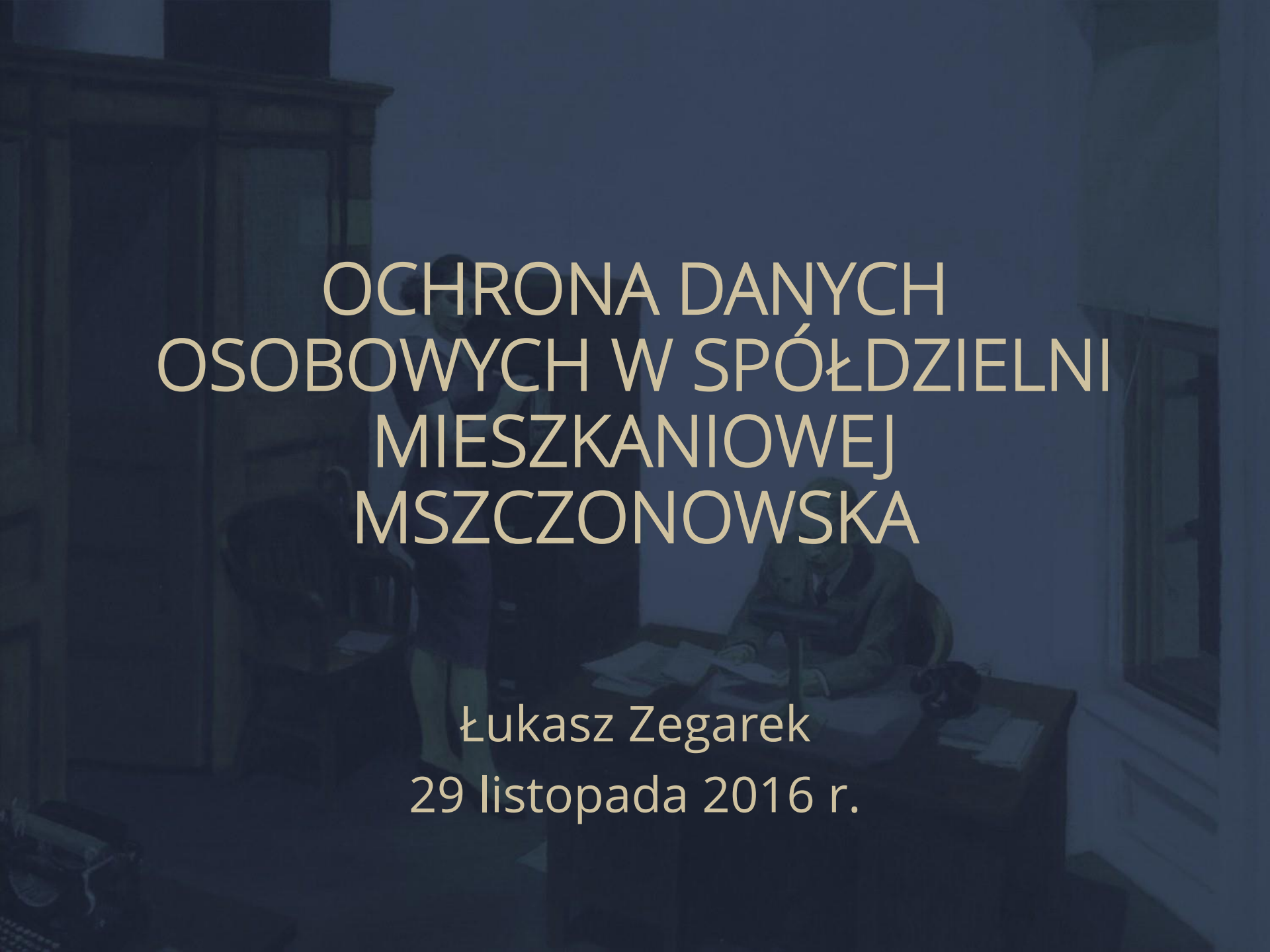




LEX ARTIST



OCHRONA DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ MSZCZONOWSKA

Łukasz Zegarek
29 listopada 2016 r.

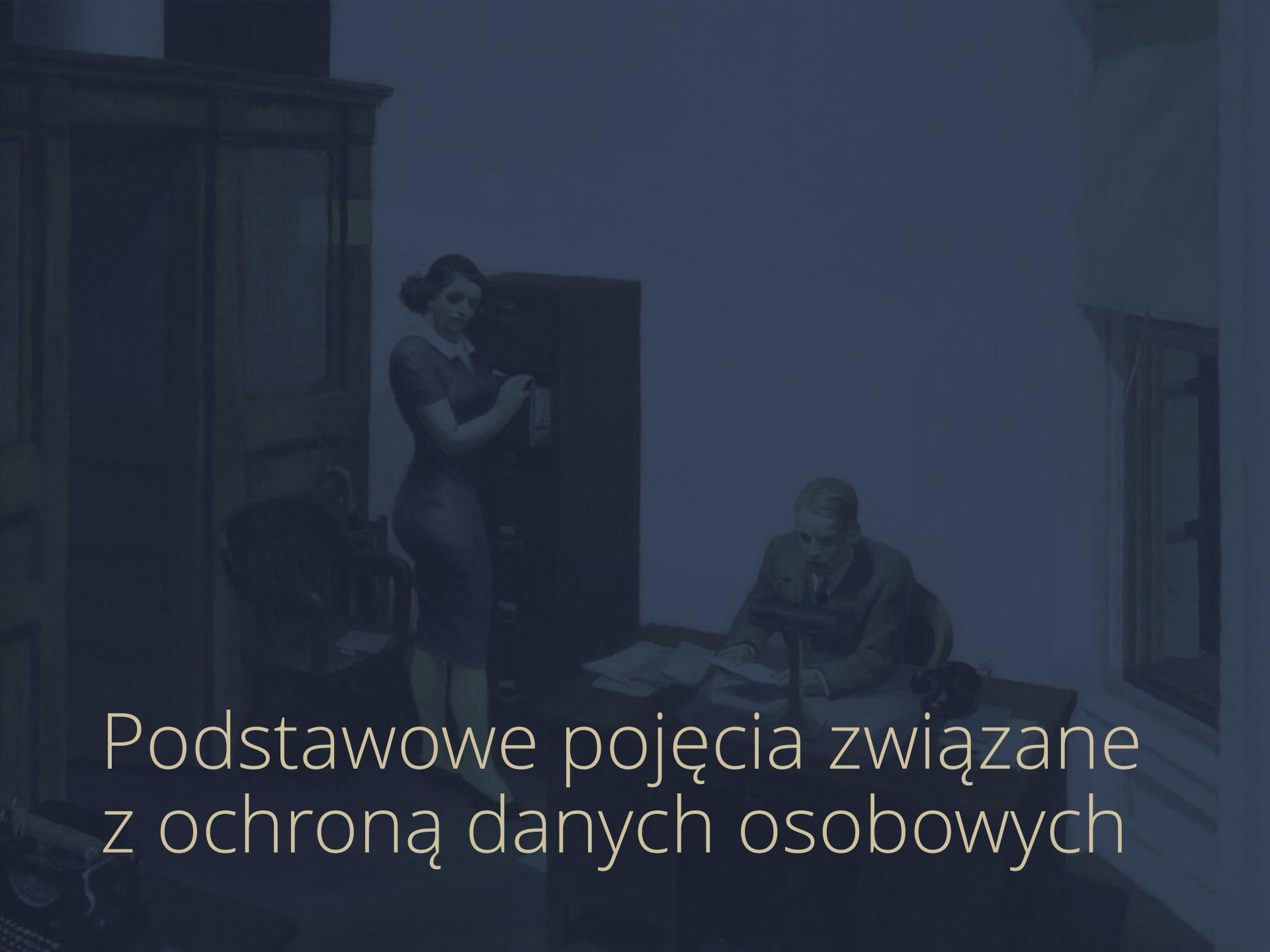
Po co nam ochrona danych osobowych?



- obowiązek: ustawa, umowa
- bezpieczeństwo własnych danych
- pewność siebie w pracy



- obowiązek: ustawa, umowy
- bezpieczeństwo faktyczne
- pozytywny wizerunek
- oszczędności – zwłaszcza po 2018 roku! Zmiana przepisów UE



Podstawowe pojęcia związane
z ochroną danych osobowych

Dane osobowe (art. 6 UODO)





Warsztat – czy to dane osobowe?

- Krystyna Janecka Ogrodnia, NIP 342-12-31, Iksińska 1, Szczecin 08-223, podwykonawca opiekujący się terenami zielonymi na obszarze SM
- Nagrania z monitoringu w siedzibie SM
- E-mail służbowy pracownika Spółdzielni, zamieszczony na stronie internetowej
- Sam numer PESEL jednego z Członków SM
- Jana Olbrachta 13, Warszawa, zadłużenie mieszkańców względem SM – 45.000 zł
- Zadłużenie piętra V względem SM – 1.000 zł



Dane wrażliwe (art. 27 UODO)

Pochodzenie
rasowe lub
etniczne

Wyroki ,
orzeczenia o
ukaraniu i
mandatach
karnych oraz inne
wydane w
postępowaniu
sadowym lub
administracyjnym

Przynależność
wyznaniowa,
partyjna lub
związkowa

Nałogi, stan
zdrowia, kod
genetyczny lub
życie seksualne



Przekonania
religijne lub
filozoficzne

Poglądy polityczne

Przetwarzanie danych osobowych (art. 7 pkt. 2)

Jakiegolwiek operacje wykonywane na danych osobowych



Zbieranie
Utrwalanie
Przechowywanie
Opracowywanie



Zmienianie
Udostępnianie
Usuwanie

Administrator Danych (art. 7 ust. 4 UODO)

JEST NIM

- organ, jednostka organizacyjna, podmiot lub osoba (...) decydująca o celach i środkach przetwarzania danych osobowych
- SM Mszczonowska reprezentowana przez Zarząd

NIE JEST

- pracownik odpowiadający za ochronę danych osobowych (ABI)
- podmiot któremu powierzono przetwarzanie danych osobowych

Administrator Bezpieczeństwa Informacji

ABI Przemysław
Zegarek

tel.: 604 – 774 - 754

Mail:

przemyslaw.zegarek@lex-artist.pl



Zastępca ABI Ewelina
Wojciechowska

tel.: 530 – 488 - 326

Mail:

ewelina.wojciechowska@lex-artist.pl



Przykładowe zbiory danych osobowych

Pracownicy

Potencjalni
pracownicy

Członkowie
Spółdzielni

Osoby fizyczne
niezrzeszone w
Spółdzielni

Kontrahenci

Dane
kontaktowe

V filarów ochrony danych osobowych

I Legalność
przetwarzania

II Świadomość

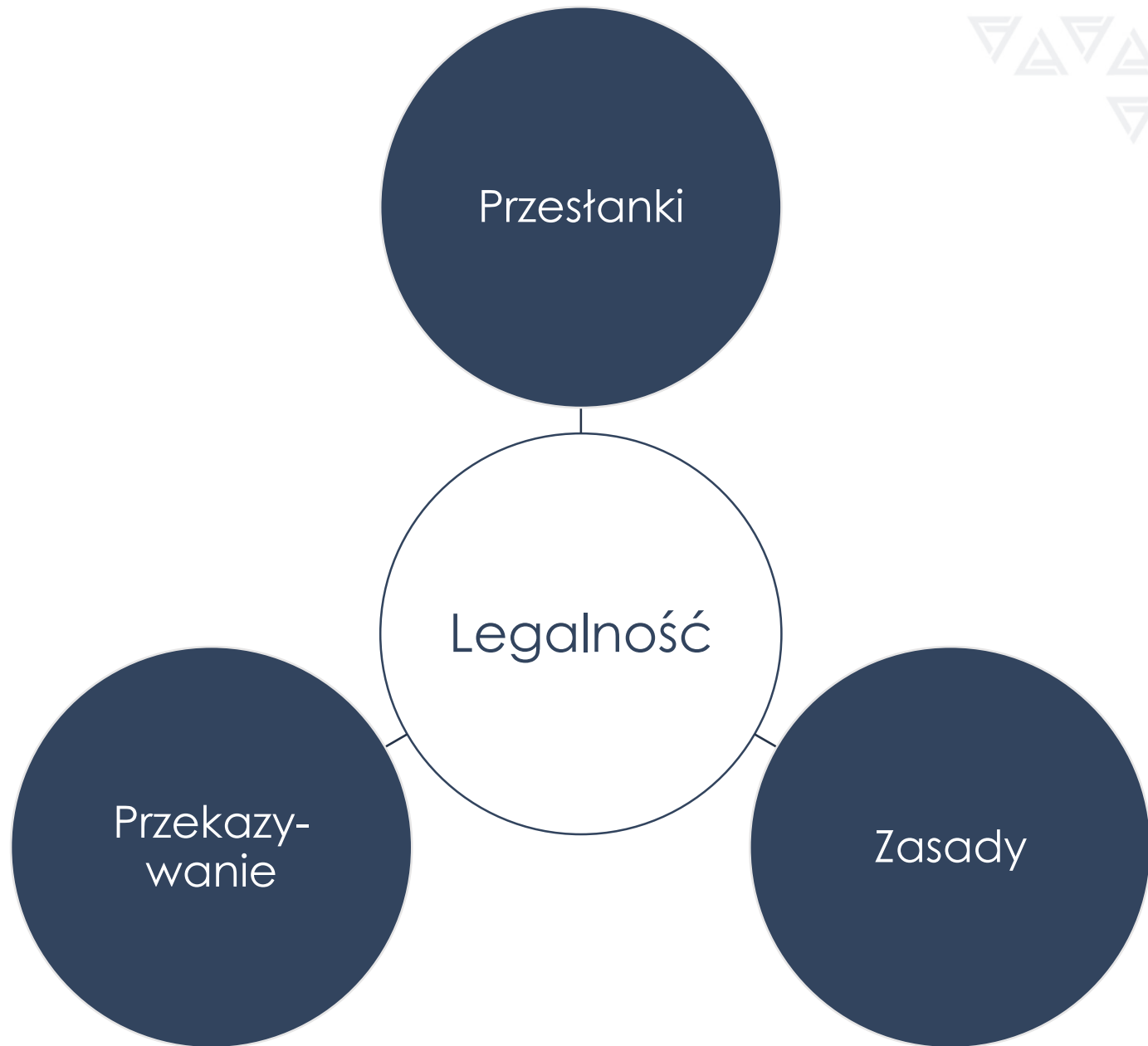
III
Zabezpieczenia

IV Rejestracja
zbiorów do
GIODO

V Obowiązek
informacyjny



I Filar – Legalność przetwarzania



Zasady przetwarzania danych osobowych

Zasada adekwatności

- Adekwatność danych w stosunku do celów, w jakich są przetwarzane.

Zasada celowości

- Zbieranie danych dla oznaczonych celów.

Zasada ograniczenia czasowego

- Nie należy przechowywać danych dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Uwaga na CV!

Przesłanki legalności przetwarzania danych zwykłych (art. 23 uodo)

Zgoda

Przepis
prawa

Realizacja
umowy

Dobro
publiczne

Prawnie
uspr. cel

Przekazywanie danych

Co legalizuje powierzenie / udostępnienie

- Powierzenie – pisemna umowa powierzenia
- Udostępnienie – jedna z przesłanek legalności

Przykłady powierzenia / udostępnienia

- Powierzenie – outsourcingi: marketing, obsługa kadr/płac/księgowości, IT (np. **Api-link**), ochrona, niszczenie/przechowywanie dokumentów
- Udostępnianie – policja, sąd, komornik, bank, ubezpieczenie



II Filar – Świadomość

Co się zmieniło od 2015 r.?

Obowiązek:

- zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych
- nadzorowania przestrzegania zasad określonych w dokumentacji

Wnioski dla SM Mszczonowska

Dostęp do danych = upoważnienie

- Każdy pracownik posiadający dostęp do zbioru danych osobowych musi posiadać upoważnienie
- Wnioski o nadanie upoważnień kieruj się do ZABI

Upoważnienie = szkolenie

- Każdy pracownik posiadający upoważnienie, musi zostać przeszkolony
- Szczególnie rekomendowane przeszkolenie pracowników: marketingu, kadr, płac, księgowości, IT



III Filar – Zabezpieczenia

Zabezpieczenia fizyczne

Szafy
zamykane na
klucz

Drzwi
zamykane na
klucz

Monitoring

Ochrona

Kraty w
oknach

SKD

Zabezpieczenia techniczne

1 użytkownik =
1 login i 1 hasło

Zmiana haseł
co 30 dni

Hasła min. 8
znaków w tym 2
znaki specjalne

Kopie
zapasowe

Systemy
firewall i anti-vir

...
Rozporządzenie
MSWiA z 2004 r.

Zabezpieczenia organizacyjne

Stworzenie Polityki
Bezpieczeństwa

Stworzenie Instrukcji
Zarządzania
Systemami
Informatycznymi

Nadawanie i
ewidencjonowanie
upoważnień

Stworzenie struktury
SODO



IV Filar – Rejestracja zbiorów do GODO

Obowiązek rejestracyjny do GIODO

The screenshot shows the e-GIODO web application. At the top, there is a navigation bar with links: Rej.ABI, Wyszukiwanie, Wyszukiwanie +, Wypełnianie wniosku, Wysyłanie/Sprawdzenie, and Twoja sprawa. Below the navigation bar, the header displays: Nr księgi: 097786 Data zatw./aktual.: 2011-05-30 Nr zgł.: 004323/2011 Data wpł.: 2011-05-11. The main content area has three tabs: A,B (selected), C, and D. Below the tabs, there is a section titled 'Część A.' with the label 'Nazwa zbioru danych osobowych:' and a text input field containing 'Osoby fizyczne niezrzeszone w spółdzielni'. Below this, there is a section titled 'Część B. Charakterystyka administratora danych'. Under this section, there is a list item '1. Wnioskodawca (administrator danych):' followed by a label 'Administrator:' and a text input field containing 'Spółdzielnia Mieszkaniowa "Mszczonowska"'. The background of the application has a subtle geometric pattern.

O czym pamiętać?

- Część zbiorów danych osobowych powinna zostać zarejestrowana na www.egiodo.giodo.gov.pl



V Filar – Obowiązek Informacyjny

Obowiązek informacyjny – art. 24 UODO

adres i pełna
nazwa ADO

cel zbierania
danych

odbiorcy danych
(lub kategorie
odbiorców)

prawo dostępu do
treści danych oraz
możliwość ich
poprawiania

dobrowolność albo
obowiązek podania
danych

Obowiązek informacyjny w SM

Mszczonowska

Kiedy zachować szczególną uwagę?

- Monitoring
- Konkursy i akcje Klubu Osiedlowego

Kiedy jesteśmy zwolnieni z obowiązku informacyjnego?

- Kiedy osoba której dane dotyczą posiada już wszystkie te informacje
- Jeśli powierzamy dane osobowe



Podstawy i rodzaje odpowiedzialności

Administracyjna

- ustawa o ochronie danych osobowych
- kodeks postępowania administracyjnego

Dyscyplinarna

- ustawa o ochronie danych osobowych
- kodeks pracy (art. 100)

Cywilna

- kodeks cywilny (art. 23)
- ustawa o prawie autorskim i prawach pokrewnych

Karna

- ustawa o ochronie danych osobowych
- kodeks karny
- kodeks postępowania karnego

Odpowiedzialność karna (art. 49-54a UODO)



nieuprawnione lub niedopuszczalne przetwarzanie danych osobowych w zbiorze (od 2 [dane zwykłe] do 3 lat [dane wrażliwe] pozbawienia wolności)



udostępnienie lub umożliwienie dostępu do danych osobowych osobom nieupoważnionym (od roku [nieumyślnie] do dwóch lat)



naruszenie obowiązku zabezpieczenia danych (do roku)



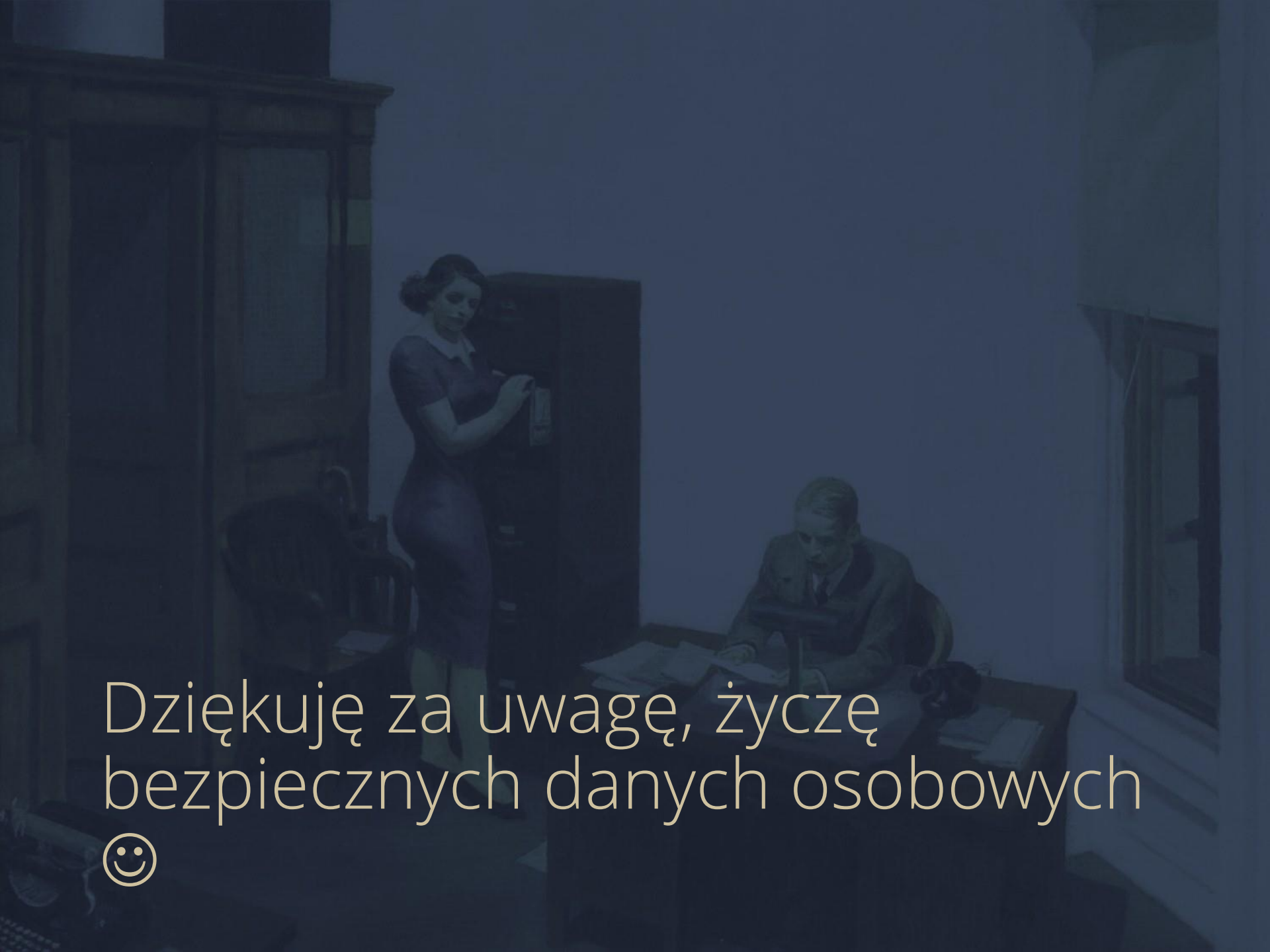
niezgłoszenie zbioru danych do rejestracji (do roku)



niedopełnienie obowiązku informacyjnego (do roku)



udaremnianie lub utrudnianie wykonania czynności kontrolnej przez inspektora



Dziękuję za uwagę, życzę
bezpiecznych danych osobowych

