Ochrona danych osobowych w praktyce na przykładzie Lubelskiego Urzędu Wojewódzkiego w Lublinie

II Lubelski Konwent Informatyków i Administracji
20 – 21.09.2016 r.

WYBRANE AKTY PRAWNE Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

- Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (art. 47 i 51)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 z późn. zm.)

- 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. 2004 nr 100 poz. 1024 ze zm.)

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

AKTY PRAWNE Z ZAKRESU OCHRONY 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 Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 poz. 745)

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 poz. 719)

Rozporządzenie Parlamentu Europejskiego

W grudniu 2015 r. Rada i Parlament Europejski porozumiały się w sprawie proponowanego rozporządzenia.

8 kwietnia 2016 r. Rada przyjęła stanowisko w pierwszym czytaniu.

14 kwietnia 2016 r. rozporządzenie zostało przyjęte przez Parlament Europejski.

W dniu 4 maja 2016 r. w Dzienniku Urzędowym UE L 119 opublikowano 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 oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – zwanym potocznie **GDPR** – General Data Protection Regulation), które będzie bezpośrednio stosowane **od 25 maja 2018 r.**

Porównanie obowiązków administratorów danych

Obowiązek:	Obecne przepisy:	Nowe przepisy:
- przetwarzania na podstawie prawnej	√	√
- zgoda na piśmie w określonych sytuacjach	√	X
- wykonania obowiązku informacyjnego	√	√ (rozbudowany)
- powierzenia przetwarzania danych umową	√	√
- zabezpieczenia danych	√	√

Porównanie obowiązków administratorów danych

Obowiązek:	Obecne przepisy:	Nowe przepisy:
- uwzględnienia ochrony danych w fazie projektowania	X	√
- prowadzenia dokumentacji operacji przetwarzania danych	X	√
- ocena skutków w zakresie ochrony danych	X	√ (rozbudowany)
- zgłaszanie naruszenia ochrony danych	√ / X (w wybranych sektorach)	√

Porównanie obowiązków administratorów danych

Obowiązek:	Obecne przepisy:	Nowe przepisy:
- konsultowania przetwarzania danych z GIODO	X	√
- rejestrowania zbiorów danych	√ (zwolnienia, gdy zarejestrowany ABI)	X
- powołania administratora bezpieczeństwa informacji / inspektora ochrony danych	X	√ / X (w określonych przypadkach)

Źródło: A. Kobylańska, *Porównanie obowiązków administratora danych w GDPR i ustawie o ochronie danych osobowych*, Warszawa, 17.05.2016 r.

ADMINISTRATOR DANYCH

zgodnie z przepisami ustawy o ochronie danych osobowych to,

organ, jednostka organizacyjna, podmiot lub osoba,

decydująca o celach i środkach przetwarzania danych osobowych.

OCHRONA INTERESÓW OSÓB, KTÓRYCH DANE DOTYCZĄ

ADO powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane przetwarza, a w szczególności jest obowiązany zapewnić, aby dane te były

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem art. 26 ust. 2
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą,
- przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:
1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;
2) z zachowaniem przepisów art. 23 i 25.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

Art. 23. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
1)osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

2) **jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa**,

3) jest konieczne dla realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH WRAŻLIWYCH

Art. 27.

1.Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:
(…)
2) przepis szczególny **innej ustawy** zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
(…)

ADMINISTRATOR DANYCH OSOBOWYCH

ADO jest zobowiązany w szczególności:

- 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 nieuprawniona, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

- prowadzić dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki zapewniające ich ochronę, adekwatne do zagrożeń i zgodne z ustawowymi wymogami,

- zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,

- zapewnić, że do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, które ADO nadaje,

ADMINISTRATOR DANYCH OSOBOWYCH

ADO jest zobowiązany w szczególności:

- prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,
- zgłosić zbiór danych do rejestracji GIODO oraz dokonywać aktualizacji tego zgłoszenia w przypadku zaistnienia zmian informacji podanych podczas rejestracji,
- poinformować osobę, której dane dotyczą o adresie swojej siedziby, celu zbierania i przetwarzania danych, o odbiorcach tych danych oraz o prawie dostępu do danych i możliwości ich aktualizacji.

ADO może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. (Art. 31 u.o.d.o)

ADO może powołać administratora bezpieczeństwa informacji (ABI). (Art. 36a ust. 1 u.o.d.o)

STRUKTURA ORGANIZACYJNA LUW
w zakresie o.d.o.

ADMINISTRATOR DANYCH OSOBOWYCH

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

LOKALNY ADMINISTRATOR DANYCH OSOBOWYCH

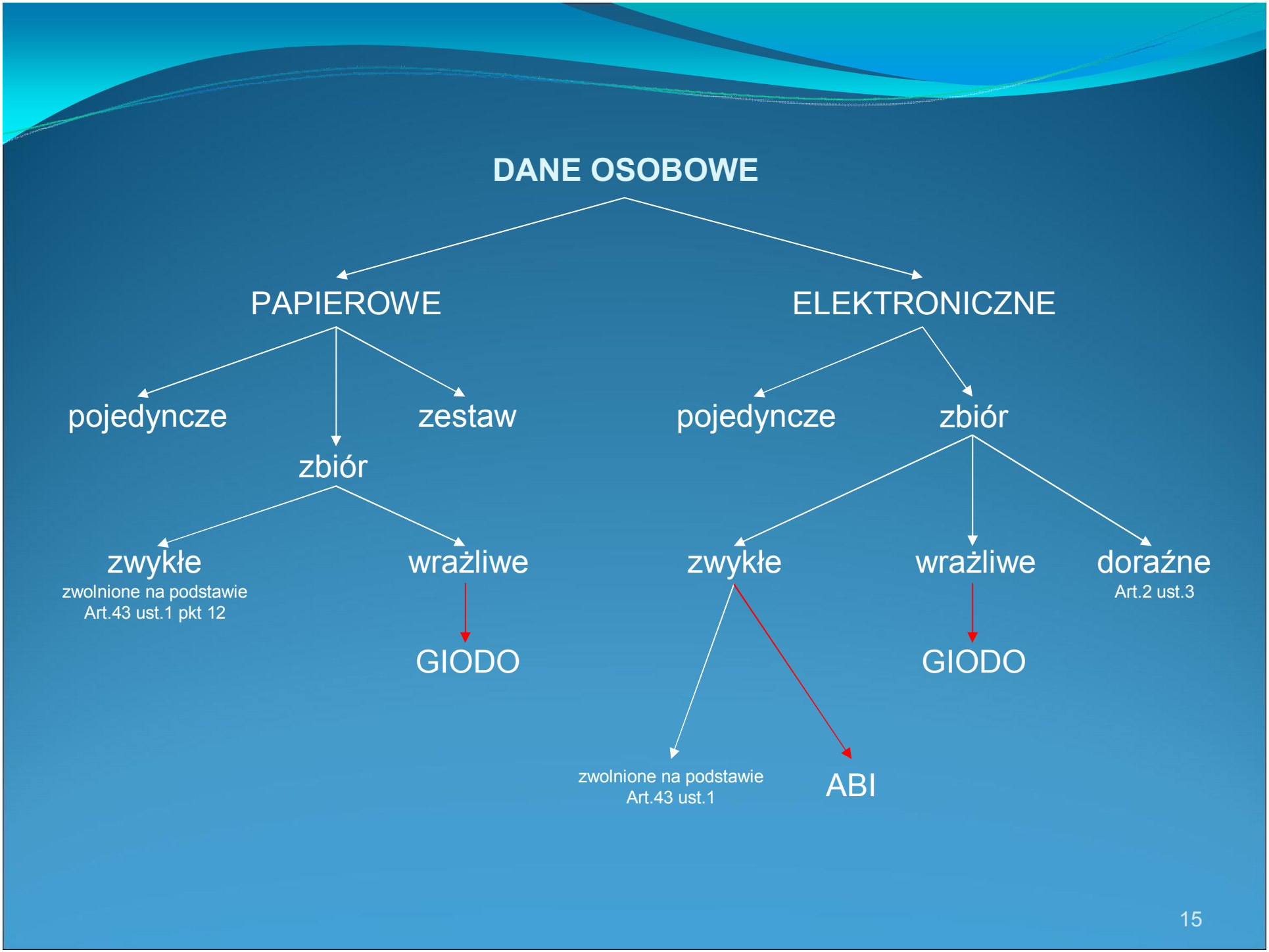
LOKALNY ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

ADMINISTRATOR SYSTEMU TELEINFORMATYCZNEGO

ADMINISTRATOR PODSYSTEMU

Osoby przetwarzające dane osobowe

Osoby przebywające w obszarze przetwarzania danych osobowych


DANE OSOBOWE
PAPIEROWE
ELEKTRONICZNE
pojedyncze
zestaw
zbiór
pojedyncze
zbiór
zwykłe
zwolnione na podstawie
Art.43 ust.1 pkt 12
wrażliwe
GIODO
zwykłe
wrażliwe
doraźne
Art.2 ust.3
GIODO
zwolnione na podstawie
Art.43 ust.1
ABI

Dokumentacja

Polityka bezpieczeństwa informacji

Polityka bezpieczeństwa danych osobowych
Wykaz zbiorów danych osobowych

Instrukcja zarządzania systemem teleinformatycznym
Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

Polityki bezpieczeństwa
Instrukcje zarządzania systemów informatycznych

Upoważnienia do przetwarzania danych osobowych

Rejestr wydanych upoważnień

Umowa powierzenia danych osobowych

Jawny rejestr zbiorów danych

ABI

Administratorem bezpieczeństwa informacji może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;

3) nie była karana za umyślne przestępstwo.

ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

Administrator danych zapewnia środki i organizacyjną odrębność ABI niezbędne do niezależnego wykonywania przez niego zadań.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Zadania ABI:

- 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 ADO,

  - nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

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

- prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7,

RODZAJE SPRAWDZEŃ I SPOSÓB ICH PRZEPROWADZANIA

- Sprawdzenie jest dokonywane:
  - dla administratora danych,
  - dla GIODO.

- Sprawdzenie jest przeprowadzane w trybie:
  1) sprawdzenia planowego – według planu sprawdzeń;
  2) sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez ABI wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
  3) w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.

RODZAJE ZABEZPIECZEŃ

Rozwiązania organizacyjne

Zabezpieczenia fizyczne

Zabezpieczenia sprzętowe

Zabezpieczenia informatyczne

Szkolenia

REALIZACJA POLITYKI BEZPIECZEŃSTWA

Przed przystąpieniem do przetwarzania danych osobowych pracownicy:

- zapoznają się z obowiązkami i odpowiedzialnością za nieprzestrzeganie obowiązujących zasad przetwarzania i ochrony danych osobowych, (zał. 1 PB LUW)
- zapoznają się z przepisami i instrukcjami obowiązującymi w tym zakresie, (zał. 2 PB LUW)
- zobowiązują się do zachowania w tajemnicy danych do których mają dostęp oraz sposobów ich zabezpieczania. (zał. 3 PB LUW)
- otrzymują imienne upoważnienie. (zał. 4 PB LUW)

REALIZACJA POLITYKI BEZPIECZEŃSTWA

Osoby upoważnione do przetwarzania danych osobowych wykonują zadania zgodnie z nadanymi uprawnieniami i chronią dane przed:

- dostępem osób nieuprawnionych,
- naruszeniem ochrony danych osobowych przez inne osoby zatrudnione przy przetwarzaniu danych,
- uszkodzeniem,
- zniszczeniem,
- nieuzasadnioną modyfikacją,
- nielegalnym ujawnieniem lub pozyskaniem.

ODPOWIEDZIALNOŚĆ KARNA

Art. 49 ustawy o ochronie danych osobowych

1. *Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

2. *Jeżeli powyższy czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3 (art. 49 UODO).*

ODPOWIEDZIALNOŚĆ KARNA

Art. 51 ustawy o ochronie danych osobowych

1. *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

2. *Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

ODPOWIEDZIALNOŚĆ KARNA

Art. 52 ustawy o ochronie danych osobowych

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

ODPOWIEDZIALNOŚĆ KARNA

Brak spełnienia obowiązku zgłoszenia zbioru do rejestracji – *podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.* Art. 53

Niespełnienie obowiązku informacyjnego wobec osoby której dane dotyczą – *podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.* Art. 54

Udaremnianie lub utrudnianie wykonania czynności kontrolnych inspektorowi – *podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.* Art. 54a

Dziękuję Państwu za uwagę

Małgorzata Koszewska

Administrator Bezpieczeństwa Informacji

Lubelski Urząd Wojewódzki
w Lublinie