPEKTOR OCHRONY DANYCH (IOD)

osoba nadzorująca przestrzeganie przepisów ustawy o ochronie danych osobowych w firmie

Zadania IOD:

- informowanie AD, podmiotu przetwarzającego oraz pracowników spoczywających na nich o obowiązkach oraz doradzanie im w tej sprawie;
- monitorowanie przestrzegania przepisów o ochronie danych osobowych;
- Prowadzenie szkoleń
- współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego

Zasady przetwarzania danych

Zasady przetwarzania danych

PODSTAWY PRAWNE – KIEDY MOŻNA PRZETWARZAĆ DANE?



KIEDY WYMAGA TEGO PRZEPIS PRAWA

- **Przykład:** Dane pracowników (na podstawie Kodeksu Pracy)



KIEDY DANA OSOBA JEST STRONĄ UMOWY

- **Przykład:** Umowa kupna - sprzedaży



KIEDY OSOBA WYRAZIŁA NA TO ZGODĘ

- **Przykład:** Dane potencjalnych klientów pozyskiwane w celach marketingowych

Zasady przetwarzania danych

PODSTAWY PRAWNE – KIEDY MOŻNA PRZETWARZAĆ DANE?



KIEDY JEST TO NIEZBĘDNE DO OCHRONY ŻYWOTNYCH INTERESÓW

- **Przykład:** Ratowanie życia



KIEDY REALIZOWANE JEST W INTERESIE PUBLICZNYM LUB W RAMACH WYKONYWANIA WŁADZY PUBLICZNEJ

- **Przykład:** Płacenie podatków



KIEDY AD MA PRAWNIE USPRAWIEDLIWIONY INTERES W PRZETWARZANIU

- **Przykład:** Nagrania z monitoringu

Zasady przetwarzania danych

ZASADY: OGRANICZENIA CELU I MINIMALIZACJI DANYCH

PRZYKŁAD



ZAKRES DANYCH NA
DOWODZIE OSOBISTYM

Imię i nazwisko

Nazwisko
panieńskie,
imiona rodziców

Data urodzenia i
płeć



Seria i nr dowodu
osobistego

Miejsce urodzenia

PESEL

Zasady przetwarzania danych

ZASADY: OGRANICZENIA CELU I MINIMALIZACJI DANYCH

PRZYKŁAD

W CELU
POTWIERDZENIA
TOŻSAMOŚCI
POTRZEBNE SĄ
JEDYNNIE:



Imię i nazwisko



Seria i nr dowodu osobistego

Obowiązki pracowników i sankcje

Obowiązki pracowników i sankcje

OBOWIĄZKI PRACOWNIKÓW



Zachowanie w poufności danych, do których pracownik ma dostęp w związku z pełnieniem obowiązków



Zakres przetwarzanych danych wynika z obowiązków służbowych – ochrona także przed innymi pracownikami na innych stanowiskach



Stosowanie się do przyjętych zasad: określonych w procedurach, przekazanych na tym szkoleniu



Zgłaszanie wszystkich zaobserwowanych nieprawidłowości

Obowiązki pracowników i sankcje

SANKCJE KARNE



Art. 266 Kodeksu karnego

Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Obowiązki pracowników i sankcje

SANKCJE KARNE



Art. 267 Kodeksu karnego

Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Tej samej karze podlega, kto informację uzyskaną w sposób określony powyżej ujawnia innej osobie.

Obowiązki pracowników i sankcje

SANKCJE KARNE



Art. 268 Kodeksu karnego –

Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Kto, dopuszczając się czynu, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Obowiązki pracowników i sankcje

SANKCJE KARNE



Art. 24. § 1. Kodeksu cywilnego

Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny

6 Obowiązki pracowników i sankcje

SANKCJE KARNE



art. 114 - 115 Kodeksu Pracy

Odpowiedzialność pracownika zachodzi m.in., gdy: nie wykonuje lub nienależycie wykonuje on swoje obowiązki pracownicze.

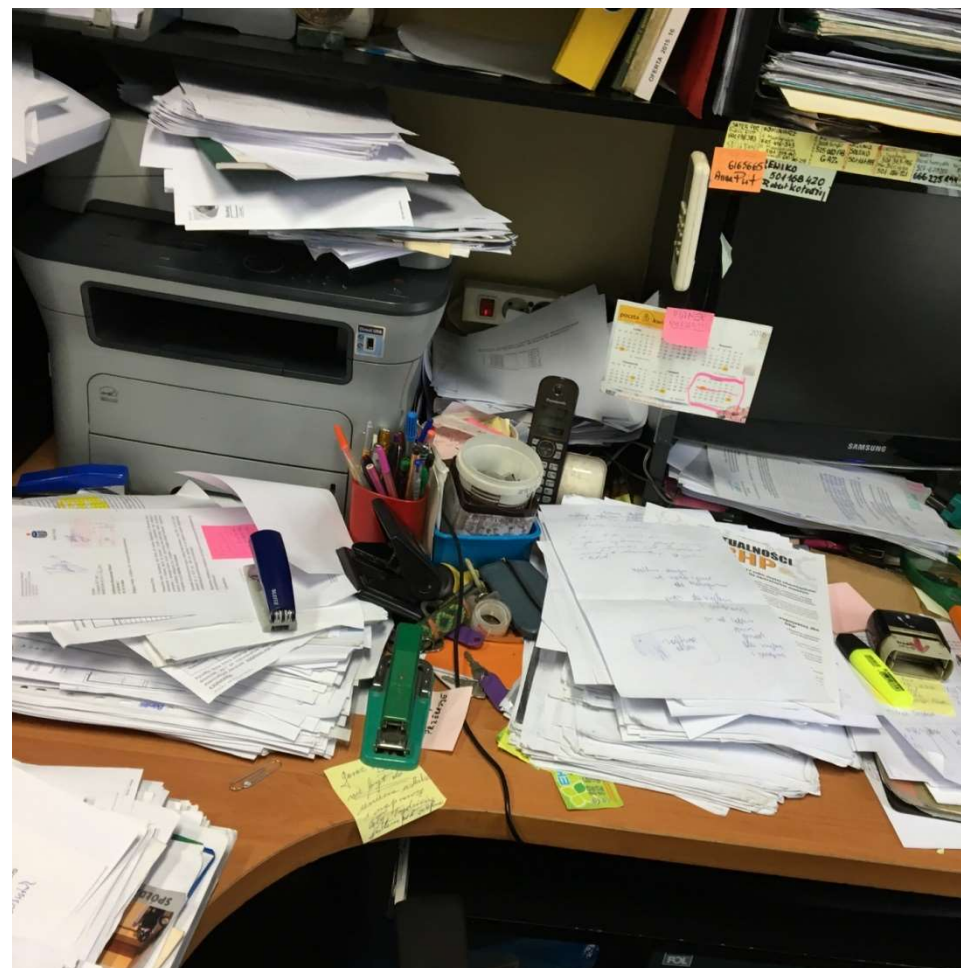
Odpowiedzialność pracownika (ograniczona jest wyłącznie do szkody wyrządzonej z winy pracownika, to oznacza, że nie można pociągnąć pracownika do odpowiedzialności w przypadku działań lub zachowań niezawinionych

Zabezpieczenia danych

Zabezpieczenia danych

ZABEZPIECZENIA DOKUMENTACJI PAPIEROWEJ

1. NIEPOTRZEBNE
DOKUMENTY I BŁĘDNE
WYDRUKI POWINNY BYĆ
OD RAZU NISZCZONE W
NISZCZARKACH



Zabezpieczenia danych

ZABEZPIECZENIA DOKUMENTACJI PAPIEROWEJ

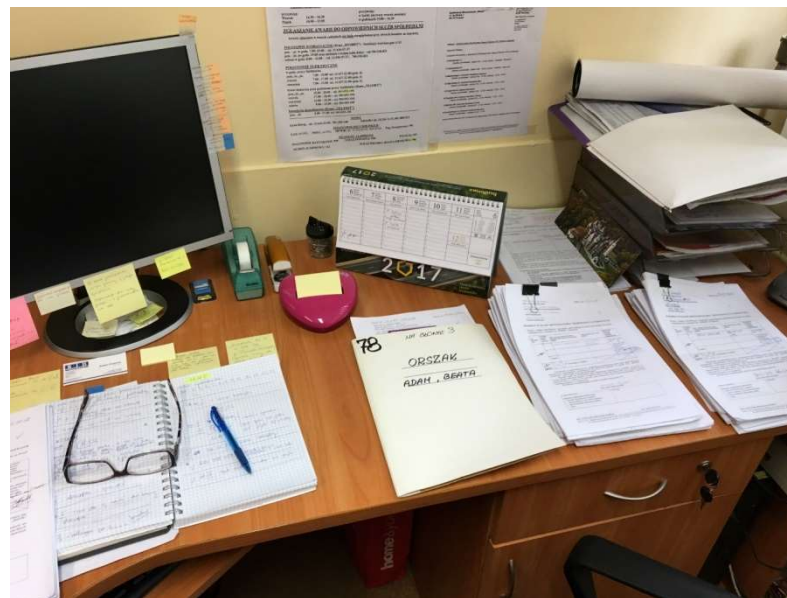
2. SZAFY, W KTÓRYCH
PRZECHOWUJE SIĘ
DOKUMENTY POWINNY
BYĆ ZAMYKANE, A KLUCZE
ZABEZPIECZANE ZGODNIE Z
WEWNĘTRZNĄ PROCEDURĄ



Zabezpieczenia danych

ZABEZPIECZENIA DOKUMENTACJI PAPIEROWEJ

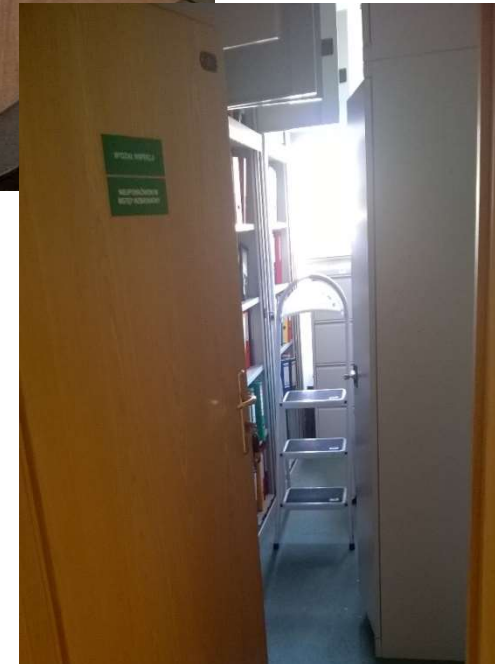
3. STOSOWANIE POLITYKI CZYSTEGO BIURKA, ZWŁASZCZA PO GODZINACH PRACY



Zabezpieczenia danych

ZABEZPIECZENIA POMIESZCZEŃ

1. POMIESZCZENIA – POKOJE
NIE POWINNY BYĆ
POZOSTAWIANE BEZ
NADZORU – NALEŻY
ZAMKNAĆ POMIESZCZENIE
PO OPUSZCZENIU GO PRZEZ
OSTATNIĄ UPOWAŻNIONĄ
OSOBĘ.



Zabezpieczenia danych

ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH

1. KAŻDA OSOBA POSIADA SWÓJ LOGIN I

HASŁO DO KOMPUTERA I JEST

ZOBOWIĄZANA DO TEGO, ABY NIE

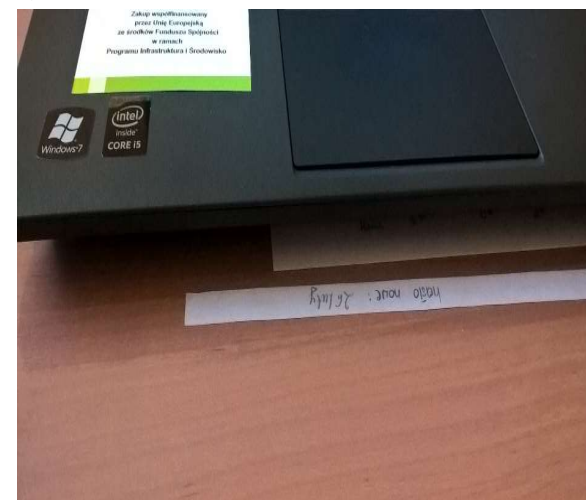
UJAWNIAĆ HASEŁ INNYM OSOBOM.

PRACOWNIK ODPOWIADA ZA

ZACHOWANIE POUFNOŚCI SWOJEGO

HASŁA, ZATEM NIEUPRAWNIONE JEST:

- ZAPISYWANIE HASEŁ
- KORZYSTANIE Z FUNKCJI ZAPAMIĘTYWANIA HASEŁ
- PRZEKAZYWANIE HASEŁ INNYM OSOBOM



Zabezpieczenia danych

ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH

2. KAŻDE ODEJŚCIE OD KOMPUTERA -
WYLOGOWANIE POPRZECZ NACIŚNIĘCIE
KOMBINACJI KŁAWISZY
CTRL + ALT + DEL LUB **WINDOWS + L**

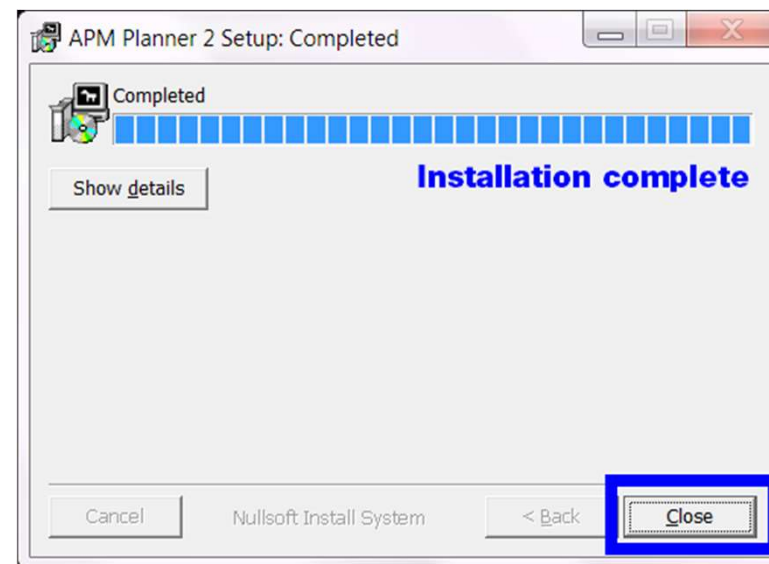
PO ZAKOŃCZENIU PRACY NALEŻY
WYLOGOWAĆ SIĘ Z WSZYSTKICH
PROGRAMÓW I APLIKACJI ORAZ
WYŁĄCZYĆ KOMPUTER.



Zabezpieczenia danych

ZASADY KORZYSTANIA Z OPROGRAMOWANIA

1. NIEDOZWOLONE JEST
INSTALOWANIE JAKIEGOKOLWIEK
OPROGRAMOWANIA NA
KOMPUTERACH SŁUŻBOWYCH
2. NIE NALEŻY WYKORZYSTYWAĆ W
PRACY SYSTEMÓW, NA KTÓRE LICENCJI
NIE POSIADA AD



Zabezpieczenia danych

ZASADY KORZYSTANIA Z INTERNETU

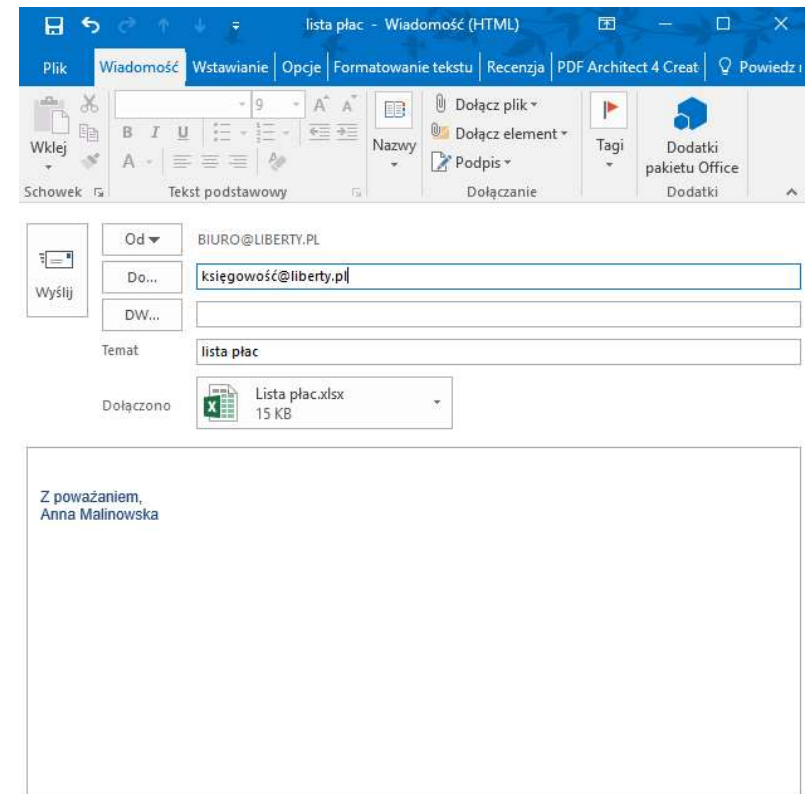
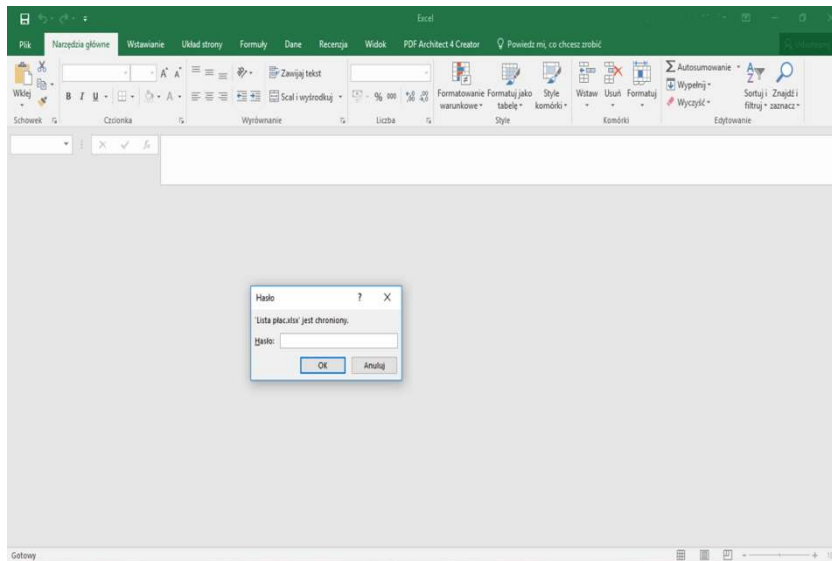
1. KORZYSTANIE W CELU WYKONYWANIA OBOWIĄZKÓW SŁUŻBOWYCH
2. ZAKAZ ŚCIAĞANIA PLIKÓW NIEZWIĄZANYCH Z OBOWIĄZKAMI SŁUŻBOWYMI
3. OBOWIĄZEK PRZESTRZEGANIA PRAWA WŁASNOŚCI PRZEMYSŁOWEJ I PRAW AUTORSKICH



Zabezpieczenia danych

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

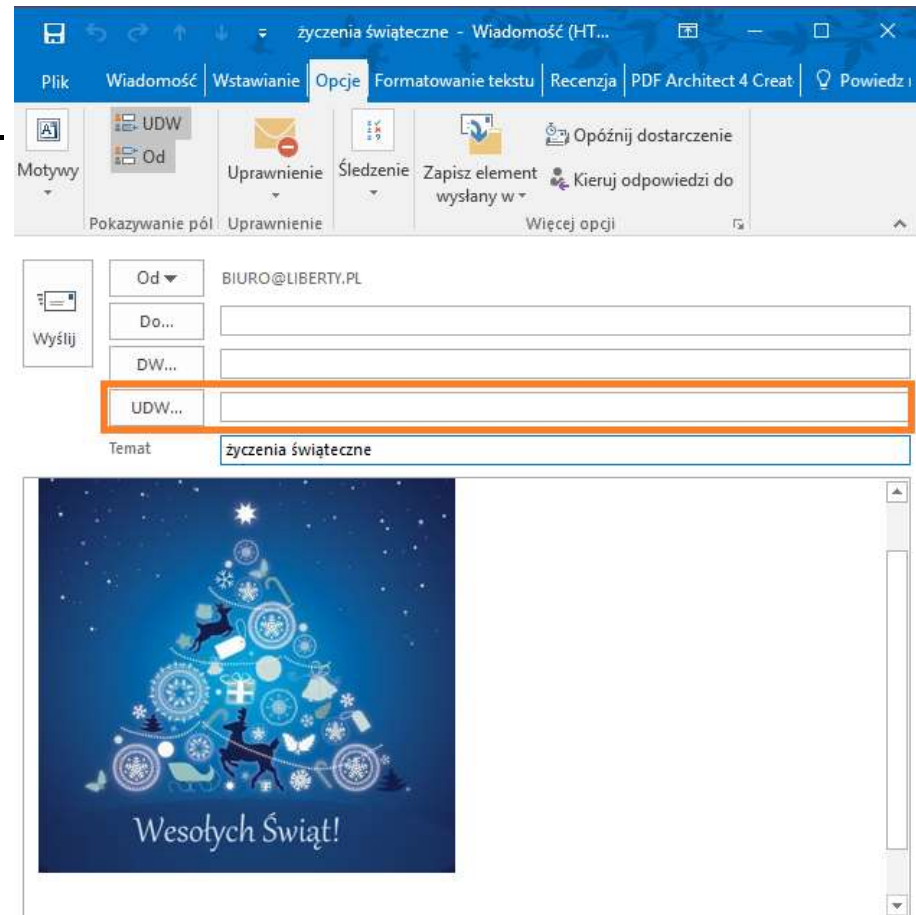
1. DANE OSOBOWE PRZESYŁANE WYŁĄCZNIE W ZASZYFROWANYM ZAŁĄCZNIKU WIADOMOŚCI E-MAIL



Zabezpieczenia danych

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. PRZY WYSYŁANIU
ZBIOROWYCH WIADOMOŚCI E-
MAIL, KTÓRYCH ADRESACI
MOGĄ SIĘ NIE ZNAĆ –
UŻYWAMY POLA **UDW**



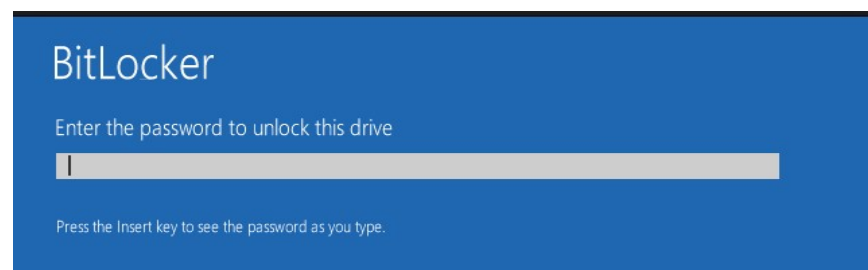
Zabezpieczenia danych

ZASADY KORZYSTANIA Z NOŚNIKÓW DANYCH

1. UŻYWANIE WYŁĄCZNIE
SŁUŻBOWYCH PENDRIVÓW DO
PRZENOSZENIA DANYCH OSOBOWYCH

2. DANE LUB SAMO URZĄDZENIE
MUSZĄ BYĆ ZASZYFROWANE

3. USZKODZONE NOŚNIKI
TRAKTUJEMY JAK DYSKI
TWARDE – PRZEKAZUJEMY DO
DZIAŁU IT



Incydenty i naruszenia

Incydenty i naruszenia



ZAWIADOMIENIE O NARUSZENIU

Administrator Danych ma obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego w terminie do **72 godzin** od chwili ujawnienia naruszenia, o ile naruszenie powoduje **wysokie ryzyko (lub uzasadnioną pewność) naruszenia praw i wolności** osób których dane dotyczą.

Incydenty i naruszenia

TYPOWE ZAGROŻENIA DLA DANYCH

Niewłaściwe zabezpieczenia fizyczne (otwarte szafki, drzwi)

Niestosowanie zasady czystego biurka, ekranu

Niewylogowywanie się z systemu

Awaria komputera

Incydenty i naruszenia

TYPOWE INCYDENTY / NARUSZENIA

Zdarzenia losowe (zalanie, pożar)

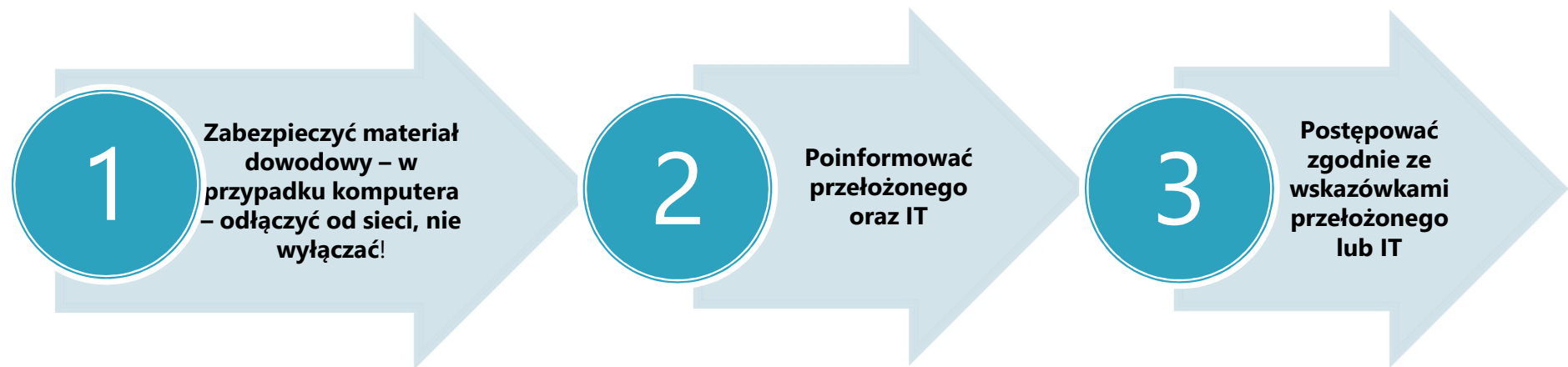
Awaria serwera, twardego dysku

Wyciek, kradzież danych

Zapoznanie się z danymi przez osobę nieupoważnioną

Incydenty i naruszenia

POSTĘPOWANIE W PRZYPADKU ZAGROŻENIA LUB INCYDENTU



Dziękujemy za uwagę