Projekt realizowany w ramach programu Obywatele dla Demokracji, finansowanego z Funduszy EOG oraz ze środków Trust Civil Society in Central and Eastern Europe.

WATCHDOG ZMIENIAMY SYSTEMOWO

Projekt realizowany jest przez Sieć Obywatelską Watchdog Polska oraz partnerów:

Projekt realizowany w ramach programu Obywatele dla Demokracji, finansowanego z Funduszy EOG oraz ze środków Trust Civil Society in Central and Eastern Europe.

WATCHDOG ZMIENIAMY SYSTEMOWO

WEBINARIUM

OCHRONA DANYCH OSOBOWYCH w organizacjach pozarządowych z uwzględnieniem zmian obowiązujących od 1 stycznia 2015 r.

ekspertka: Agnieszka Majdzińska

host: Dorota Kostowska

Warszawa 06.03.2015

Projekt realizowany jest przez Sieć Obywatelską Watchdog Polska oraz partnerów:

O czym dziś...

1. **Podstawy prawne dotyczące ochrony danych osobowych**
2. **Podstawowe pojęcia**
3. **Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO**

WATCHDOG
ZMIENIAMY
SYSTEMOWO

O czym dziś...

4 **Kontrole**

5 **Przydatne informacje**

6 **Pytania**

WATCHDOG
ZMIENIAMY
SYSTEMOWO

1 Podstawy prawne dotyczące ochrony danych osobowych

WATCHDOG ZMIENIAMY SYSTEMOWO

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.; **nowy tekst jednolity**: Dz. U. z 2014 r., poz. 1182 z późn. zm. wprowadzonymi ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, Dz. U. z 2014 r., poz. 1662)

1 Podstawy prawne dotyczące ochrony danych osobowych

WATCHDOG ZMIENIAMY SYSTEMOWO

Przepisy wykonawcze:

a) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

b) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz. 1536)

c) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014 r., poz. 1934)

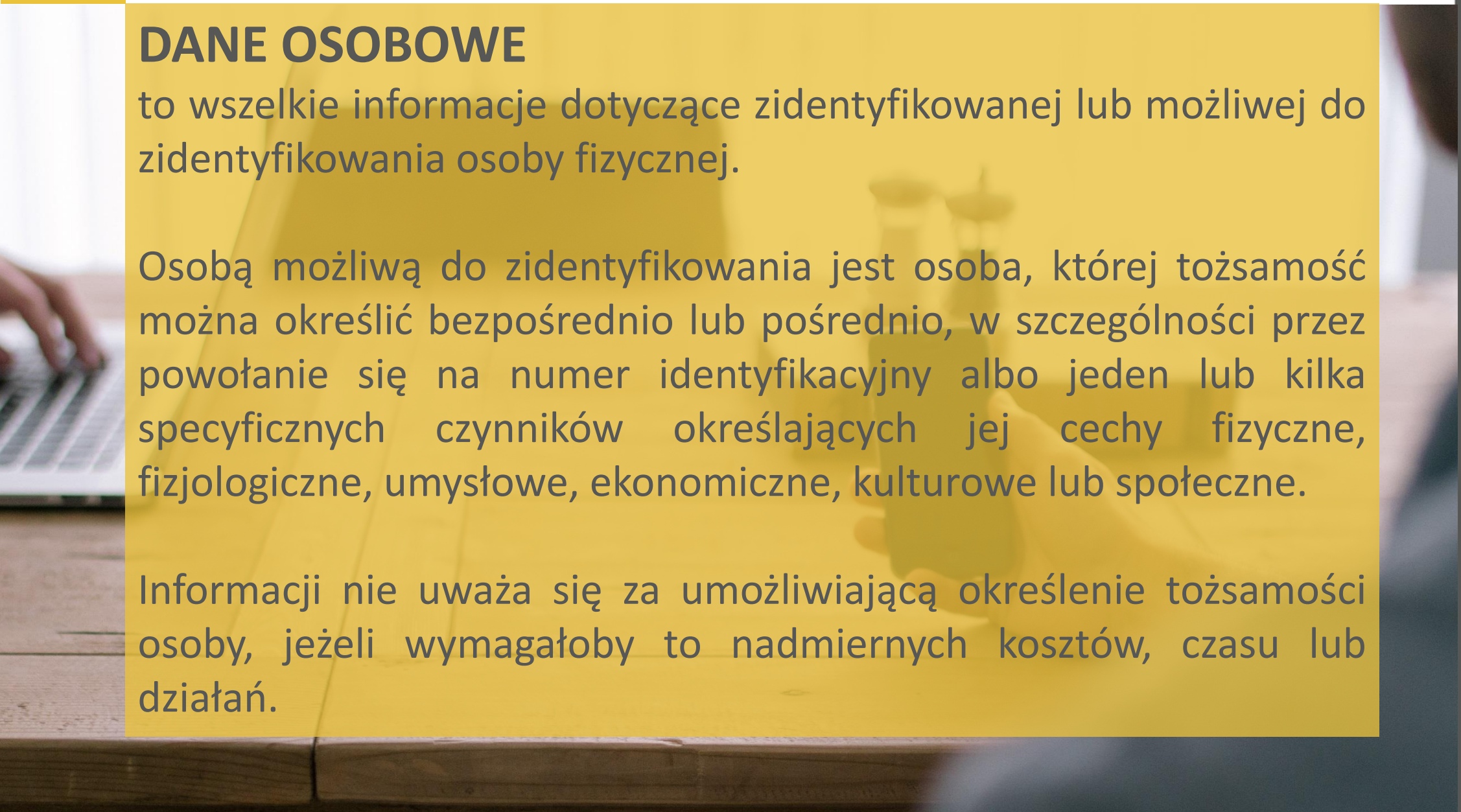
1 Podstawy prawne dotyczące ochrony danych osobowych

WATCHDOG ZMIENIAMY SYSTEMOWO

Regulacje wewnętrzne organizacji pozarządowej:

a) Polityka Bezpieczeństwa
b) Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

2 Podstawowe pojęcia



DANE OSOBOWE

to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

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

Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

WATCHDOG ZMIENIAMY SYSTEMOWO

2 Podstawowe pojęcia

DANE OSOBOWE
dzielą się na:

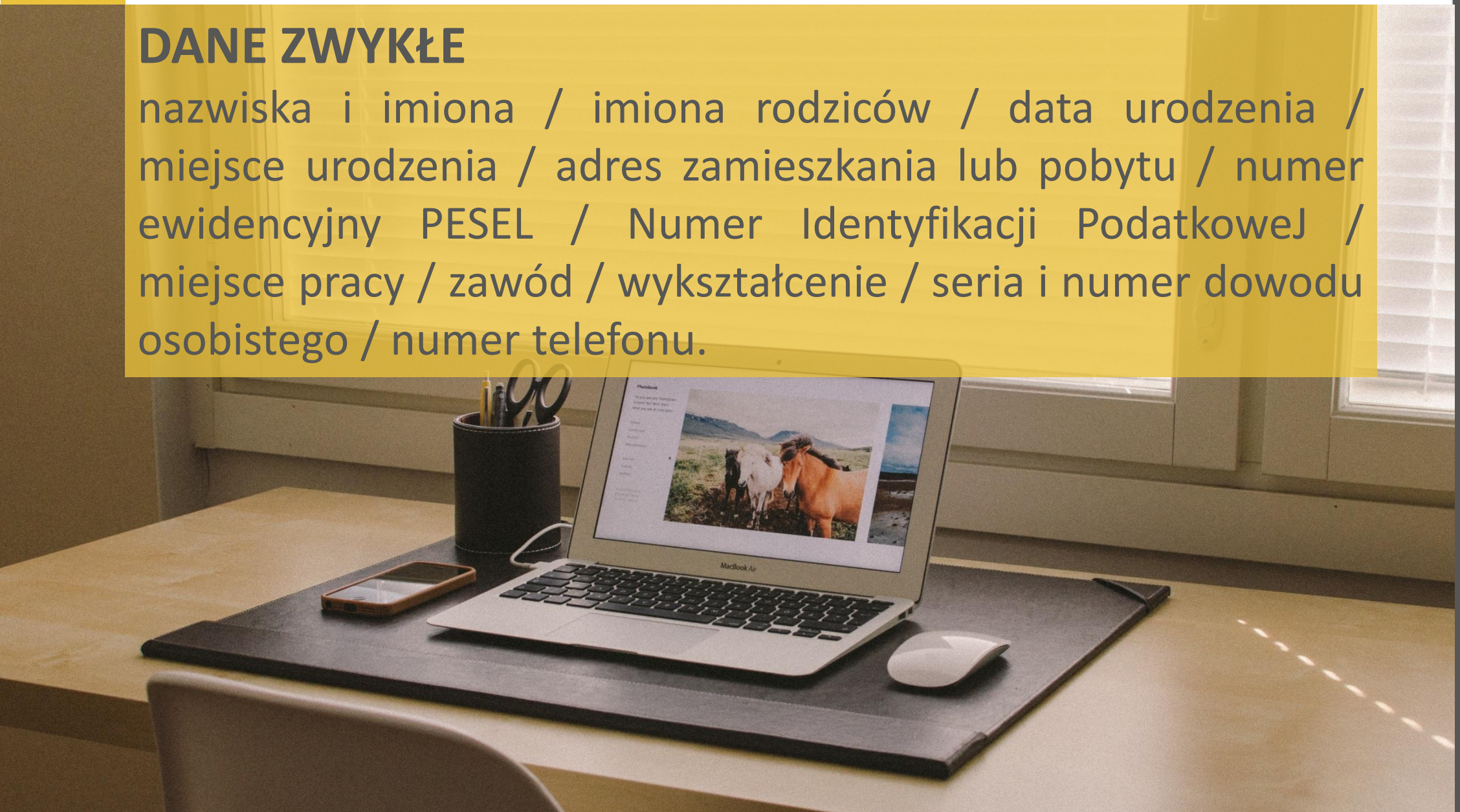
dane tzw. „zwykłe”,

dane wrażliwe/sensytywne.

2 Podstawowe pojęcia

DANE ZWYKŁE

nazwiska i imiona / imiona rodziców / data urodzenia / miejsce urodzenia / adres zamieszkania lub pobytu / numer ewidencyjny PESEL / Numer Identyfikacji PodatkoweJ / miejsce pracy / zawód / wykształcenie / seria i numer dowodu osobistego / numer telefonu.



WATCHDOG ZMIENIAMY SYSTEMOWO

2 Podstawowe pojęcia

WATCHDOG ZMIENIAMY SYSTEMOWO

DANE ZWYKŁE

tzw. „inne dane”, o których mówi ustawa:

adres IP komputera / adres poczty elektronicznej / numer rachunku bankowego / numer formularza rekrutacyjnego do projektu (wyrażony np.: kodem literowo-cyfrowym) / imię i nazwisko oraz telefon kontaktowy do osoby, którą należy powiadomić w razie wypadku (w kwestionariuszu osobowym pracownika organizacji pozarządowej) / imię i nazwisko oraz telefon kontaktowy do osoby pełnoletniej, która jest rodzicem lub opiekunem prawnym małoletniego dziecka (jeśli organizacja pozarządowa realizuje działania adresowane do dzieci albo młodzieży szkolnej) / ...

2 Podstawowe pojęcia

WATCHDOG ZMIENIAMY SYSTEMOWO

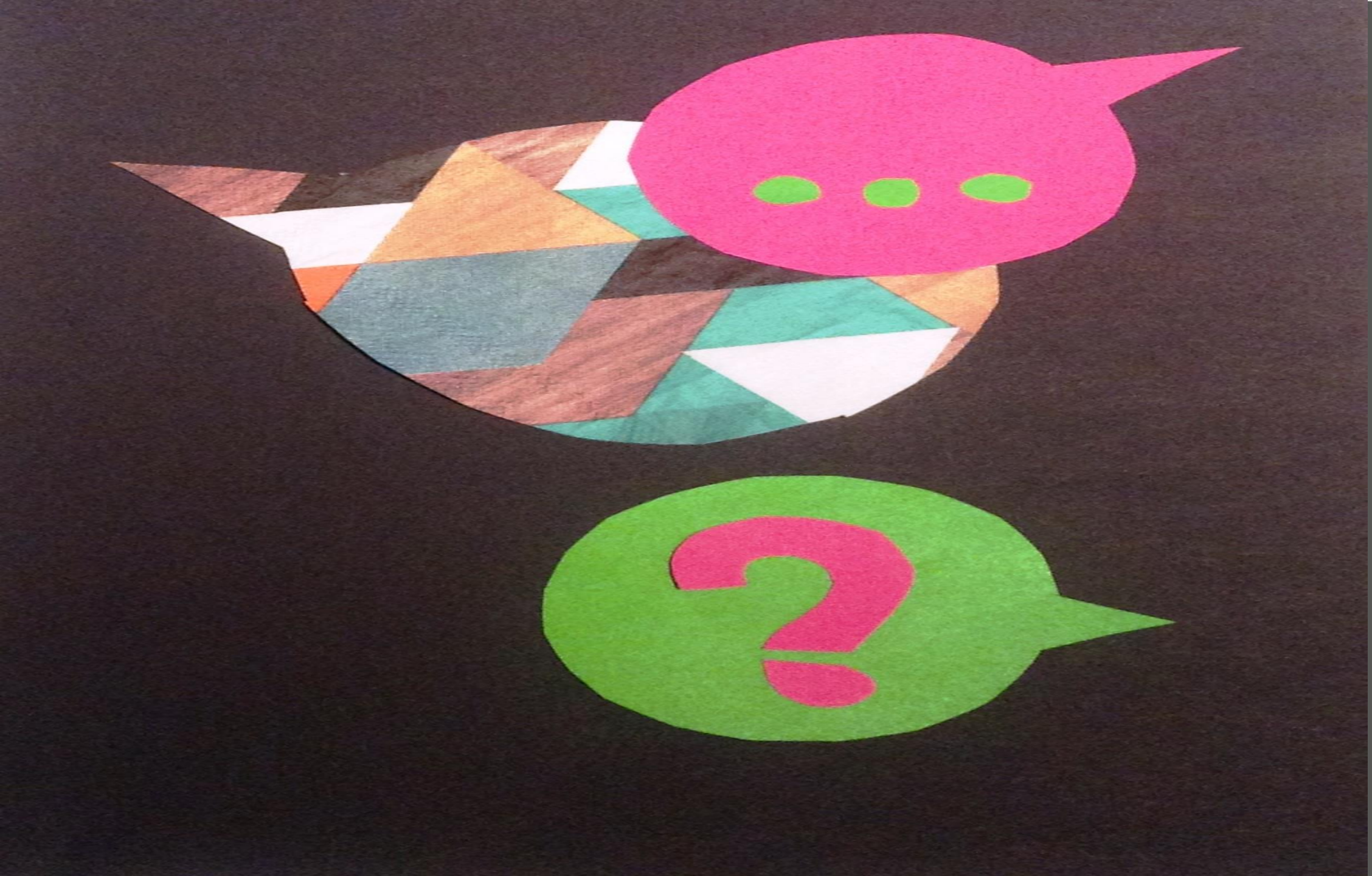
DANE WRAŻLIWE/SENSYTYWNE

ujawniają bezpośrednio lub w kontekście:
pochodzenie rasowe / etniczne / poglądy polityczne / przekonania religijne / filozoficzne /

przynależność wyznaniową / partyjną / związkową /

stan zdrowia / kod genetyczny / nałogi / życie seksualne

dotyczą też: skazań / mandatów karnych / orzeczeń o ukaraniu / innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.



WATCHDOG
ZMIENIAMY
SYSTEMOWO

2 Podstawowe pojęcia

WATCHDOG ZMIENIAMY SYSTEMOWO

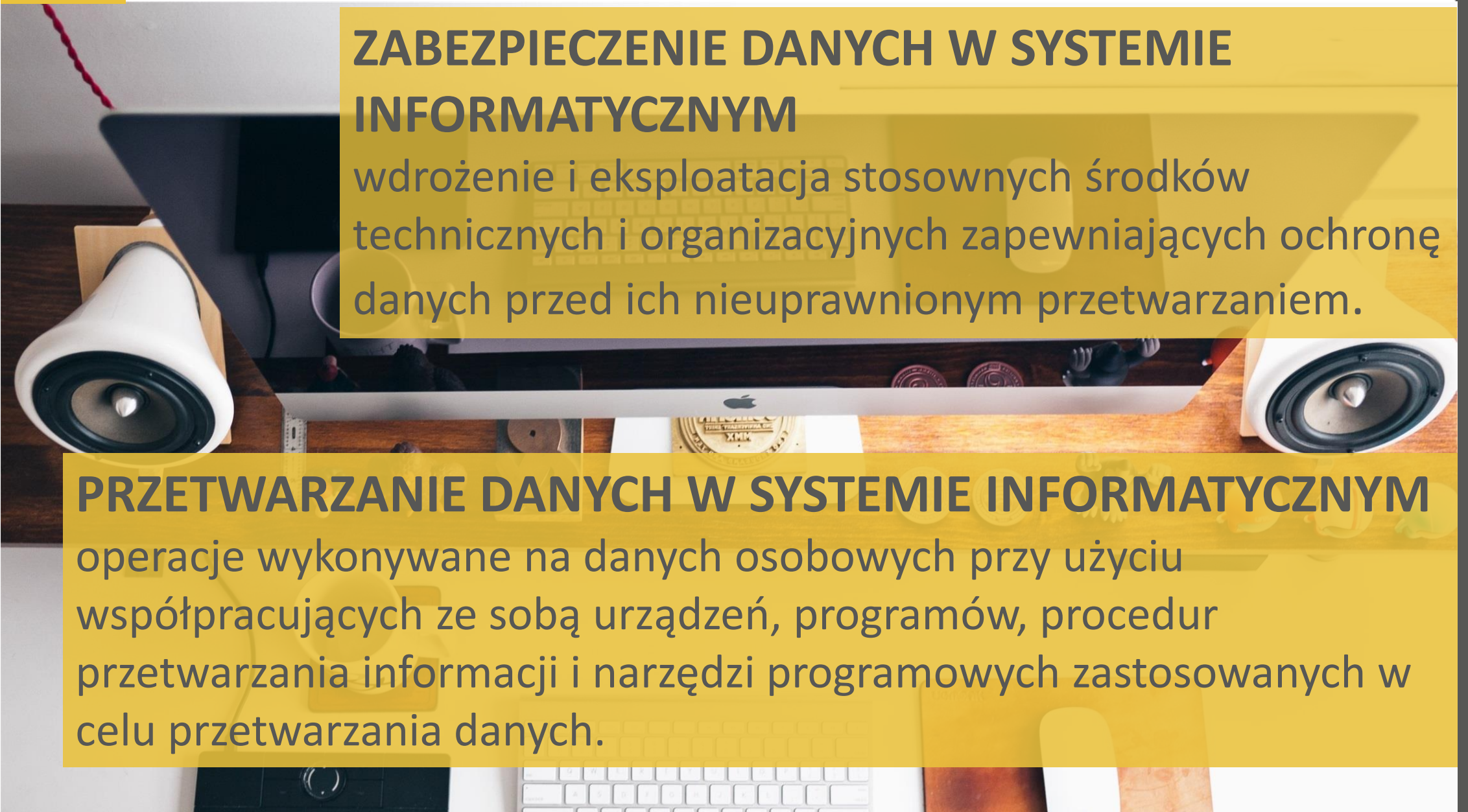
ZBIÓR DANYCH

to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

ZGODA OSOBY, KTÓREJ DANE DOTYCZĄ

to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

2 Podstawowe pojęcia



ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM

wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

PRZETWARZANIE DANYCH W SYSTEMIE INFORMATYCZNYM

operacje wykonywane na danych osobowych przy użyciu współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

2 Podstawowe pojęcia

WATCHDOG ZMIENIAMY SYSTEMOWO

PRZETWARZANIE DANYCH

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

USUWANIE DANYCH

zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

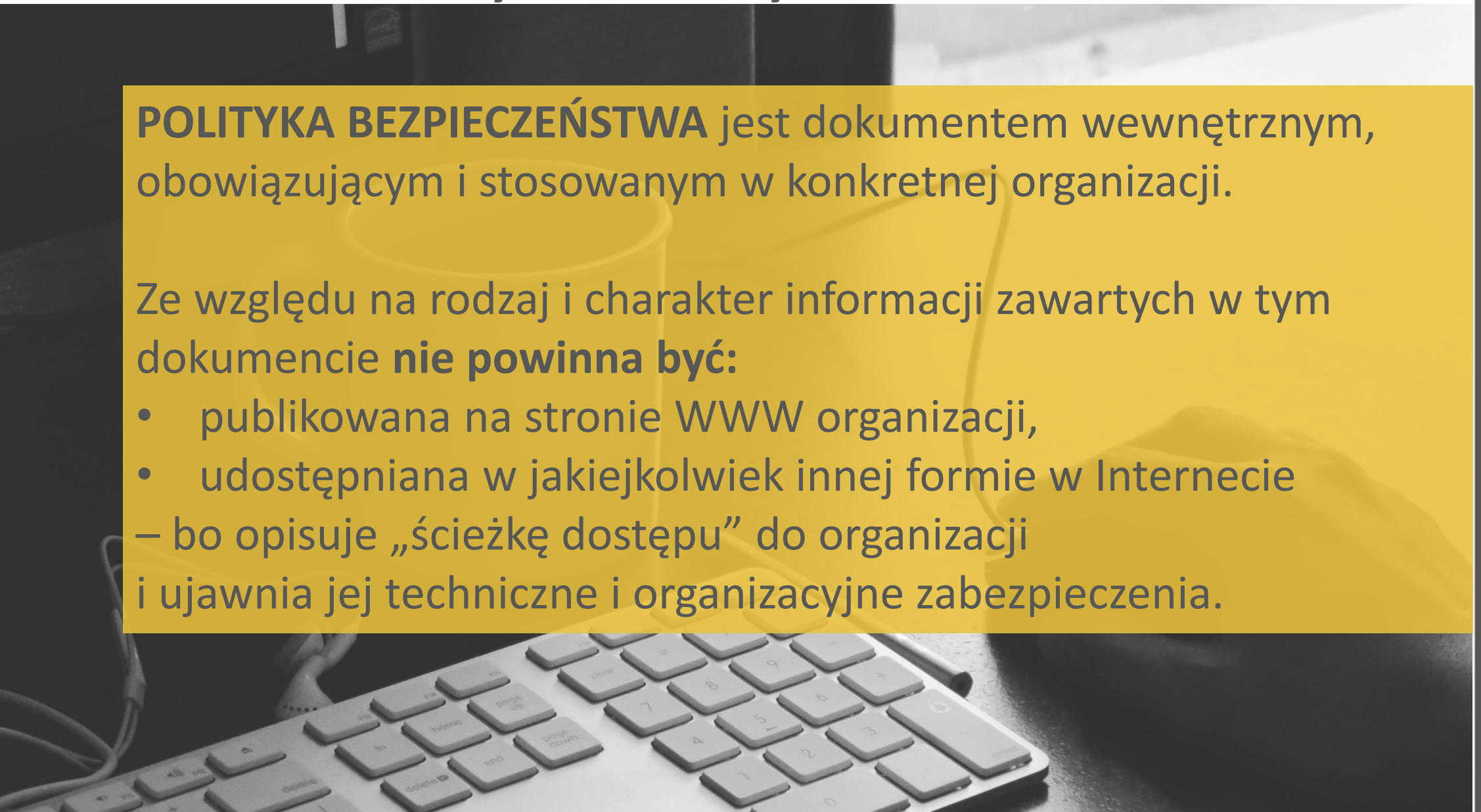
WATCHDOG ZMIENIAMY SYSTEMOWO

POLITYKA BEZPIECZEŃSTWA dokument wewnętrzny regulujący i opisujący zasady przetwarzania danych osobowych w organizacji pozarządowej. Zawiera:

1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4. sposób przepływu danych pomiędzy poszczególnymi systemami;
5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

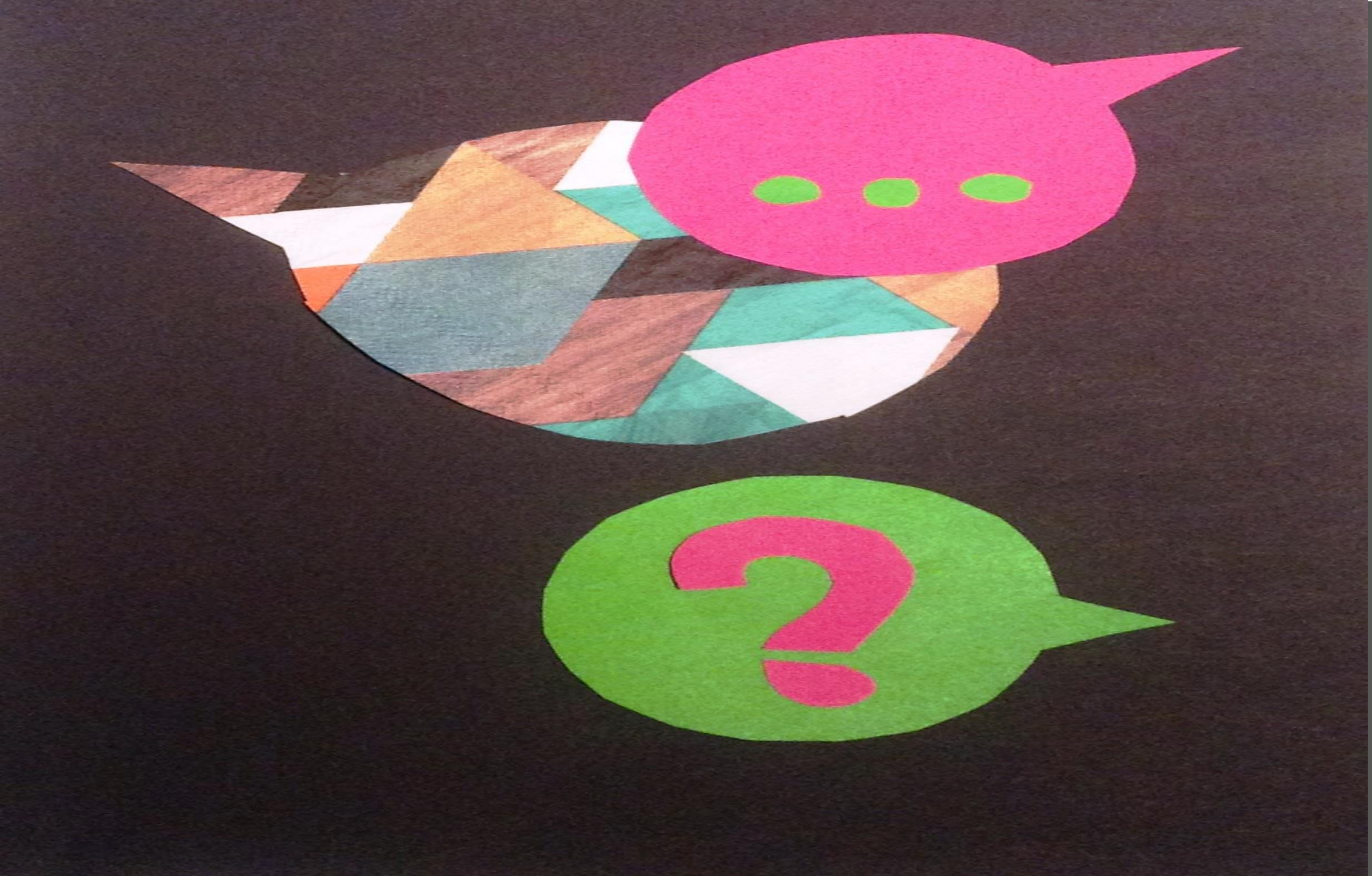


POLITYKA BEZPIECZEŃSTWA jest dokumentem wewnętrznym, obowiązującym i stosowanym w konkretnej organizacji.

Ze względu na rodzaj i charakter informacji zawartych w tym dokumencie **nie powinna być:**

- publikowana na stronie WWW organizacji,
- udostępniana w jakiejkolwiek innej formie w Internecie

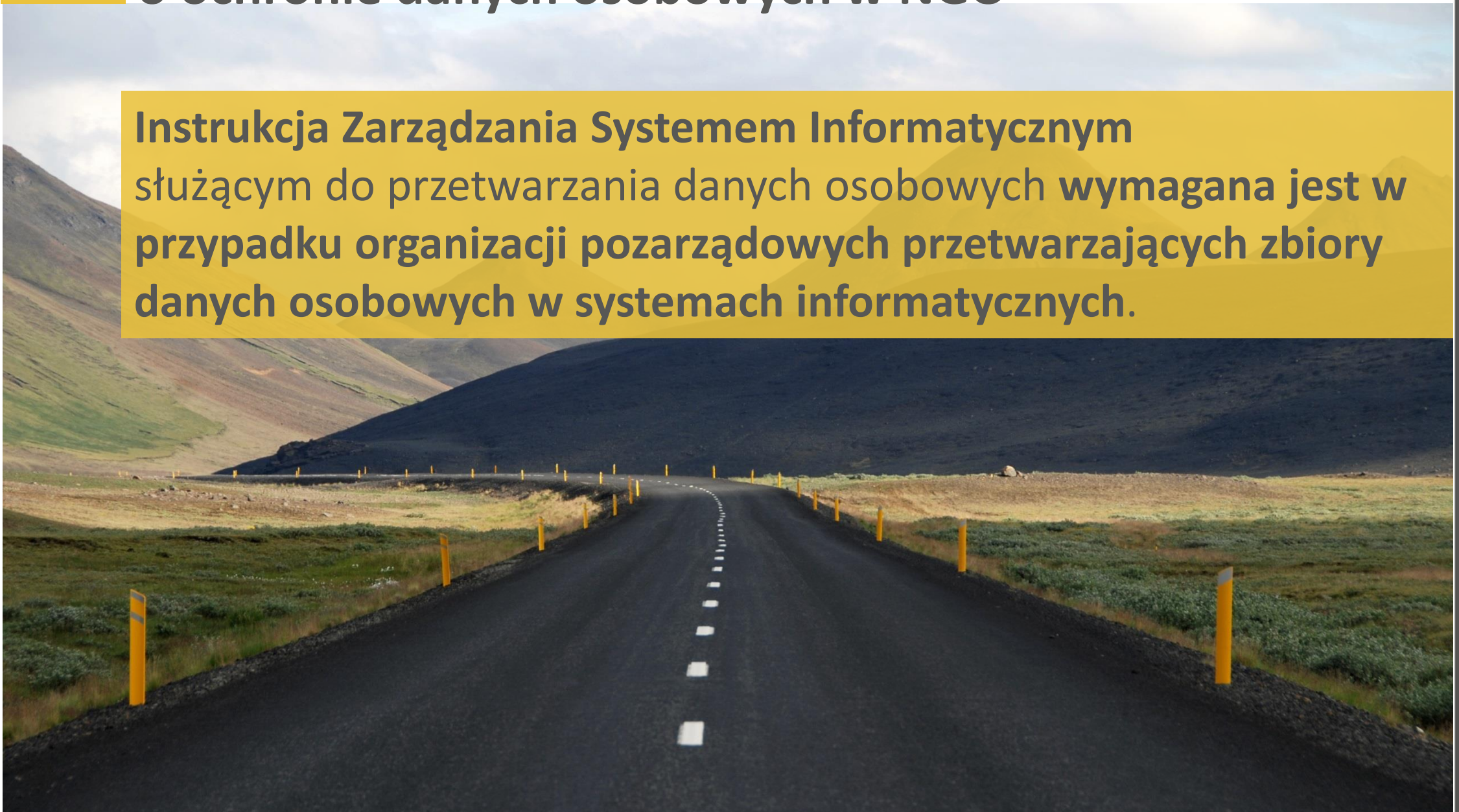
– bo opisuje „ścieżkę dostępu” do organizacji i ujawnia jej techniczne i organizacyjne zabezpieczenia.



WATCHDOG
ZMIENIAMY
SYSTEMOWO

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

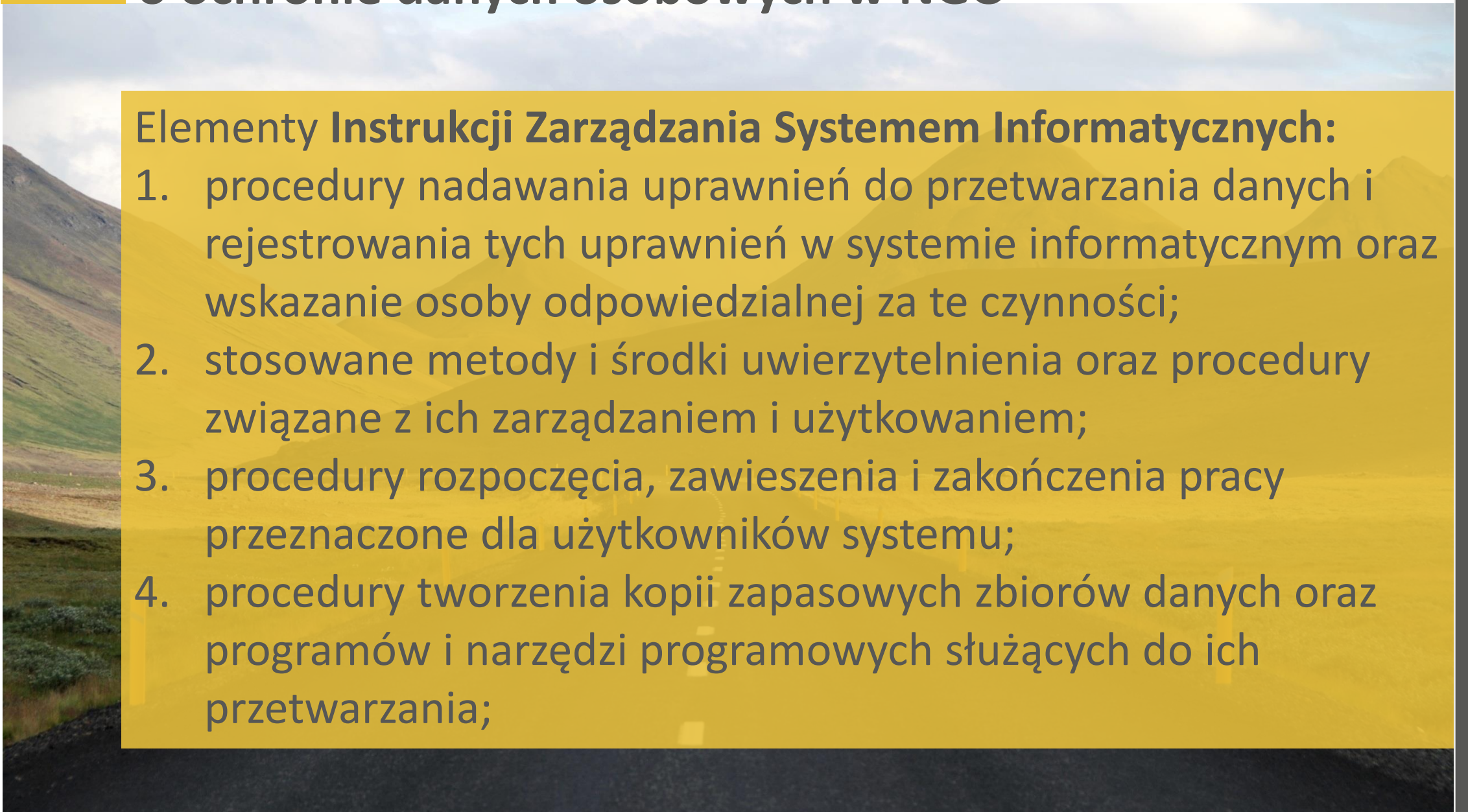
WATCHDOG ZMIENIAMY SYSTEMOWO



Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych **wymagana jest w przypadku organizacji pozarządowych przetwarzających zbiory danych osobowych w systemach informatycznych**.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



Elementy **Instrukcji Zarządzania Systemem Informatycznych:**

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

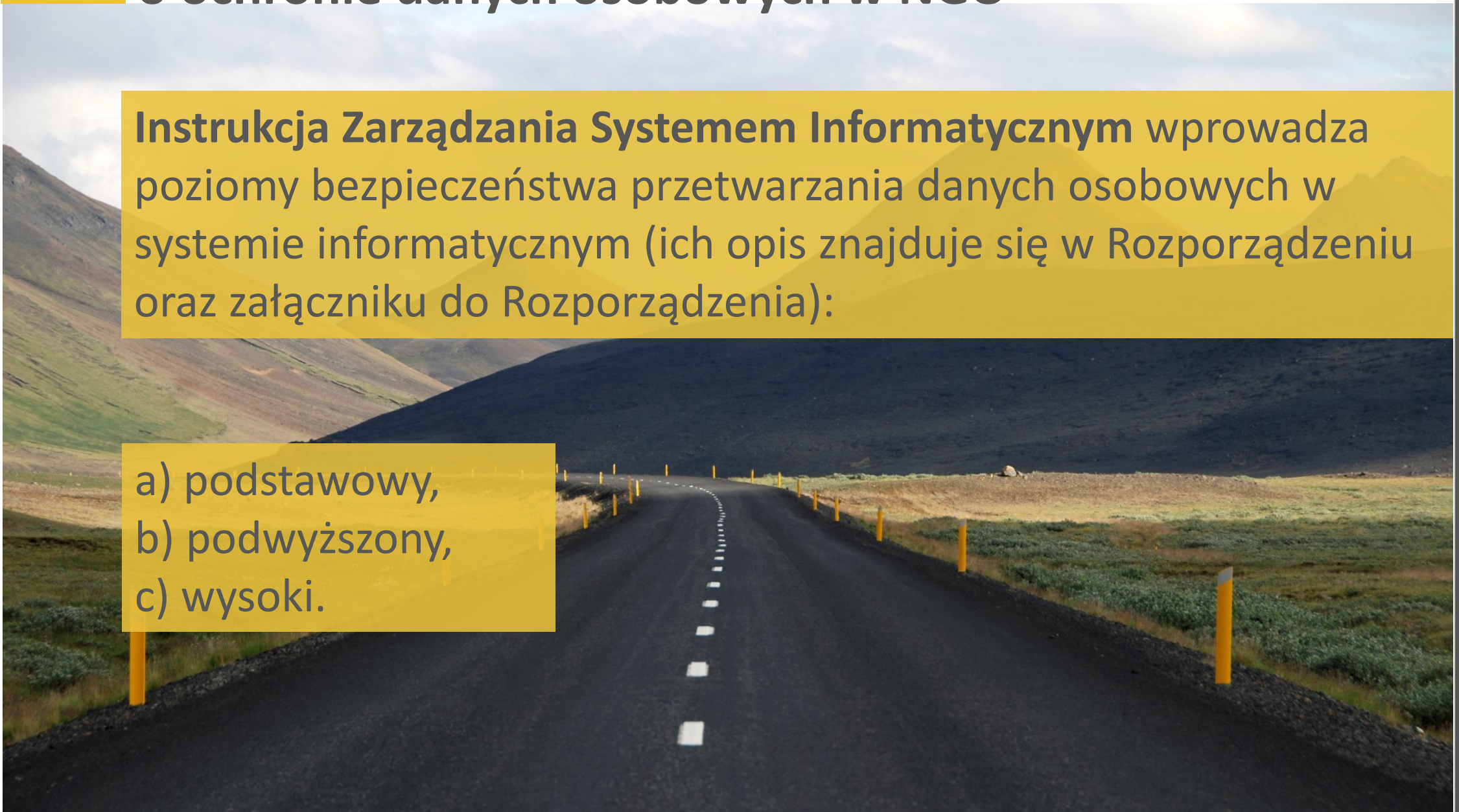
WATCHDOG ZMIENIAMY SYSTEMOWO

Elementy **Instrukcji Zarządzania Systemem Informatycznym:**

5. sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych (o których mowa powyżej);
6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
7. sposób realizacji wymogów informacji o odbiorcach (w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych), którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych);
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

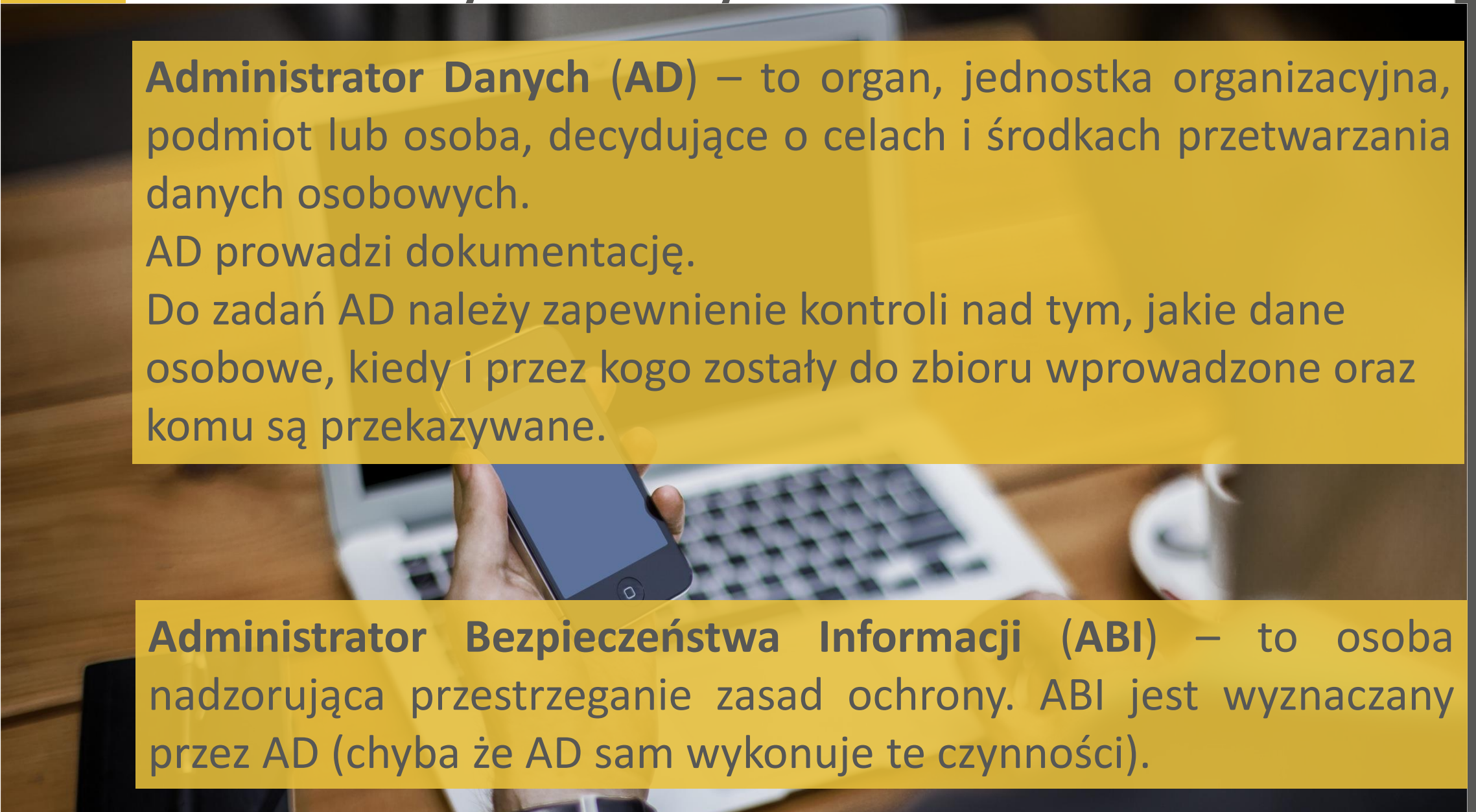


Instrukcja Zarządzania Systemem Informatycznym wprowadza poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym (ich opis znajduje się w Rozporządzeniu oraz załączniku do Rozporządzenia):

a) podstawowy,
b) podwyższony,
c) wysoki.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



Administrator Danych (AD) – to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych.
AD prowadzi dokumentację.
Do zadań AD należy zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Administrator Bezpieczeństwa Informacji (ABI) – to osoba nadzorująca przestrzeganie zasad ochrony. ABI jest wyznaczany przez AD (chyba że AD sam wykonuje te czynności).

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

W przypadku przetwarzania danych osobowych w systemie informatycznym konieczne jest powołanie **Administratora Systemu Informatycznego** (**ASI**) – czyli osoby nadzorującej przestrzeganie zasad ochrony w związku z przetwarzaniem danych w systemie informatycznym.

Administrator Danych (**AD**) – to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych.
AD jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
AD prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.
Do zadań AD należy jednak przede wszystkim zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Administrator Bezpieczeństwa Informacji (**ABI**) – to osoba nadzorująca przestrzeganie zasad ochrony. ABI jest wyznaczany przez AD (chyba że AD sam wykonuje te czynności).

WATCHDOG
ZMIENIAMY
SYSTEMOWO

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Od 1 stycznia 2015 r. Administrator Danych (AD), którym jest organizacja pozarządowa musi zdecydować, czy:

powołać administratora bezpieczeństwa informacji (ABI) i zgłosić go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO)?

nie powoływać ABI?

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Administrator Danych (AD) powołuje administratora bezpieczeństwa informacji (ABI) i zgłasza go do rejestracji GIODO:

AD w zakresie zabezpieczenia danych osobowych może:

- powołać ABI,
- powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania jego podstawowych obowiązków.

AD musi zapewnić środki i organizacyjną odrębność ABI niezbędną do niezależnego wykonywania przez niego przypisanych mu zadań.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Administrator Danych (AD) powołuje administratora bezpieczeństwa informacji (ABI) i zgłasza go do rejestracji GIODO:

AD w zakresie dotyczącym rejestracji zbiorów danych osobowych:

- ma obowiązek zgłoszenia do rejestracji GIODO jedynie zbiorów obejmujących **dane wrażliwe/sensytywne** (pod warunkiem, że ABI zgłoszony do rejestracji GIODO nie został wykreślony z rejestru administratorów bezpieczeństwa informacji prowadzonego przez GIODO);

- ma obowiązek zgłoszenia do rejestracji GIODO: faktu powołania ABI, odwołania ABI, zmian informacji objętych zgłoszeniem.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Administrator Danych (AD) nie powołuje administratora bezpieczeństwa informacji (ABI) i sam wykonuje zadania ABI:

Zadania:

nadzorowanie opracowania i aktualizowania dokumentacji, która opisuje:

- sposób przetwarzania danych,
- środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Administrator Danych (AD) nie powołuje administratora bezpieczeństwa informacji (ABI) i sam wykonuje zadania ABI:

W zakresie dotyczącym rejestracji zbiorów danych osobowych AD jest obowiązany zgłosić do rejestracji GIODO zbiór danych obejmujących:

- dane zwykłe – z wyjątkiem zbiorów ustawowo zwolnionych z rejestracji*;
- dane wrażliwe/sensytywne.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

AD są zwolnieni z obowiązku rejestracji zbioru danych gdy dane są:

- przetwarzane wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych;
- przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane wrażliwe/sensytywne.

W przypadku przetwarzania danych osobowych w systemie informatycznym konieczne jest powołanie **Administratora Systemu Informatycznego** (**ASI**) – czyli osoby nadzorującej przestrzeganie zasad ochrony w związku z przetwarzaniem danych w systemie informatycznym.

Taki stan rzeczy obowiązywał do 31 grudnia 2014 r.
Od 1 stycznia 2015 r. Administrator Danych (AD), którym jest organizacja pozarządowa reprezentowana w sposób określony w Statucie i dokumentach rejestrowych pochodzących z Krajowego Rejestru Sądowego, musi zdecydować, czy:
1) powołać administratora bezpieczeństwa informacji (ABI) i zgłosić go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO)?
2) nie powoływać ABI?

Kolejne slajdy przedstawią dalszy sposób postępowania, w zależności od wybranej możliwości:

1. **Administrator Danych (AD) powołuje administratora bezpieczeństwa informacji** (ABI) **i zgłasza go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych** (GIODO):

Znowelizowana ustawa o ochronie danych osobowych:
a) w zakresie zabezpieczenia danych osobowych daje AD możliwość:
+ powołania ABI i (w razie konieczności) zastępców ABI – *pamiętać jednak należy, że ABI musi podlegać bezpośrednio kierownikowi jednostki organizacyjnej*,
+ powierzenia ABI wykonywania innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania jego podstawowych obowiązków

- nakładając jednocześnie na AD konieczność zapewnienia środków i organizacyjnej odrębności ABI niezbędnej do niezależnego wykonywania przez niego przypisanych mu zadań;

b) w zakresie dotyczącym rejestracji zbiorów danych osobowych:
+ obowiązek zgłoszenia do rejestracji GIODO jedynie zbiorów obejmujących **dane wrażliwe/sensytywne** (pod warunkiem, że ABI zgłoszony do rejestracji GIODO nie został wykreślony z rejestru administratorów bezpieczeństwa informacji prowadzonego przez GIODO);
+ obowiązek zgłoszenia do rejestracji GIODO: powołania ABI (w terminie 30 dni od jego powołania), odwołania ABI (w terminie 30 dni od jego odwołania), zmian informacji objętych zgłoszeniem (w terminie 14 dni od dnia zmiany).

2. **AD nie powołuje ABI** - w tej sytuacji AD sam wykonuje zadania ABI, do których należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
- nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad określonych w tej dokumentacji;

- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

W zakresie dotyczącym rejestracji zbiorów danych osobowych AD jest obowiązany zgłosić do rejestracji GIODO zbiór danych obejmujących:

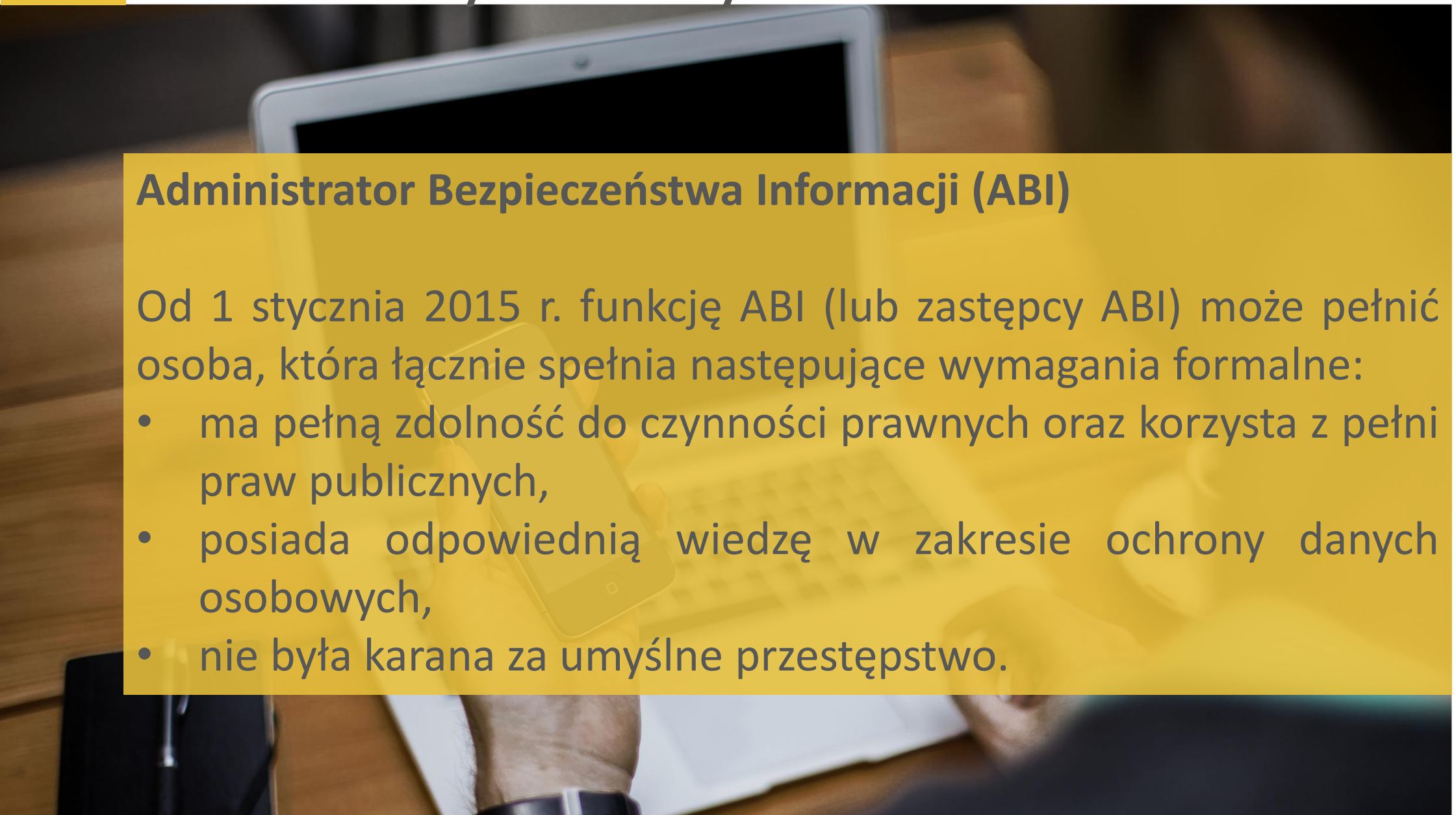
- dane zwykłe – z wyjątkiem zbiorów ustawowo zwolnionych z rejestracji*;
- dane wrażliwe/sensytywne.

* Z obowiązku rejestracji zbioru danych zwolnieni są AD:

- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
- powszechnie dostępnych;
- przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane wrażliwe/sensytywne (czyli dane zwykłe przetwarzane w formie papierowej).

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



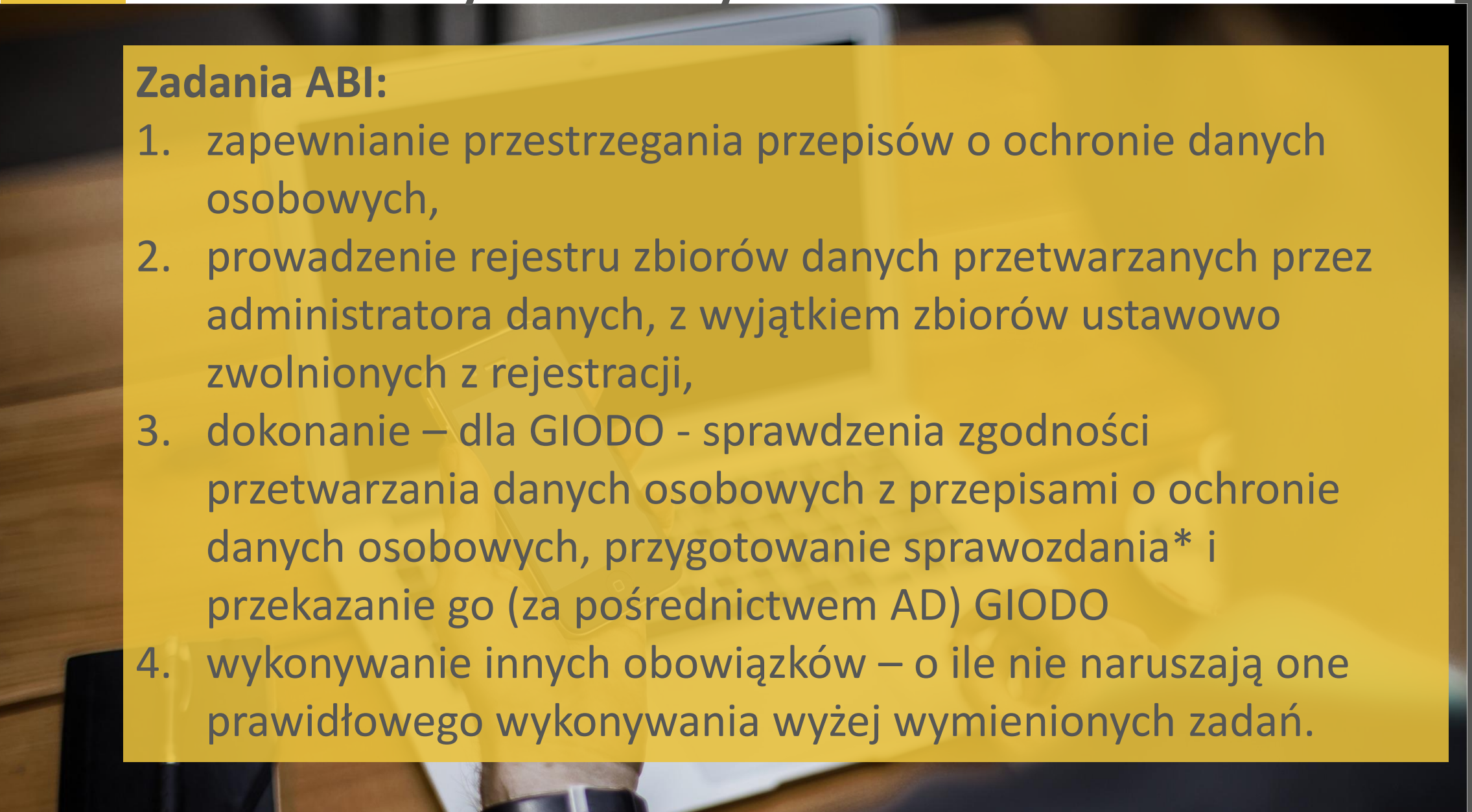
Administrator Bezpieczeństwa Informacji (ABI)

Od 1 stycznia 2015 r. funkcję ABI (lub zastępcy ABI) może pełnić osoba, która łącznie spełnia następujące wymagania formalne:

- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- nie była karana za umyślne przestępstwo.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



Zadania ABI:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych,
2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów ustawowo zwolnionych z rejestracji,
3. dokonanie – dla GIODO - sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, przygotowanie sprawozdania* i przekazanie go (za pośrednictwem AD) GIODO
4. wykonywanie innych obowiązków – o ile nie naruszają one prawidłowego wykonywania wyżej wymienionych zadań.

WATCHDOG ZMIENIAMY SYSTEMOWO

Administrator Bezpieczeństwa Informacji (ABI)

Od 1 stycznia 2015 r. funkcję ABI (lub zastępcy ABI) może pełnić osoba, która łącznie spełnia następujące wymagania formalne:
- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
- nie była karana za umyślne przestępstwo.

Do zadań ABI należy:
1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla AD;
- nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające

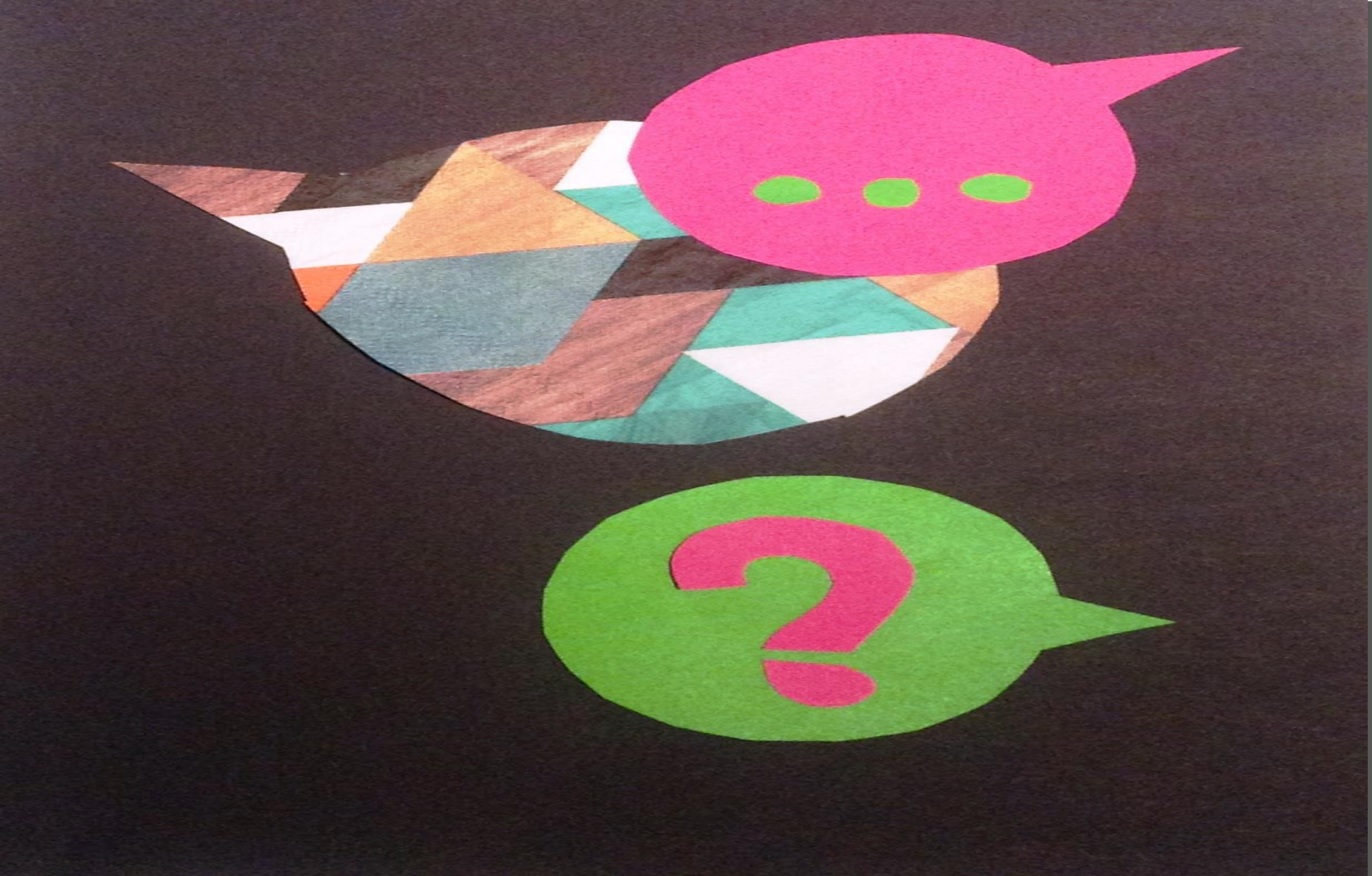
ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad określonych w tej dokumentacji;
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów ustawowo zwolnionych z rejestracji, zawierającego:
- nazwę zbioru;
- oznaczenie AD i adres jego siedziby, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej (REGON), jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru;
- cel przetwarzania danych;
- sposób zbierania oraz udostępniania danych;
- informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane;
- informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego;

WATCHDOG
ZMIENIAMY
SYSTEMOWO

3) dokonanie – dla GIODO w wyznaczonym przez niego zakresie i terminie – sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, przygotowanie sprawozdania* i przekazanie go (za pośrednictwem AD) GIODO – **dokonanie sprawdzenia przez ABI nie wyłącza prawa GIODO do przeprowadzenia kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych**;
4) wykonywanie innych obowiązków – o ile nie naruszają one prawidłowego wykonywania wyżej wymienionych zadań.

* Sprawozdanie dla AD powinno zawierać: **1)** oznaczenie AD i adres jego siedziby; **2)** imię i nazwisko ABI; **3)** wykaz czynności podjętych przez ABI w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach; **4)** datę rozpoczęcia i zakończenia sprawdzenia; **5)** określenie przedmiotu i zakresu sprawdzenia; **6)** opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych; **7)** stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem; **8)** wyszczególnienie załączników stanowiących składową część sprawozdania; **9)** podpis ABI, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy ABI na każdej stronie sprawozdania; **10)** datę i miejsce podpisania sprawozdania przez ABI.

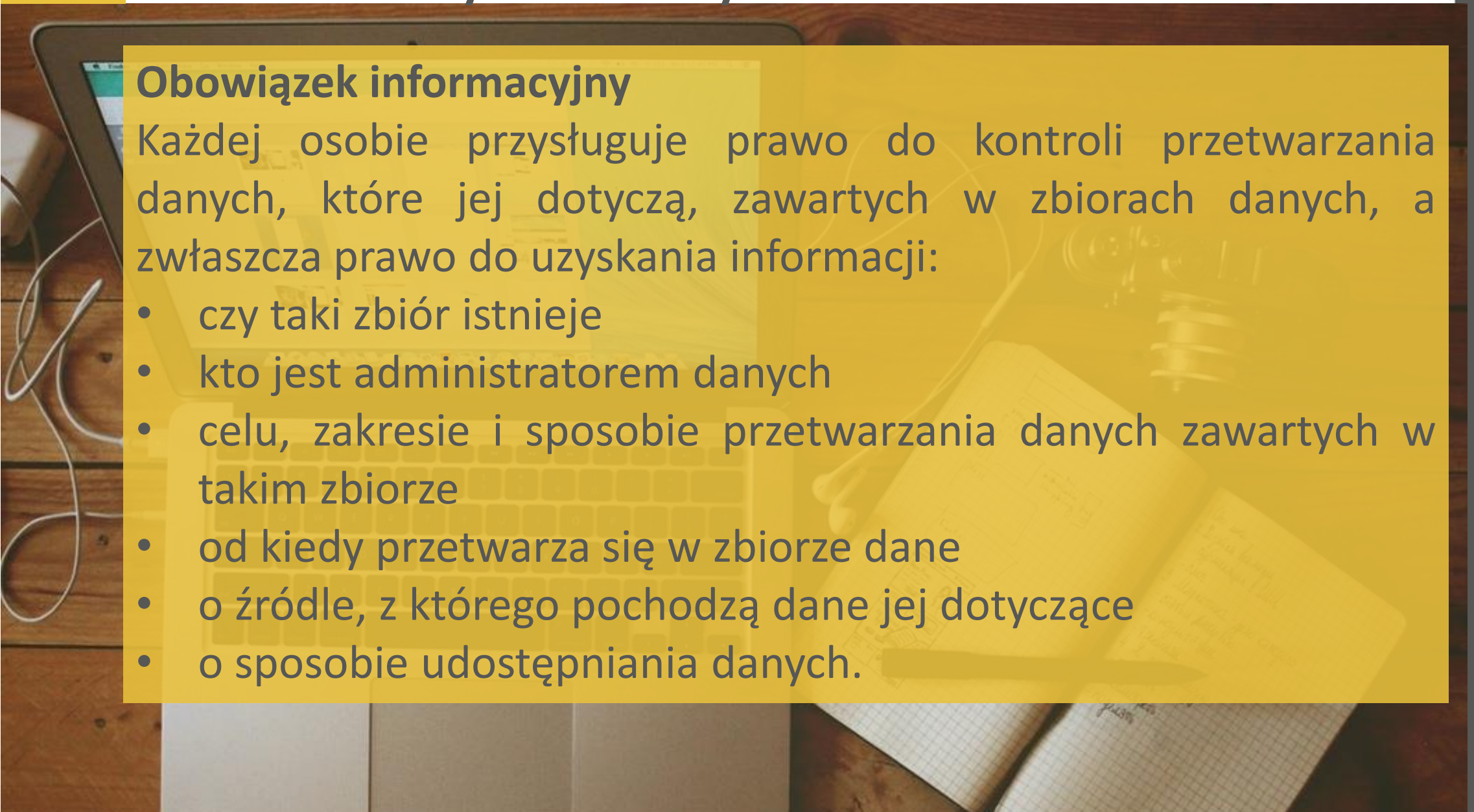
WATCHDOG
ZMIENIAMY
SYSTEMOWO



WATCHDOG
ZMIENIAMY
SYSTEMOWO

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



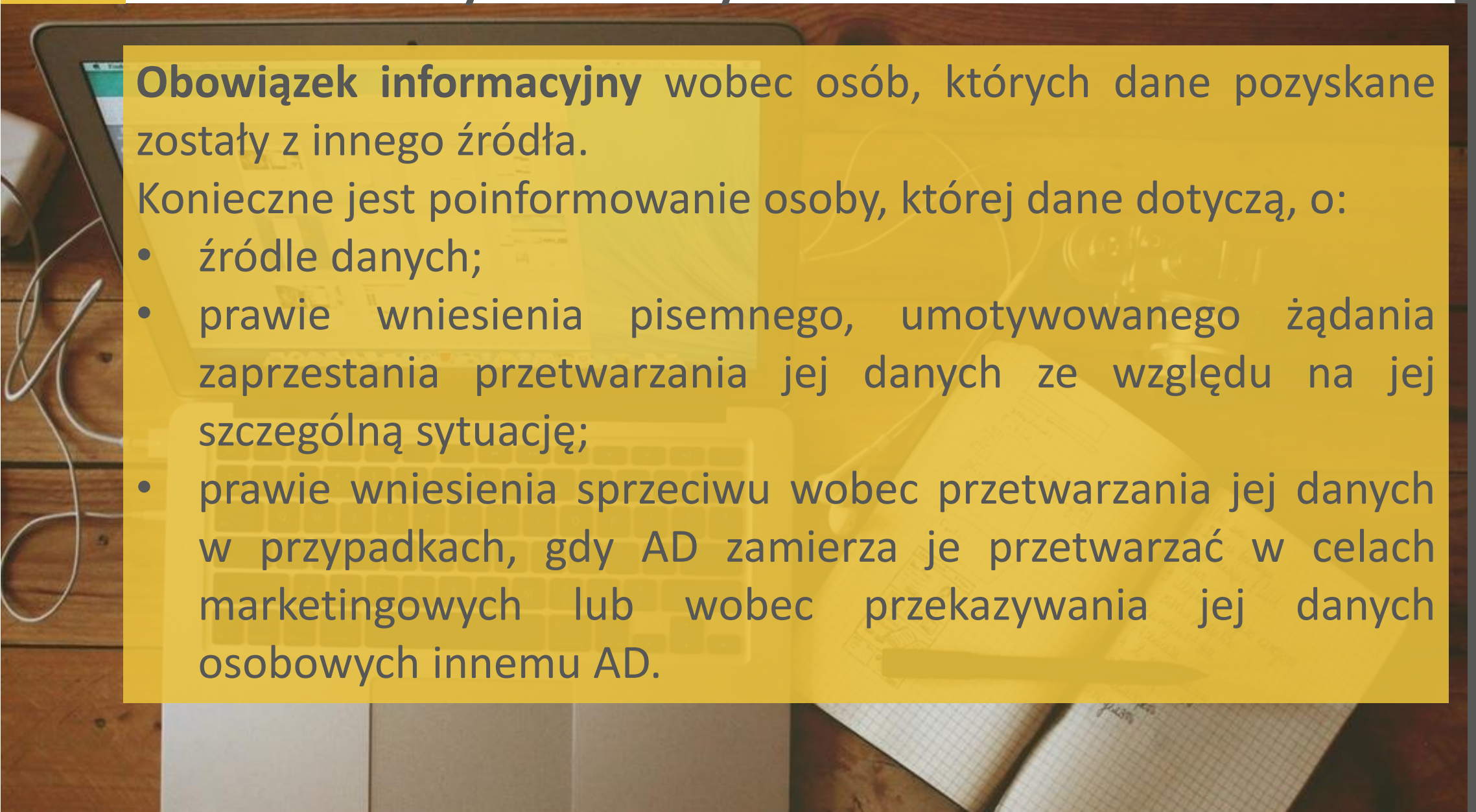
Obowiązek informacyjny

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do uzyskania informacji:

- czy taki zbiór istnieje
- kto jest administratorem danych
- celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze
- od kiedy przetwarza się w zbiorze dane
- o źródle, z którego pochodzą dane jej dotyczące
- o sposobie udostępniania danych.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



Obowiązek informacyjny wobec osób, których dane pozyskane zostały z innego źródła.

Konieczne jest poinformowanie osoby, której dane dotyczą, o:

- źródle danych;
- prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;
- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy AD zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu AD.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Obowiązek informacyjny
przykład

Zawiadomienie o przetwarzaniu danych osobowych

Pragniemy poinformować, że na podstawie art. 25 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U.2002.101.926 z późn. zm.), Pana/Pani dane osobowe przetwarzane są przez Administratora Danych, którym jest spółka :
MAKRO Cash and Carry Polska S.A. z siedzibą w Al. Krakowskiej 61, 02-183 Warszawa, NIP: 522-000-28-60,
wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy KRS, pod numerem 0000047354, dysponująca kapitałem zakładowym w wysokości 257 068 680,00 zł, wpłaconym w całości. Dane przetwarzane są w celach promocji towarów i usług oferowanych przez MAKRO Cash and Carry Polska S.A. (marketing bezpośredni własnych produktów i usług).
Zbiór danych, w którym przetwarzane są dotyczące Pana/Pani informacje zawiera:

regon, nazwa firmy, imię, nazwisko, ulica, nr posesji/lokalu, kod pocztowy, miejscowość.

Ma Pan/Pani prawo dostępu do danych, prawo ich poprawiania, prawo żądania zaprzestania przetwarzania danych osobowych z uwagi na szczególną sytuację, a także prawo sprzeciwu wobec ich przetwarzania dla celów marketingowych oraz wobec przekazywania ich innym podmiotom.
Pana/Pani dane osobowe zostały pozyskane z Głównego Urzędu Statystycznego.

MAKRO Cash and Carry Polska S.A., Aleja Krakowska 61, 02-183 Warszawa
www.makro.pl

ZASADY REALIZACJI BONU TOWAROWEGO

1. Bon towarowy jest dokumentem upoważniającym do zakupu towarów sprzedawanych przez MAKRO Cash and Carry Polska S.A.
2. Klient w momencie dokonywania zapłaty za towar, przekazuje bon towarowy kasjerowi.
3. Bon może być zrealizowany jedynie w formie częściowej zapłaty. Pozostałą część ceny Klient jest zobowiązany dopłacić w innej formie np. gotówką lub kartą płatniczą Visa, MasterCard lub Maestro.
4. Bon towarowy nie podlega wymianie na gotówkę.
5. Nie jest dopuszczalna płatność bonem towarowym za zakup wyrobów tytoniowych oraz paliw.
6. Bon towarowy nie może być zrealizowany, jeśli nosi oznaki fałszerstwa lub zniszczenia (zamazania, kreślenia, klejenia itp.).
7. W przypadku zniszczenia bonu duplikat nie będzie wydawany.
8. Bon towarowy zachowuje ważność do dnia wskazanego na bonie i po tej dacie nie może być przedstawiony do realizacji.
9. Szczegółowe zasady dostępne są w regulaminie.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

Obowiązek informacyjny
przykład

"Am-Odo" Agnieszka Majdzińska
18023343
Południowa 21
95-030 Rzgów

Eniro Polska Sp. z o.o.
ul. Postępu 14A
02-676 Warszawa
panoramafirm.pl

Biuro Obsługi Klienta
Tel. +48 22 289 20 00
Fax +48 22 289 20 01
Infolinia 801 801 600
eniro@eniro.pl

Sąd Rej. dla m. st. Warszawy
XII Wydział Gospodarczy
KRS 116894
Kapitał Zakładowy 20 000 000 zł
NIP 521-01-25-377

Szanowni Państwo!

Uprzejmie informujemy, że Państwa firma znajduje się w bazie danych Eniro Polska, która od 20 lat funkcjonuje pod renomowaną marką Panorama Firm i zawiera ponad 2 miliony rekordów. Dzięki obecności w bazie Panoramy Firm, informacje o polskich firmach docierają do milionów użytkowników Internetu i telefonów komórkowych.

W związku z tym pragniemy poinformować, że administratorem danych odnoszących się do Państwa działalności gospodarczej (pełna nazwa firmy wraz z imieniem i nazwiskiem właściciela*, adres siedziby, nr REGON*, nr NIP*, adres e-mail*, nr telefonu*, nr faksu* oraz dane osoby kontaktowej – imię i nazwisko*, stanowisko służbowe*, nr telefonu służbowego*, służbowy adres e-mail*) jest Eniro Polska Sp. z o.o. z siedzibą w Warszawie, przy ul. Postępu 14A. Dane przetwarzane są w związku z prowadzeniem bazy danych Panorama Firm oraz w celach marketingowych i mogą być udostępniane partnerom biznesowym Eniro Polska Sp. z o.o. Dane zostały pozyskane z Głównego Urzędu Statystycznego w drodze umowy zawartej zgodnie z art. 45 ust. 3 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej lub z innych powszechnie dostępnych źródeł.

Jednocześnie informujemy, że każdej osobie przysługuje prawo dostępu do treści swoich danych i możliwość ich poprawiania, a także prawo wniesienia umotywowanego, pisemnego żądania zaprzestania ich przetwarzania ze względu na szczególną sytuację oraz możliwość zgłoszenia sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania ich innym podmiotom.

Ponadto informujemy, że dane przetwarzane są na podstawie art. 23 ust. 1 pkt. 5 ustawy o ochronie danych osobowych.

Dodatkowe informacje oraz możliwość aktualizacji i uzupełnienia danych uzyskacie Państwo w Biurze Obsługi Klienta Eniro Polska Sp. z o.o. .

Poufne
NR STRONY
1 (1)
DATA
16 września 2014

220

Z poważaniem

Michał Sztąberek
Michał Sztąberek

Administrator Bezpieczeństwa Informacji

WATCHDOG
ZMIENIAMY
SYSTEMOWO

Obowiązek informacyjny

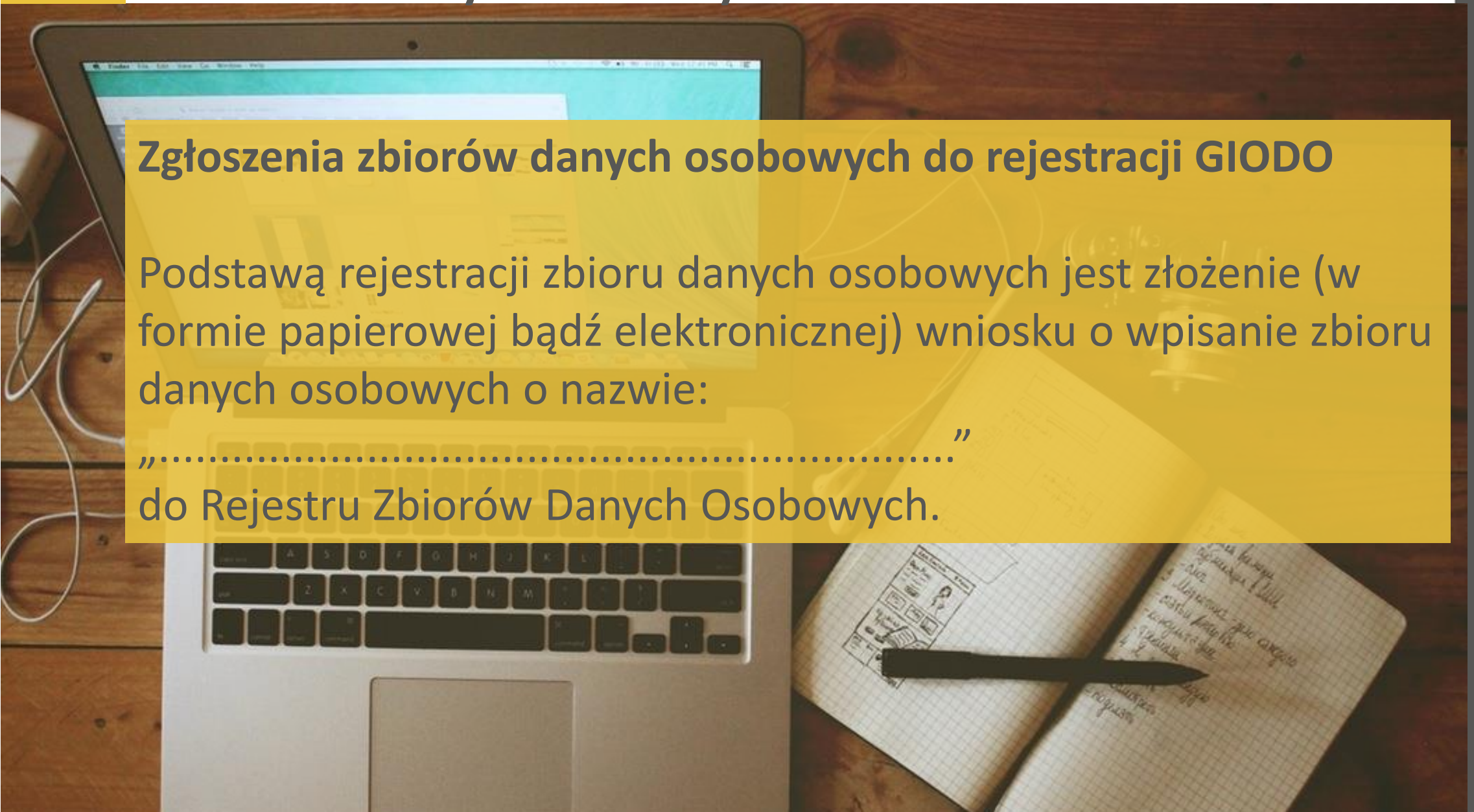
1. Obowiązek informacyjny wobec osób, od których zbierane są dane osobowe:
a) zakres informacji:
Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do uzyskania informacji:
- czy taki zbiór istnieje, oraz do ustalenia administratora danych – adresu jego siedziby i pełnej nazwy (a w przypadku, gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska);
- o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
- od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- o źródle, z którego pochodzą dane jej dotyczące (chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej);
- o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.

b) sankcje karne za nie dopełnienie obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach:
Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie o ochronie danych osobowych, podlega ***grzywnie, karze ograniczenia wolności*** *albo* ***pozbawienia wolności do roku****.*

2. Obowiązek informacyjny wobec osób, których dane pozyskane zostały z innego źródła – w tej sytuacji dodatkowo konieczne jest poinformowanie osoby, której dane dotyczą, o:
- źródle danych;
- prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;
- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy AD zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu AD.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO



Zgłoszenia zbiorów danych osobowych do rejestracji GIODO

Podstawą rejestracji zbioru danych osobowych jest złożenie (w formie papierowej bądź elektronicznej) wniosku o wpisanie zbioru danych osobowych o nazwie:

„.....”

do Rejestru Zbiorów Danych Osobowych.

WATCHDOG ZMIENIAMY SYSTEMOWO

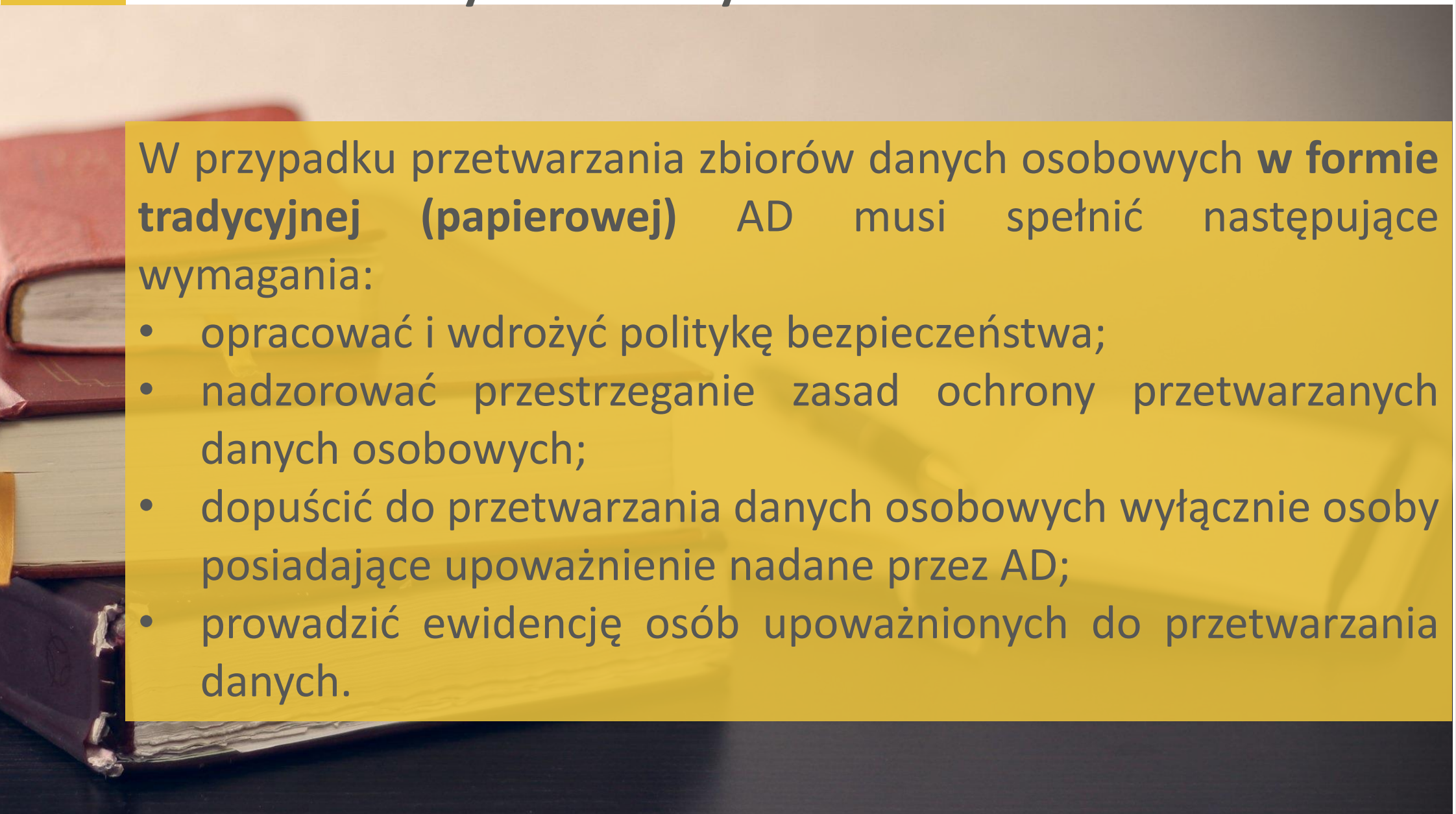
Zgłoszenia zbiorów danych osobowych do rejestracji GIODO

Podstawą rejestracji zbioru danych osobowych jest złożenie (w formie papierowej bądź elektronicznej) wniosku o wpisanie zbioru danych osobowych o nazwie: „.....” do Rejestru Zbiorów Danych Osobowych.

Wniosek stanowi załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz. 1536).

UWAGA!!!
Niezależnie od tego, czy AD powoła ABI, czy też nie – dane osobowe przetwarzane w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych (czyli dane zwykłe przetwarzane w formie papierowej), z wyjątkiem zbiorów zawierających dane wrażliwe/sensytywne, od 1 stycznia 2015 r. zwolnione są z obowiązku ich rejestracji u GIODO.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO



W przypadku przetwarzania zbiorów danych osobowych **w formie tradycyjnej (papierowej)** AD musi spełnić następujące wymagania:

- opracować i wdrożyć politykę bezpieczeństwa;
- nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych;
- dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD;
- prowadzić ewidencję osób upoważnionych do przetwarzania danych.

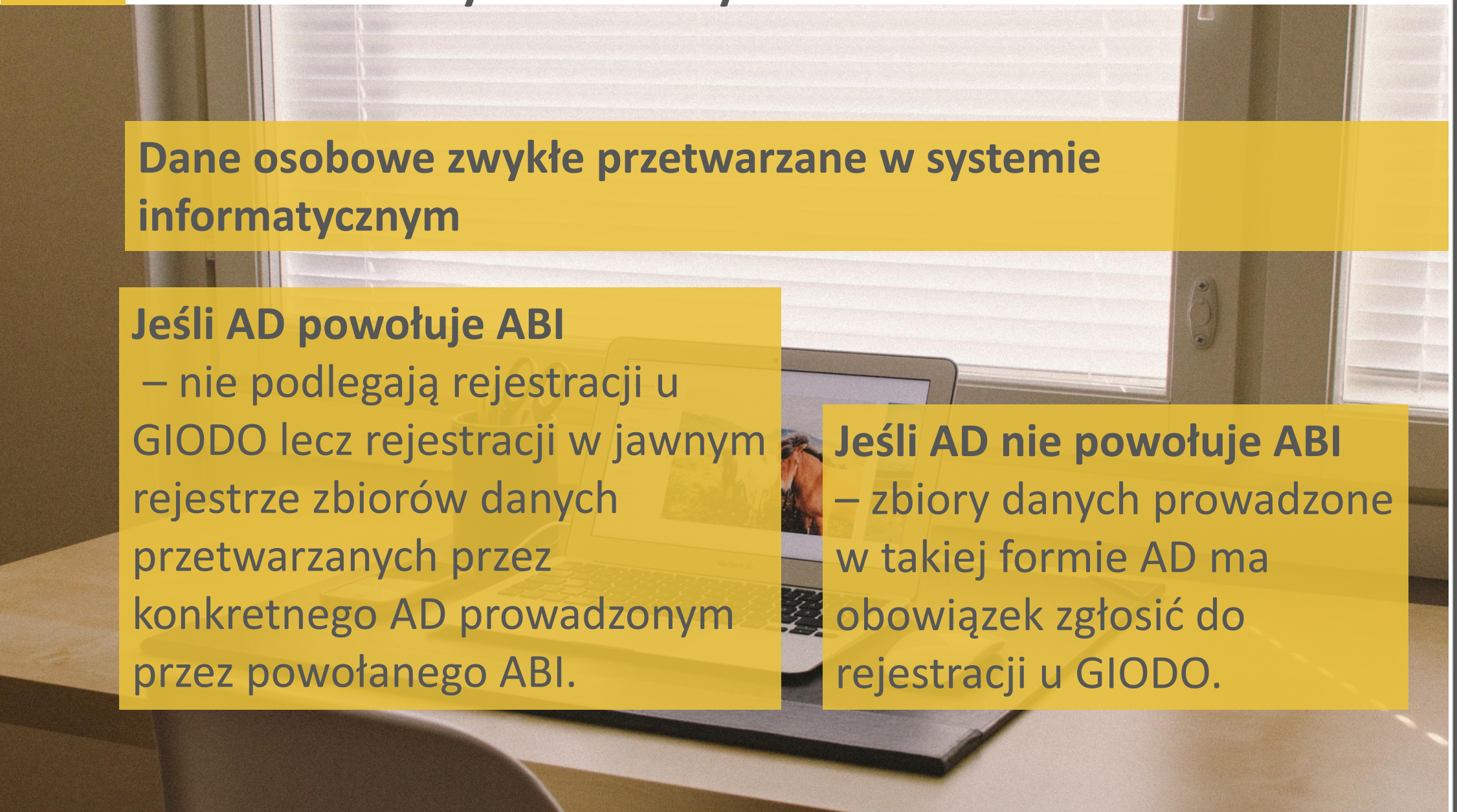
WATCHDOG ZMIENIAMY SYSTEMOWO

W przypadku przetwarzania zbiorów danych osobowych w formie tradycyjnej (papierowej) AD musi spełnić następujące wymagania:
- opracować i wdrożyć politykę bezpieczeństwa;
- nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych;
- dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD;
- prowadzić ewidencję osób upoważnionych do przetwarzania danych.

UWAGA!!!
Zwolnienie z rejestracji u GIODO zbiorów danych zwykłych przetwarzanych w formie papierowej nie oznacza zwolnienia AD z obowiązku zapewnienia ochrony przetwarzanym danym osobowym.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO

WATCHDOG ZMIENIAMY SYSTEMOWO

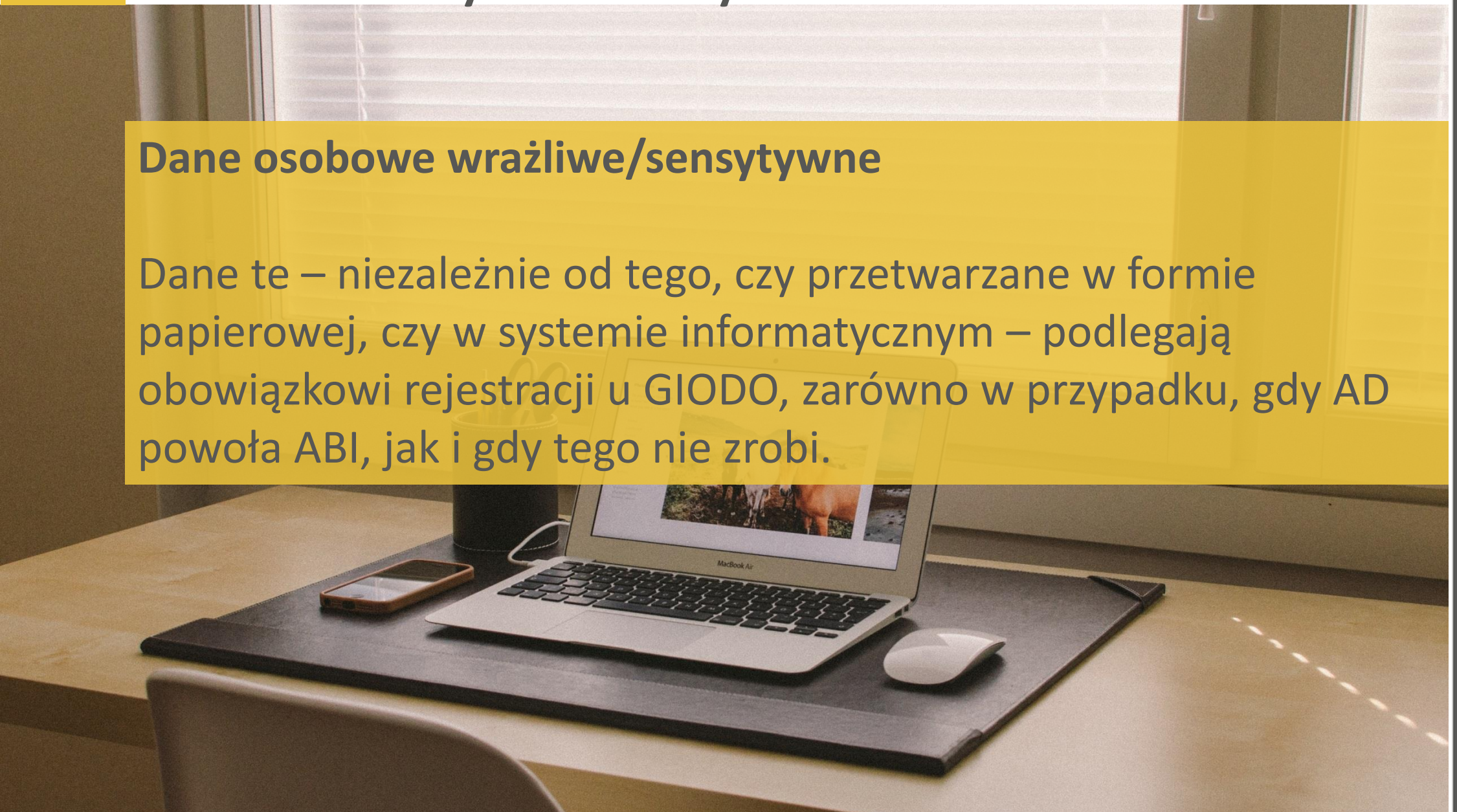


Dane osobowe zwykłe przetwarzane w systemie informatycznym

Jeśli AD powołuje ABI
– nie podlegają rejestracji u GIODO lecz rejestracji w jawnym rejestrze zbiorów danych przetwarzanych przez konkretnego AD prowadzonym przez powołanego ABI.

Jeśli AD nie powołuje ABI
– zbiory danych prowadzone w takiej formie AD ma obowiązek zgłosić do rejestracji u GIODO.

3 Praktyczne aspekty wdrażania przepisów o ochronie danych osobowych w NGO



Dane osobowe wrażliwe/sensytywne

Dane te – niezależnie od tego, czy przetwarzane w formie papierowej, czy w systemie informatycznym – podlegają obowiązkowi rejestracji u GIODO, zarówno w przypadku, gdy AD powoła ABI, jak i gdy tego nie zrobi.

WATCHDOG ZMIENIAMY SYSTEMOWO

Dane osobowe zwykłe przetwarzane w systemie informatycznym

1) W przypadku powołania ABI przez AD – nie podlegają rejestracji u GIODO lecz rejestracji w jawnym rejestrze zbiorów danych przetwarzanych przez konkretnego AD prowadzonym przez powołanego ABI.

2) W przypadku nie powołania ABI przez AD – zbiory danych prowadzone w takiej formie AD ma obowiązek zgłosić do rejestracji u GIODO.

Dane osobowe wrażliwe/sensytywne

Dane te – niezależnie od tego, czy przetwarzane w formie papierowej, czy w systemie informatycznym – podlegają obowiązkowi rejestracji u GIODO, zarówno w przypadku, gdy AD powoła ABI, jak i gdy tego nie zrobi.

W przypadku przetwarzania zbiorów danych osobowych w systemie informatycznym AD musi spełnić następujące wymagania:
- opracować i wdrożyć politykę bezpieczeństwa;
- opracować i wdrożyć instrukcję zarządzania systemem informatycznym;
- nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych;
- dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD;
- prowadzić ewidencję osób upoważnionych do przetwarzania danych.

Wypełniony i podpisany wniosek można:
- doręczyć osobiście do Biura GIODO;
- przesłać pocztą na adres Biura GIODO;
- przesłać faxem do Kancelarii Biura GIODO;
- przesłać pocztą elektroniczną do Kancelarii Biura GIODO.

Dane kontaktowe do Biura GIODO

Biuro Generalnego Inspektora
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
Polska
tel. +48 (22) 860-70-86
e-mail: kancelaria@giodo.gov.pl

Wniosek można także wypełnić i podpisać elektronicznie w serwisie e-GIODO (rejestracja zbiorów, ogólnokrajowy Rejestr zbiorów oraz Rejestr ABI) - http://egiodo.giodo.gov.pl/index.dhtml

WATCHDOG
ZMIENIAMY
SYSTEMOWO

WATCHDOG
ZMIENIAMY
SYSTEMOWO

Proces rejestracji zbiorów danych osobowych

Zwykłych przetwarzanych w systemie informatycznym:
- następuje w momencie dokonania zgłoszenia,
- dane osobowe można legalnie przetwarzać od momentu dokonania zgłoszenia;

Wrażliwych/sensytywnych
- następuje w momencie wydania przez Zastępcę Generalnego Inspektora Ochrony Danych Osobowych zaświadczenia o zarejestrowaniu w jawnym, ogólnokrajowym rejestrze zbiorów danych osobowych zbioru danych osobowych o nazwie „.....”,
- dane osobowe można legalnie przetwarzać od daty wydania zaświadczenia,
- **proces rejestracji trwa od około 3-4 miesięcy** (jeśli jest się w stałym kontakcie z urzędnikiem Biura GIODO prowadzącym sprawę rejestracji zbioru danych) **do roku lub dłużej** (jeśli po dokonaniu zgłoszenia zbioru danych do rejestracji GIODO pozostawia się sprawę jej własnemu biegowi).

Zaświadczenie o rejestracji zbioru danych wrażliwych /sensytywnych

Zawiera następujące elementy:
a) miejscowość i datę wydania (= data podpisania zaświadczenia przez Zastępcę Generalnego Inspektora Ochrony Danych Osobowych);
b) sygnaturę akt;
c) treść zaświadczenia stanowią:
- podstawa prawna wydania zaświadczenia (art. 42 ust. 4 ustawy o ochronie danych osobowych – tekst jednolity Dz. U. z 2014 r., poz. 1182 z późn. zm.);
- numer zgłoszenia nadany wnioskowi przez urzędników Biura GIODO;
- pełna nazwa administratora danych osobowych dokonującego zgłoszenia;
- informacja o rejestracji zbioru danych osobowych o nazwie „.....”
w ogólnokrajowym, jawnym rejestrze zbiorów danych osobowych, prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych;
d) podpis i pieczątkę Zastępcy Generalnego Inspektora Ochrony Danych Osobowych;

e) wskazanie kto otrzymuje zaświadczenie (1. Administrator Danych – pełna nazwa i adres, 2. a/a);
f) informację o zwolnieniu z opłaty skarbowej (nie podlega opłacie skarbowej na podstawie ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej – Dz. U. z 2006 r. Nr 225, poz. 1635 z późn. zm.);
g) podpis i pieczątkę urzędnika prowadzącego sprawę (specjalisty albo referenta prawnego).

Korespondencja dotycząca rejestracji zbiorów danych osobowych

- w razie stwierdzenia we wniosku uchybień formalnych lub nieprawidłowości merytorycznych Pracownicy Departamentu Rejestracji Zbiorów Danych Osobowych prześlą do instytucji wnioskującej (organizacji pozarządowej) wezwanie do usunięcia braków formalnych lub wyjaśnień dotyczących kwestii merytorycznych w ciągu 7 dni (od daty otrzymania wezwania) pod rygorem odmowy rejestracji zbioru danych osobowych.

WATCHDOG
ZMIENIAMY
SYSTEMOWO

UWAGA!!!

Prawidłowo (pod względem formalnym) wypełniony wniosek z dołączonym do niego dobrze przygotowanym uzupełnieniem daje gwarancję przeprowadzenia procesu rejestracji zbioru danych osobowych bez komplikacji.

Korespondencja z Biura GIODO zawierającą zaświadczenie o rejestracji zbioru danych osobowych obejmującego dane wrażliwe nie zawsze jest wysyłana natychmiast po podpisaniu zaświadczenia przez Zastępcę GIODO (czas oczekiwania wynosi zwykle od kilku do kilkunastu dni).
Dla legalności przetwarzania danych osobowych w ramach rejestrowanego zbioru nie ma to jednak większego znaczenia, gdyż liczy się data podpisania zaświadczenia przez Zastępcę GIODO, a nie data jego wpływu do administratora danych.
Zaświadczenie o rejestracji zbioru danych osobowych przesyłane jest do administratora danych listem poleconym za zwrotnym potwierdzeniem odbioru.

Sankcje karne za nie dopełnienie obowiązku zgłoszenia zbioru danych do rejestracji GIODO

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega ***grzywnie, karze ograniczenia wolności*** *albo* ***pozbawienia wolności do roku****.*

WATCHDOG
ZMIENIAMY
SYSTEMOWO

Podsumowanie

Podsumowując przedstawione powyżej zmiany należy dodać, iż:
- ABI wyznaczony przez AD do dnia 31 grudnia 2014 r. pełni swoją funkcję w rozumieniu przepisów ustawy o ochronie danych osobowych w brzmieniu obowiązującym od 1 stycznia 2015 r. do czasu zgłoszenia go do rejestru administratorów bezpieczeństwa informacji – **nie dłużej** jednak **niż do dnia 30 czerwca 2015 r**.;

- do postępowań rejestracyjnych prowadzonych przez GIODO – wszczętych na podstawie dotychczas obowiązujących zgłoszeń i nie zakończonych przed dniem wejścia w życie ustawy o ułatwieniu wykonywania działalności gospodarczej wprowadzającej zmiany w ustawie o ochronie danych osobowych – stosuje się przepisy dotychczasowe (tzn. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.).

Wnioski na przyszłość

Czas pokaże, czy możliwość, jaką od 1 stycznia 2015 r. daje AD ustawa o ochronie danych osobowych, a którą jest powołanie ABI i zgłoszenie go do rejestracji u GIODO m.in. celem prowadzenia wewnętrznego rejestru przetwarzanych zbiorów danych osobowych, przyczyni się do przyspieszenia postępowań dotyczących rejestracji zbiorów danych prowadzonych przez GIODO.

Statystyki przedstawione przez Pracowników Biura GIODO podczas konferencji pt.: „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne”* podają, że w porównaniu do analogicznego okresu z ubiegłego roku (styczeń 2014/styczeń 2015), w pierwszym miesiącu obowiązywania ustawy o ochronie danych osobowych w nowym brzmieniu, nie zmniejszyła się liczba zgłoszonych do rejestracji zbiorów danych osobowych i wynosi ona 2.500.

4 Kontrole

WATCHDOG ZMIENIAMY SYSTEMOWO

Kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych w organizacji pozarządowej mogą przeprowadzić:

- **pracownicy Biura GIODO**
  – na mocy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r., poz. 1182 z późn. zm.);
- **pracownicy Państwowej Inspekcji Pracy**
  – na mocy porozumienia zawartego z Generalnym Inspektorem Ochrony Danych Osobowych;
- **pracownicy Urzędów Marszałkowskich i Wojewódzkich Urzędów Pracy (Instytucja Pośrednicząca i Instytucja Pośrednicząca 2-Stopnia)**
  – na mocy zapisów zawartych w umowach o dofinansowanie realizacji projektów współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego zawieranych pomiędzy tymi instytucjami a organizacjami pozarządowymi.*

4 Kontrole

WATCHDOG ZMIENIAMY SYSTEMOWO

Kontrola GIODO – trwa od kilku do kilkunastu dni i jest kontrolą kompleksową.

Kontrola PIP – jest kontrolą fragmentaryczną i może dotyczyć np.: zakresu upoważnienia do przetwarzania danych osobowych pracownika odpowiadającego w organizacji za prowadzenie kadr i płac.

4 Kontrole

WATCHDOG ZMIENIAMY SYSTEMOWO

Kontrola Urzędu Marszałkowskiego/Wojewódzkiego Urzędu Pracy – może mieć charakter planowy bądź być kontrolą doraźną. Czas trwania: kilka dni.

Zakres tematyczny kontroli jest węższy od kontroli GIODO i szerszy od kontroli PIP –sprawdza się czy NGO posiada:

- politykę bezpieczeństwa;
- instrukcję zarządzania systemem informatycznym;
- prowadzenie i aktualność ewidencji osób upoważnionych do przetwarzania danych;
- czy dane osobowe przetwarzają osoby posiadające upoważnienie nadane przez AD.

Kontrolerom UM/WUP należy udostępnić wymagane dokumenty, a upoważnieni pracownicy organizacji pozarządowej mogą na miejscu odpowiadać na pytania kontrolujących i udzielać im wyjaśnień. Z przeprowadzonej kontroli sporządzana jest w terminie 30 dni informacja pokontrolna, którą otrzymuje organizacja pozarządowa. Może ona od razu ją podpisać lub w ciągu 14 dni przekazać swoje stanowisko na piśmie. Następnie UM/WUP przygotowuje protokół kontroli zawierający m.in. zalecenia pokontrolne i czas dany organizacji pozarządowej na ich wdrożenie. UM/WUP może zweryfikować wdrożenie zaleceń pokontrolnych np.: w trakcie następnej kontroli projektu.
Kontrole UM/WUP prowadzone są w związku z przetwarzaniem przez organizacje pozarządowe danych osobowych uczestników projektu m.in. w systemie informatycznym o nazwie „PEFS2007”.

UWAGA!!!

W przypadku realizacji przez organizację pozarządową projektu współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego – AD na etapie:
- rekrutacji kandydatów do udziału w projekcie – jest organizacja pozarządowa;
- realizacji projektu – danymi uczestników projektu administruje Minister Rozwoju Regionalnego.

W przypadku środków publicznych pozyskiwanych na realizację projektów z innych źródeł (np.: Programu Operacyjnego Fundusz Inicjatyw Obywatelskich, Dotacja Prezydenta) kontrole zgodności przetwarzania danych z przepisami o ochronie danych osobowych nie występują.

5 Przydatne informacje

Strona internetowa Generalnego Inspektora Ochrony Danych Osobowych
www.giodo.gov.pl

WATCHDOG ZMIENIAMY SYSTEMOWO

5 Przydatne informacje

Przepisy prawa krajowego w zakresie ochrony danych osobowych

http://www.giodo.gov.pl/144/j/pl/

WATCHDOG ZMIENIAMY SYSTEMOWO

O Urzędzie | Prawo | Edukacja | Współpraca | Wydarzenia | Serwis prasowy | Odpowiedzi na pytania | Kontakt

Strona główna / Prawo / Przepisy prawa / **Krajowe**

Menu

- Reforma unijnych przepisów
- Przepisy prawa
  - Krajowe
  - Europejskie
  - Międzynarodowe
- Wyroki
- Decyzje GIODO
- Wystąpienia, sygnalizacje, wnioski GIODO

JEŚLI CHCESZ

Krajowe

PRZEPISY RANGI USTAWOWEJ

- Krajowe akty prawne z zakresu ochrony danych osobowych
- Ustawa o ochronie danych osobowych (Dz. U. 2014.1182)
- Konstytucja Rzeczypospolitej Polskiej *(art. 47, 51)*
- Ustawy wprowadzające zmiany w ustawie o ochronie danych osobowych
- Przepisy proceduralne

AKTY WYKONAWCZE DO USTAWY O OCHRONIE DANYCH OSOBOWYCH

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011, Nr

Aktualności

- Konkurs na projekty informatyczne instytucji publicznych
- Dane medyczne wymagają szczególnej ochrony, 29.01.2015 r.
- O wpływie nowych przepisów na skuteczność ochrony danych - debata w „Dzienniku Gazecie Prawnej", 27.01.2015 r.
- Czy dzieci wiedzą jak ważna jest ochrona prywatności?
- Nowe prawo i edukacja odpowiedzią na wyzwania w ochronie danych

5 Przydatne informacje

serwis edukacyjny GIODO
https://edugiodo.giodo.gov.pl/

WATCHDOG ZMIENIAMY SYSTEMOWO

5 Przydatne informacje

rejestracja zbiorów, ogólnokrajowy Rejestr zbiorów oraz Rejestr ABI
http://egiodo.giodo.gov.pl/index.dhtml

WATCHDOG ZMIENIAMY SYSTEMOWO

5 Przydatne informacje

GIODO newsletter - https://news.giodo.gov.pl/

WATCHDOG ZMIENIAMY SYSTEMOWO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

NEWSLETTER GIODO

Nowa polityka prywatności i plików Cookies dla serwisów GIODO

Usługa „Newsletter GIODO" umożliwia wszystkim zainteresowanym osobom automatyczne otrzymywanie informacji, związanych z problematyką ochrony danych osobowych.

- Korzystanie z usługi „Newsletter GIODO" jest dobrowolne i bezterminowe.
- W celu świadczenia usługi „Newsletter GIODO" Generalny Inspektor Ochrony Danych Osobowych pozyskuje od osób zainteresowanych nazwy adresów poczty elektronicznej.
- Zarejestrowana osoba, w każdej chwili, ma możliwość dokonania zmiany bądź usunięcia swoich danych wprowadzonych w procesie rejestracji.
- Informacje dotyczące sposobu rejestracji, modyfikacji i usunięcia danych oraz informacje dotyczące polityki prywatności dostępne są po kliknięciu na linki: "Instrukcje dla subskrybentów Newsletter GIODO" oraz „Polityka prywatności GIODO".
- Administratorem danych jest Generalny Inspektor Ochrony Danych Osobowych (GIODO), z siedzibą w Warszawie, przy ul. Stawki 2. Dane osobowe (tj. adresy e-mail) zbierane są przez GIODO wyłącznie w celu ich przetwarzania dla realizacji usługi „Newsletter GIODO". Dane nie będą udostępniane odbiorcom danych w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych. Osobie, której dane dotyczą, przysługuje prawo dostępu do treści jej danych oraz możliwość ich poprawiania. Dane są podawane przez osoby, których dotyczą, dobrowolnie, niemniej bez ich podania nie jest możliwa realizacja usługi „Newsletter GIODO".

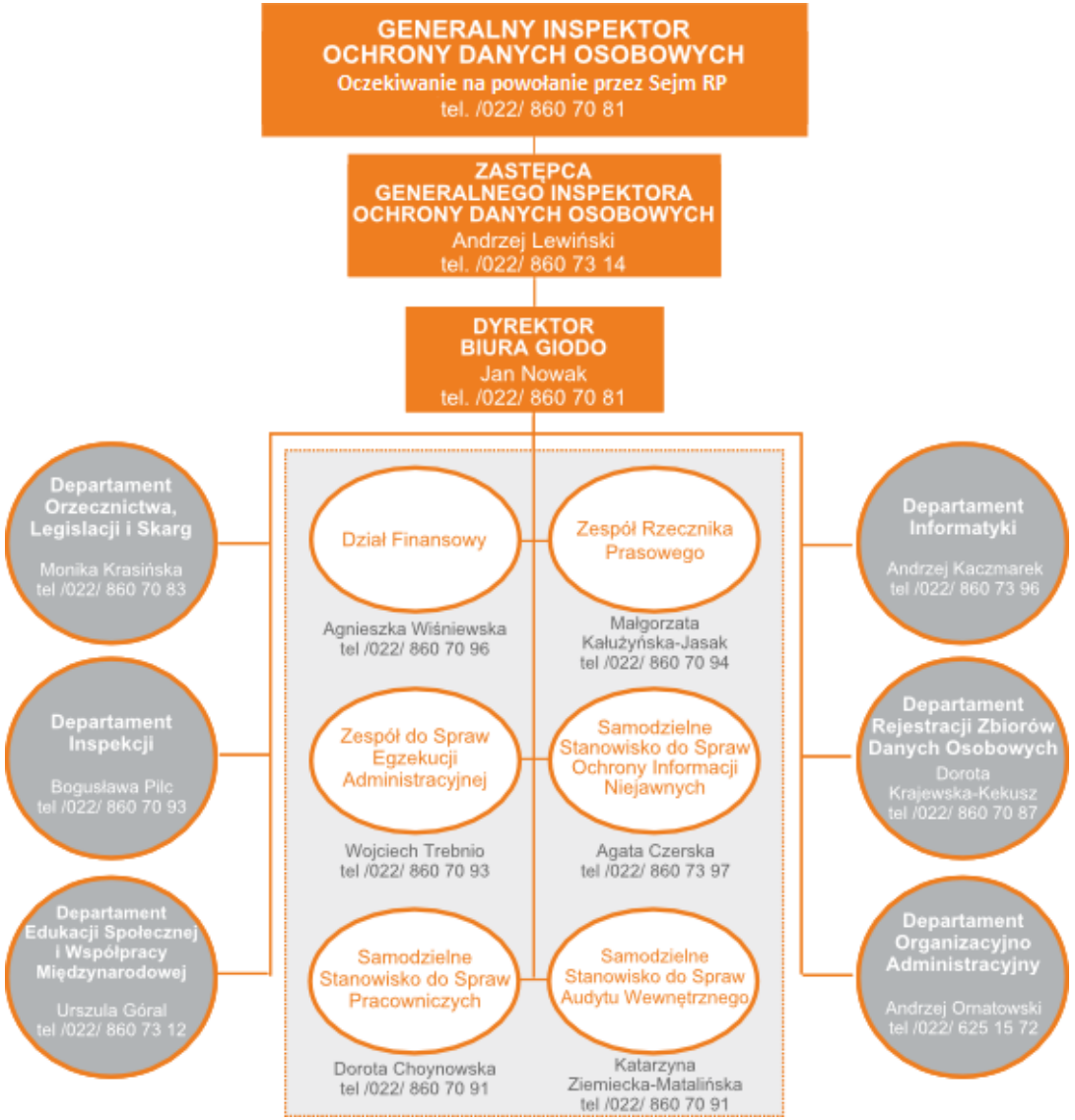
Zarejestruj się

* Twój e-mail:

5 Przydatne informacje

Struktura Biura GIODO

http://www.giodo.gov.pl/140/j/pl



WATCHDOG ZMIENIAMY SYSTEMOWO

Ciekawostki

WATCHDOG
ZMIENIAMY
SYSTEMOWO

28 stycznia jest
Europejskim Dniem
Ochrony Danych Osobowych

28 stycznia przypada Europejski Dzień Ochrony Danych Osobowych. W tym roku był obchodzony po raz 9. Z okazji Dnia Ochrony Danych Osobowych GIODO i Biuro GIODO organizują Dzień Otwarty.
Podczas tego dnia miały miejsce następujące wydarzenia:

- konferencja pt.: „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne" – materiał wideo z nagraniem przebiegu konferencji dostępny jest na stronie internetowej GIODO (link: http://www.giodo.gov.pl/410/id_art/8303/j/pl),

- otwarcie stoisk informacyjnych, przy których dyżurowali pracownicy Biura GIODO – w godz. 10:00 – 16:00 **można było** uzyskać bezpłatną poradę prawną z zakresu ochrony danych osobowych oraz **otrzymać** (również **bezpłatne**) **publikacje Generalnego Inspektora Ochrony Danych Osobowych i inne materiały edukacyjne dotyczące ochrony danych osobowych i prywatności**.

6

PYTANIE: Jak tworzyć listy odbiorców biuletynu?

OPOWIEDŹ: Podczas konferencji pt.: „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne”, zorganizowanej przez Biuro GIODO w związku z przypadającym w dniu 28 stycznia br. IX Dniem Ochrony Danych Osobowych, w hallu gmachu Centralnej Biblioteki Rolniczej (w której odbyła się konferencja) na jednym ze stolików leżała kartka papieru, na której zainteresowani dziennikarze mogli wpisywać swoje dane kontaktowe. Po zakończeniu konferencji kartka z tymi danymi prawdopodobnie trafiła do rzecznik prasowej GIODO.

Podobny sposób można wykorzystać w organizacji pozarządowej.

Można też prowadzić zapisy subskrybentów przez stronę internetową organizacji.

Tworzenie list odbiorców biuletynu w formie papierowej (od 1 stycznia br.) nie wymaga zgłoszenia do GIODO, w przypadku jednak, gdy tworzymy ją w wersji elektronicznej – to od 1 stycznia br. konieczność zgłoszenia takiego zbioru do rejestracji będzie zależała od tego czy organizacja powoła ABI (jeśli to zrobi – ABI będzie musiał zarejestrować zbiór w wewnętrznym jawnym rejestrze zbiorów danych przetwarzanych w organizacji) czy też nie (wtedy organizacja musi zgłosić taki zbiór do rejestracji GIODO).

W sytuacji, gdy listę odbiorców biuletynu tworzymy w formie papierowej, a biuletyn wysyłamy w formie elektronicznej – i tak trzeba będzie taki zbiór zarejestrować albo w wewnętrznym rejestrze zbiorów danych osobowych, albo u GIODO.

Do utworzenia listy odbiorców biuletynu powinno wystarczyć: imię i nazwisko oraz adres e-mail (warto sprawdzić, czy w przypadku elektronicznego zapisywania się na listę subskrybentów dodatkową daną nie będzie adres IP komputera).

Osoby wpisujące się na listę powinny wyrazić zgodę na przetwarzanie danych osobowych ich dotyczących oraz zostać poinformowane (najlepiej pisemnie) o tym: *kto*, *w jakim celu*, *w jakim zakresie*, *od kiedy przetwarza dane* tych osób dotyczące, *z jakiego źródła je pozyskał* i *komu może je udostępnić*.

WATCHDOG
ZMIENIAMY
SYSTEMOWO

6

PYTANIE: Na robionych przez nas wydarzeniach zbieram listy obecności z danymi kontaktowymi - wpisuję je potem do swojego dokumentu z kontaktami - czy mogę to robić?

ODPOWIEDŹ: TAK, ale trzeba się do tego dobrze przygotować:

1. Sporządzić listę obecności w formie tabeli, do której wpisywane będą dane osobowe, uwzględniając dwie dodatkowe kolumny: w jednej z nich wpisać treść zgody na przetwarzanie danych osobowych, w drugiej – zostawić miejsce na podpis osoby, która obok wpisała swoje dane (najlepszy do tego będzie poziomy układ dokumentu). W kolumnie z podpisem można umieścić informację, że podpis oznacza jednocześnie potwierdzenie otrzymania informacji, o której mowa poniżej.
2. Na osobnych kartkach przygotować informacje o tym: *kto*, *w jakim celu*, *w jakim zakresie*, *od kiedy przetwarza dane* tych osób dotyczące, *z jakiego źródła je pozyskał* i *komu może je udostępnić*. Jeśli to możliwe – informacje te powinny zostać opieczętowane pieczątką nagłówkową organizacji oraz podpisane przez AD lub ABI (jeśli zostanie powołany). Jeśli AD lub ABI mają pieczątki imienne – one także powinny znaleźć się na tak przygotowanych informacjach. Tak przygotowane informacje można przekazywać uczestnikom spotkań.
3. Domyślam się, że ten dokument, do którego przenoszone są dane z list obecności, ma formę elektroniczną. Od 1 stycznia 2015 r. zatem taki zbiór powinien zostać zarejestrowany albo przez wewnętrznego ABI-ego (w przypadku jego powołania) albo przez GIODO.
4. W przypadku przetwarzania zbiorów danych osobowych w systemie informatycznym AD musi spełnić następujące wymagania: - opracować i wdrożyć politykę bezpieczeństwa; - opracować i wdrożyć instrukcję zarządzania systemem informatycznym; - nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych; - dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD; - prowadzić ewidencję osób upoważnionych do przetwarzania danych.

WATCHDOG ZMIENIAMY SYSTEMOWO

6

WATCHDOG ZMIENIAMY SYSTEMOWO

PYTANIE:

Mamy w organizacji pudełko na korytarzu, gdzie klienci, którzy chcą otrzymywać od nas informacje mogą wrzucać swoje adresy mailowe - czy musimy dodatkowo dawać im do wypełnienia zgody na przetwarzanie danych osobowych jeśli i tak będąc naszymi klientami muszą coś takiego podpisywać (bo wymaga tego Centrum Obsługi Projektów Europejskich)?

ODPOWIEDŹ: Dodatkowe zgody są w tej sytuacji konieczne z tego względu, że zgoda na przetwarzanie danych osobowych udzielona w ramach Centrum Obsługi Projektów Europejskich dotyczy tylko tego obszaru/działania/projektu. Proszę dokładnie sprawdzić, co jest napisane w treści oświadczenia o wyrażeniu zgody. Na przetwarzanie danych w celu innym, niż wskazany w zgodzie, potrzebna jest dodatkowa/odrębna zgoda.

Dla przykładu – uczestnicy projektów współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego (Program Operacyjny Kapitał Ludzki) określając zakres swoich zgód na przetwarzanie danych osobowych wskazywali, że ich *„dane osobowe będą przetwarzane wyłącznie w celu udzielenia wsparcia, realizacji projektu „.....”, ewaluacji, monitoringu i sprawozdawczości w ramach Programu Operacyjnego Kapitał Ludzki*”. Na przetwarzanie danych osobowych uczestników tych projektów w celach marketingowych (np.: do informowania o innych realizowanych przez organizację projektach), po zakończeniu ich realizacji, organizacje pozarządowe musiały uzyskać odrębne zgody (zanim uczestnicy zakończyli udział w projekcie).

6

WATCHDOG ZMIENIAMY SYSTEMOWO

PYTANIE:

Czy są jakieś różnice w zakresie tego co obejmuje polityka bezpieczeństwa w zależności od celów dla których jest tworzona. Czy musi być osobna polityka bezpieczeństwa w zależności od tego jakie dane zbieramy - np do rekrutacji osobna, do szkolenia osobna itd.

ODPOWIEDŹ: Polityka bezpieczeństwa jest dokumentem, który powinien opisywać całość zagadnień dotyczących przetwarzania danych osobowych w organizacji, stworzonym po to, by zapewnić przetwarzanym danym osobowym bezpieczeństwo i ochronę adekwatną do zagrożeń.

W jej treści znaleźć się muszą – zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) – następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

6

PYTANIE:

Dla jakich danych nie trzeba mieć polityki i nie trzeba rejestrować bazy w GIODO?

ODPOWIEDŹ: To dwa pytania w jednym ☺

1) Nie ma takich zbiorów danych osobowych, dla których nie jest konieczne posiadanie polityki bezpieczeństwa – AD ma obowiązek zapewnić ochronę wszystkim przetwarzanym przez siebie zbiorom danych osobowych. Pomóc w tym ma polityka bezpieczeństwa, w której opisane zostaną wszystkie (na moment jej tworzenia) zbiory danych osobowych występujące u AD (a jeśli pojawią się nowe – to trzeba zaktualizować politykę bezpieczeństwa o dane przetwarzane w ramach nowych zbiorów).

2) Od 1 stycznia 2015 r. w zakresie rejestracji zbiorów danych osobowych sytuacja przedstawia się następująco:

a) zbiory danych zwykłych przetwarzane w formie tradycyjnej (papierowej) – zostały zwolnione z obowiązku rejestracji (niezależnie od tego, czy AD powoła ABI, czy też nie);

b) zbiory danych zwykłych przetwarzane w systemach informatycznych – w sytuacji, gdy:

- AD powoła ABI – podlegają rejestracji przez ABI w wewnętrznym jawnym rejestrze zbiorów danych przetwarzanych przez AD;
- AD nie powoła ABI – podlegają rejestracji u GIODO (tak, jak było do tej pory);

c) zbiory danych wrażliwych/sensytywnych – podlegają rejestracji u GIODO niezależnie od tego, czy AD powoła ABI, czy też nie (tak, jak było do tej pory).

Podsumowując – chronić należy wszystkie zbiory danych osobowych, ale nie wszystkie zbiory danych podlegają rejestracji. Brak obowiązku rejestracji zbioru danych osobowych nie zwalnia z obowiązku posiadania wymaganej przepisami dokumentacji (w tym m. in. polityki bezpieczeństwa).

WATCHDOG
ZMIENIAMY
SYSTEMOWO

6

PYTANIE:

Procedura krok po roku: opracowanie polityki/polityk, rejestracja bazy, zbieranie danych - ale szczegółowo.

ODPOWIEDŹ: AD powinien wykonać następujące czynności:

0-1) dokonać szczegółowej analizy zakresu przetwarzanych w organizacji w formie tradycyjnej (papierowej) danych osobowych zwykłych i wrażliwych/sensytywnych występujących we wszystkich przetwarzanych u niego zbiorach danych osobowych (przejrzeć wszystkie rejestry, wzory dokumentów/stosowanych formularzy/kwestionariuszy/ankiet/danych do zgłoszeń do ubezpieczeń/umów zawieranych z pracownikami i współpracownikami/...);

0-2) sprawdzić, jakie dane z dokumentów tradycyjnych (papierowych) są wprowadzane do systemów informatycznych i jak się te systemy nazywają (np.: Płatnik, nazwa programu księgowego, „PEFS2007" – w przypadku organizacji realizujących projekty współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, ...);

1) opracować, wdrożyć oraz aktualizować politykę bezpieczeństwa (wykorzystując analizę z pkt 0-1 i 0-2);

2) opracować, wdrożyć oraz aktualizować instrukcję zarządzania systemem informatycznym – *w przypadku organizacji przetwarzających dane osobowe w systemie informatycznym* (wykorzystując analizę jak wyżej);

3) nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych;

4) dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD;

5) prowadzić ewidencję osób upoważnionych do przetwarzania danych;

6) Zgłosić do rejestracji zbiory podlegające temu obowiązkowi i aktualizować je w razie wystąpienia zmian;

7) Zbierać dane osobowe i zgody na ich przetwarzanie oraz informować o tym, co się będzie działo z danymi

6

PYTANIE:
Obowiązkowe formuły będące wrażeniem zgody na przetwarzanie danych

ODPOWIEDŹ: W ustawie o ochronie danych osobowych nie ma gotowego wzoru zgody na przetwarzanie danych osobowych. Ustawa w tym zakresie mów tylko tyle, że „przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą wyrazi na to zgodę", a dalej, że „zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania".

Poniżej zamieszczam kilka przykładów, z którymi sama się spotkałam:

1) „Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w ofercie pracy do realizacji procesu rekrutacji zgodnie z ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r., poz. 1182 z późn. zm.)."

2) „...(pełna nazwa instytucji)... z siedzibą w ...(nazwa miejscowości)..., ul. ...(nazwa i nr ulicy)..., jako administrator danych osobowych informuje, że dane osobowe kandydatów do pracy będą przetwarzane wyłącznie w celu rekrutacji na stanowisko ...(nazwa stanowiska).... Kandydatowi/-ce przysługuje prawo dostępu do treści danych i ich poprawiania, podanie danych jest dobrowolne. W przypadku podania danych w zakresie szerszym aniżeli wynikający z art. 221 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz.94 ze zm.). Prosimy o zamieszczenie w przesyłanych dokumentach klauzuli zgody na przetwarzanie danych osobowych."

3) „Wyrażam zgodę na przetwarzanie danych osobowych zawartych w formularzu (kontaktowym) przez .....(nazwa instytucji)..... z siedzibą w ...(miejscowość)...., przy ul. ...(nazwa i nr ulicy)... w celu przesłania oferty."

4) „Przesłanie niniejszego formularza (kontaktowego) oznacza zgodę na przetwarzanie Pani/Pana danych osobowych przez ...(nazwa instytucji)... w celach marketingowych, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014 r., poz. 1182 z późn. zm.)."

5) „Zgodnie z Ustawą z dnia 18/07/2002 r. (Dz. U. z 2002 r., Nr 144, poz. 1204) "O świadczeniu usług drogą elektroniczną" wyrażam zgodę na otrzymywanie informacji handlowych drogą elektroniczną od firmy ...(pełna nazwa firmy)... na mój adres e-mail."

WATCHDOG ZMIENIAMY SYSTEMOWO

6

WATCHDOG ZMIENIAMY SYSTEMOWO

PYTANIE:
Jak zalegalizować już posiadane dane?

ODPOWIEDŹ: Posiadanych danych osobowych (w sensie *bazy danych*) nigdzie nie zgłaszamy ani nie wysyłamy – a zwłaszcza do GIODO (bo w takim przypadku GIODO z urzędu składa do prokuratury doniesienie o popełnieniu przestępstwa).

By móc legalnie przetwarzać dane osobowe, które obecnie podlegają obowiązkowi rejestracji (dane zwykłe przetwarzane w systemie informatycznym i dane wrażliwe/sensytywne) AD powinien:

1) opracować i wdrożyć politykę bezpieczeństwa;

2) opracować i wdrożyć instrukcję zarządzania systemem informatycznym – *w przypadku organizacji przetwarzających dane osobowe w systemie informatycznym*;

3) nadzorować przestrzeganie zasad ochrony przetwarzanych danych osobowych;

4) dopuścić do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie nadane przez AD;

5) prowadzić ewidencję osób upoważnionych do przetwarzania danych;

6) zgłosić do rejestracji zbiór podlegający temu obowiązkowi i aktualizować go w razie wystąpienia zmian:

a) w przypadku zgłoszeń rejestracyjnych obejmujących przetwarzanie danych zwykłych – dane osobowe można przetwarzać już od momentu dokonania zgłoszenia;

b) w przypadku zgłoszeń rejestracyjnych obejmujących przetwarzanie danych wrażliwych/sensytywnych – dane można przetwarzać dopiero od momentu wydania przez GIODO zaświadczenia o rejestracji zbioru danych;

7) zbierać dane osobowe i zgody na ich przetwarzanie oraz informować o tym, co się będzie działo z danymi.

6

WATCHDOG
ZMIENIAMY
SYSTEMOWO

PYTANIE:

Co to znaczy w praktyczne zapewniać bezpieczeństwo - szafa zamykana, komputer bez dostępu do internetu w wersji minimum i bardziej rozbudowane (KRATY W OKNACH BIURA itp).

ODPOWIEDŹ: To znaczy zapewnić i zastosować środki ochrony w stopniu adekwatnym do rodzaju przetwarzanych danych (zwykłe bądź wrażliwe/sensytywne) i kategorii mogących wystąpić zagrożeń.

6

WATCHDOG ZMIENIAMY SYSTEMOWO

PYTANIE:
weszły zmiany w ustawie ale nie ma przepisów wykonawczych - pytanie - o konsekwencje zmian i o to w którym momencie pojawia się te przepisy wykonawcze

ODPOWIEDŹ: Mamy już rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014 r., poz. 1934).
Pozostałych rozporządzeń wykonawczych rzeczywiście brak i cały czas na nie czekamy.
Niestety nie wiem, kiedy zostaną opublikowane.
Biuro GIODO zamieści je na stronie internetowej http://www.giodo.gov.pl/144/j/pl/ kiedy tylko zostaną opublikowane.

Projekt realizowany w ramach programu Obywatele dla Demokracji, finansowanego z Funduszy EOG oraz ze środków Trust Civil Society in Central and Eastern Europe.

WATCHDOG
ZMIENIAMY
SYSTEMOWO

dziękuję

Projekt realizowany jest przez Sieć Obywatelską Watchdog Polska oraz partnerów: