RODO w działalności biegłych sądowych

W jakiej roli zdefiniowanej w RODO występuje biegły sądowy przetwarzający dane osobowe na zlecenie Sądu ?

- Podmiot przetwarzający? - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; art. 4 pkt. 8 RODO
- Strona trzecia? - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe, art. 4 pkt. 9 RODO
- Odbiorca danych? - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania; art. 4 pkt. 9 RODO
- Osoba należąca do personelu Administratora? – czy decyzje o ustanowieniu biegłym i odebrane od biegłego ślubowanie jest poleceniem przetwarzania danych i upoważnieniem w rozumieniu art. 29 RODO?

Cechy operacji przetwarzania danych związanych z przygotowaniem opinii eksperckiej dla potrzeb postępowania sądowego

- Przetwarzanie przez biegłego danych osobowych szczególnych kategorii, co zwiększa ryzyko naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych,
- Różnorodność dziedzin i specjalizacji powoduje, że niemożliwe wydaje się stworzenie przez Administratora – Sąd, szczegółowego wykazu kategorii przetwarzanych danych w związku z powierzaniem biegłych przetwarzania danych w celu wydania opinii,
- Cel przetwarzania danych wyznaczony jest treścią wydanego w toku postępowania sądowego postanowienia o dopuszczeniu dowodu opinii biegłego,
- Zakres przetwarzanych danych w celu wydania opinii jest determinowany treścią postanowienia Sądu i wymogami opinii biegłego właściwymi dla danej dziedziny,
- Wymagania, jakie musi spełniać ekspert by wykonywać opinie na zlecenie sądu, dają gwarancję realizacji przesłanki prawidłowości przetwarzania danych osobowych, o których mowa w art. 5 ust. 1d

Cechy operacji przetwarzania danych związanych z przygotowaniem opinii eksperckiej dla potrzeb postępowania sądowego

- Przewlekłość sporządzania opinii a zasada ograniczenia przechowywania danych,
- Kwalifikowany charakter danych przetwarzanych przy wydawaniu opinii a adekwatność stosowanych środków zabezpieczających komunikację na linii biegły – Sąd,
- Czy utrata, zniszczenie, zagubienie akt sądowych jest naruszeniem ochrony danych podlegającym obowiązkowemu zgłoszeniu do PUODO?
- Czy właściwość organu nadzorczego obejmuje działalność biegłego sądowego?
- Jakie są ograniczenia stosowania RODO w związku z działalnością biegłego sądowego?

Podstawowe informacje i definicje

Co to jest RODO/GDPR i jakie są powody wdrożenia tych przepisów w skali UE?

Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) / General Data Protection Regulation (GDPR) to przepisy przyjęte przez Parlament Europejski i Radę Unii Europejskiej w 27 kwietnia 2016 roku, które zaczęły obowiązywać 25 maja 2018 r. Celem nowej regulacji jest wprowadzenie takich przepisów, które byłyby aktualne niezależnie od postępów rozwoju technologii. Rozporządzenie obowiązuje we wszystkich krajach UE wprost, a w Polce zastępuje ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Podstawowe informacje i definicje

Motyw 6 preambuły RODO:

Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.

Podstawowe informacje i definicje

Rozporządzenie ma na celu przyczyniać się do:

- tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej,
- postępu społeczno-gospodarczego,
- wzmacniania i konwergencji gospodarek na rynku wewnętrznym,
- pomyślności ludzi.

Podstawowe informacje i definicje

Kogo dotyczy RODO?

Przepisy obejmują wszystkie podmioty, które gromadzą i wykorzystują dane dotyczące osób fizycznych. Zmiany dotyczą zarówno firm, jak i administracji. RODO musiały wdrożyć wszystkie organy administracji publicznej. Do tej pory nie było takiego obowiązku. Teraz zarówno te duże firmy, czy urzędy, jak i te małe kilku-, czy kilkunastoosobowe firmy, sklepy internetowe, szkoły, ośrodki pomocy społecznej czy domy kultury itp. muszą przetwarzać dane osobowe zgodnie z prawem i być zdolnym by to wykazać.

Podstawowe informacje i definicje

Motyw 20 preambuły RODO:

Niniejsze rozporządzenie ma zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości.

Podstawowe informacje i definicje

Motyw 20 preambuły RODO:

Powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych.

Podstawowe informacje i definicje

Motyw 19 preambuły RODO

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz swobodny przepływ takich danych podlegają szczególnemu aktowi prawnemu Unii. Niniejsze rozporządzenie nie powinno zatem mieć zastosowania do czynności przetwarzania w tych celach.

Wyłączenie stosowania RODO w działalności organów ścigania – stosowanie tzw. dyrektywy policyjnej dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Podstawowe informacje i definicje

Dyrektywa policyjna cd.

- Warto nadmienić, że przepisy dyrektywy policyjnej miały zostać transponowane do krajowego porządku prawnego do 6 maja 2018 roku, a nie zostały. W związku z powyższym, aby nie powstała luka w prawie w zakresie podstawy prawnej przetwarzania danych osobowych, częściowo pozostawiono jako obowiązującą ustawę z 29 sierpnia 1997 roku o ochronie danych osobowych.
- Część przepisów dawnej ustawy zachowała moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie.

Akty prawne i inne dokumenty regulujące materię ochrony danych osobowych

System ochrony danych osobowych oparty jest na stosownych przepisach prawa międzynarodowego i krajowego oraz polskich normach, a także wytycznych właściwych organów UE i RP odnoszących się do tematyki zarządzania bezpieczeństwem informacji oraz ochrony danych osobowych. W szczególności realizuje wymagania zawarte w:

- rozporządzeniu 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),
- ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r, .poz. 1000),
- rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113),
- zarządzeniu Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych Dz. Urz. MS z 2012 r. poz. 93,
- normach z rodziny ISO/IEC 27000,
- wytycznych Grupy Roboczej art. 29,
- wytycznych i opiniach Prezesa Urzędu Ochrony Danych Osobowych,

Akty prawne i inne dokumenty regulujące materię ochrony danych osobowych

W sądach powszechnych gwarancję bezpieczeństwa informacji i ochrony danych osobowych daje wdrożony i utrzymywany System Zarządzania Bezpieczeństwem Informacji, w którego skład wchodzi m.in.

- Polityka Bezpieczeństwa Informacji (PBI),
- Polityka Ochrony Danych Osobowych (PODO),
- Polityka Bezpieczeństwa Systemu Teleinformatycznego (PBST),
- Polityki Bezpieczeństwa Systemów Informatycznych (PBSI)
- Regulamin Użytkownika Systemów Teleinformatycznych,
- Procedury Zarządzania Bezpieczeństwem Informacji i Ochroną Danych Osobowych,
- Inne zarządzenia Prezesa i Dyrektora Sądu wdrażające środki fizyczne, techniczne i organizacyjne bezpieczeństwa danych

Podstawy prawne przetwarzania danych osobowych w sądach powszechnych

PODSTAWY PRAWNE PRZETWARZANIA DANYCH (PRZESŁANKI LEGALIZUJĄCE PRZETWARZANIE DANYCH)W WYMIARZE SPRAWIEDLIWOŚCI NALEŻY ROZPATRYWAĆ WG KATEGORII PODMIOTÓW, KTÓRYCH DANE SĄ PRZETWARZANE

Podstawy prawne przetwarzania danych osobowych w sądach powszechnych

W przypadku danych osobowych uczestników postępowania sądowego (strony postępowania i ich pełnomocnicy, świadkowie, biegli sądowi, lekarze sądowi, mediatorzy, adwokaci i radcy prawni, osoby zainteresowane, i inni Interesanci Sądu) – dane przetwarzane są w celu wykonania zadań realizowanych w ramach sprawowania władzy publicznej powierzonej Sądowi Okręgowemu w Radomiu, tzn. sprawowania wymiaru sprawiedliwości i innych zadań z zakresu ochrony prawnej;

Podstawy prawne przetwarzania danych osobowych w sądach powszechnych

- podstawa prawna przetwarzania danych w związku ze sprawowaniem wymiaru sprawiedliwości zawarta jest w art. 6 ust. 1 e RODO oraz przepisach szczególnych regulujących działalność sądów powszechnych w tym m.in.

Podstawy prawne przetwarzania danych osobowych w sądach powszechnych

- ustawie z dnia 27 lipca 2001 r. Prawo ustroju sądów powszechnych,
- ustawie z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego,
- ustawie z dnia z dnia 6 czerwca 1997 r. Kodeks postępowania karnego,
- ustawie z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia ,
- ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 z późn. zm.),

Podstawy prawne przetwarzania danych osobowych w sądach powszechnych

- rozporządzeniu Ministra Sprawiedliwości z dnia 23 grudnia 2015 r. Regulamin urzędowania sądów powszechnych (Dz.U. poz. 2316),
- rozporządzenie Ministra Sprawiedliwości z dnia 9 maja 2012 r. w sprawie skarg i wniosków dotyczących działalności sądów powszechnych (Dz. U. poz. 524),
- ustawa z dnia 14 czerwca 1960r. Kodeks postępowania administracyjnego (Dz.U. 2017r. poz. 1257 j.t.),
- zarządzeniu Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej z późn. zm.,
- ustawie z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz.U z 2016r. poz. 1764 j.t. ze zm.), rozporządzeniu z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej i innych ustawach szczególnych i aktach wykonawczych regulujących działalność sądów powszechnych,
- i wielu innych

Nowe zasady ochrony danych w praktyce Sądu

Jak będzie wyglądał model systemu ochrony danych osobowych w sądach

Pion wymiaru sprawiedliwości

Nadzór wyspecjalizowanych organów powołanych ustawodawstwem państwa członkowskiego
w ramach wymiaru sprawiedliwości

Nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy będzie oparty o poniższy model:
1) w zakresie działalności sądu rejonowego – prezes sądu okręgowego;
2) w zakresie działalności sądu okręgowego – prezes sądu apelacyjnego;
3) w zakresie działalności sądu apelacyjnego – Krajowa Rada Sądownictwa

Wyznaczony w Sądzie IOD nie może monitorować przetwarzania danych w wymiarze sprawiedliwości

Pion Sądu jako jednostki sektora finansów publicznych

Nadzór Prezesa Urzędu Ochrony Danych Osobowych w zakresie nie związanym z orzekaniem i postępowaniem sądowym (w szczególności - realizacja zadań administracyjnych Sądu, ochrona danych w zatrudnieniu, ochrona danych w zawieraniu umów, ochrona danych w fazie domyślnej i w fazie projektowania)

Wyznaczenie niezależnego Inspektora Ochrony Danych, który nadzoruje wszystkie operacje przetwarzania i jest punktem kontaktowym dla organu nadzorczego PUODO

Nowe zasady ochrony danych w praktyce Sądu

Działalności orzecznicza

„Instytucje publiczne, w tym także sądy, jako podmioty o szczególnym znaczeniu z punktu widzenia funkcjonowania państwa, ale także z punktu widzenia praw obywateli, muszą wejście w życie RODO potraktować szczególnie poważnie, (…) mieć świadomość odpowiedzialności za prawidłowe przetwarzanie danych osobowych, którymi dysponują" – dr Edyta Bielak-Jomaa, GIODO

„Zasada podejścia opartego na ryzyku wyznaczająca zakres stosowanych środków zabezpieczenia danych zadziała w ten sposób, że zakres danych przetwarzanych w sądach – dane dotyczące skazań, dane o stanie zdrowia, dane genetyczne itp. – wymusi stosowanie zwiększonych środków zabezpieczenia danych. Z dużym prawdopodobieństwem trzeba będzie też przeprowadzić ocenę skutków dla ochrony danych" - dr **Paweł Litwiński** Ekspert Komisji Europejskiej do spraw ochrony danych osobowych.

Nowe zasady ochrony danych w praktyce Sądu

- Mając na względzie, że stosownie do art. 178 ust. 1 Konstytucji Rzeczpospolitej Polskiej sędziowie w sprawowaniu swojego urzędu są niezawiśli i podlegają tylko konstytucji i ustawom, a przetwarzanie danych osobowych w postępowaniach sądowych oraz w rejestrach sądowych określają przepisy ustaw szczególnych regulujących poszczególne procedury sądowe oraz rejestry sądowe, za celowe i uzasadnione uznano wyłączenie stosowania niektórych przepisów RODO.

Nowe zasady ochrony danych w praktyce Sądu

Artykuł 23 RODO
Ograniczenia

1.Prawo Unii lub **prawo państwa członkowskiego**, któremu podlegają administrator danych lub podmiot przetwarzający, **może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym**:

a) bezpieczeństwu narodowemu;
b) obronie;
c) bezpieczeństwu publicznemu
d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
f) ochronie niezależności sądów i postępowania sądowego;
g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g);
i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
j) egzekucji roszczeń cywilnoprawnych.

Nowe zasady ochrony danych w praktyce Sądu

Według projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 zmiany ograniczające stosowanie niektórych zapisów RODO w obszarze wymiaru sprawiedliwości mają dotyczyć zgodnie z art. 75 i następne niniejszej ustawy wyłączenia m.in. praw osób których dane dotyczą odnośnie biegłych sądowych, ławników, mediatorów, kandydatów na syndyków, braku obowiązku zawiadamiania osób których dane dotyczą o naruszeniach ochrony ich danych oraz zakresu obowiązywania ogólnych zasad przetwarzania danych.

„Art. 175dc. Do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych, przepisów art. 13-16 oraz art. 18-21 rozporządzenia 2016/679 nie stosuje się. „

Nowe zasady ochrony danych w praktyce Sądu

Jak będzie wyglądał model systemu ochrony danych osobowych w sądach

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 art. 75 i następne przewiduje nowelizację ustawy z dnia 27 lipca 2001 r. Prawo ustroju sądów powszechnych pod kątem dostosowania operacji przetwarzania danych osobowych w zakresie działalności sądów i przewiduje dodatkowo:

- Określenie, kto jest Administratorami danych osobowych referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów **(prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości, w zakresie realizowanych zadań),**

- Określenie modelu nadzoru nad operacjami przetwarzania związanymi ze sprawowaniem wymiaru sprawiedliwości – **organami nadzorczymi mają być Prezesi Sądów wyższej instancji, nad Sądem w którym dokonuje się przetwarzania danych.**

Jak RODO zmienia podejście do ochrony danych osobowych

NOWOŚCI

- ★ Proaktywne podejście do ochrony danych osobowych
- ★ Raportowanie do GIODO o własnych naruszeniach
- ★ U d Wyłączenie uprawnień organu nadzorczego w wymiarze sprawiedliwości
- ★ Wysokie kary pieniężne

ZMIANY

- Nowe obowiązki Procesora ★
- Rejestr czynności przetwarzania ★
- Zmiana statusu ABI > IOD ★
- Zwiększenie uprawnień osób których dane dotyczą ★

Jak RODO zmienia podejście do ochrony danych osobowych

Przed RODO	RODO
Różne przepisy w każdym kraju członkowskim UE	Jednolite rozporządzenie obowiązujące w takim samym brzmieniu na terenie całej UE
Podejście od strony jednorazowej oceny potrzeb ochrony danych osobowych	Podejście zakładające każdorazowo dokonanie analizy ryzyka naruszenia praw i wolności osób fizycznych przed rozpoczęciem przetwarzania danych, ochrona danych jest procesem ciągłym
Możliwość podjęcia działań korygujących po wykryciu naruszenia, by uchronić się przed konsekwencjami ze strony organu nadzorczego	Zgłaszanie naruszeń ochrony danych organowi nadzorczemu w ciągu 72 godzin od wykrycia naruszenia. Istotne ograniczenie lub brak możliwości podjęcia działań korygujących po wykryciu naruszenia ochrony danych osobowych
Ograniczone realne możliwości egzekwowania zgodności z przepisami	Odstraszająca wysokość kar administracyjnych

Jak RODO zmienia podejście do ochrony danych osobowych

RODO wzmacnia prawa obywateli

Przejrzystość - Obywatel ma prawo uzyskania informacji na temat sposobu przetwarzania jego danych osobowych

Prawo żądania sprostowania danych, ograniczenia przetwarzania, prawo przeniesienia danych, prawo do bycia zapomnianym, prawo do otrzymania kopii danych, sprzeciw wobec przetwarzania danych

Wzmocnione prawo egzekwowania roszczeń – obywatel ma prawo dochodzić odszkodowania w sądzie cywilnym

Podstawowe informacje i definicje

„DANE OSOBOWE” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Podstawowe informacje i definicje

Dane osobowe szczególnych kategorii to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych dane genetyczne, dane biometryczne, seksualności lub orientacji seksualnej, dane o stanie zdrowia zmierzające do jednoznacznego zidentyfikowania osoby fizycznej.

Art. 9 ust. 1 RODO zawiera zakaz przetwarzania w/w danych, chyba że wystąpi jedna z przesłanek wyminionych w art. 9 ust. 2 RODO – np. pkt. f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

Podstawowe informacje i definicje

Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa przez podmioty nie upoważnione na podstawie przepisów prawa

- Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO wolno dokonywać **wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych**

Podstawowe informacje i definicje

„Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Podstawowe informacje i definicje

„Podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Administratorzy są zobowiązani do zawierania z podmiotami przetwarzającymi **umów powierzenia danych osobowych** i audytowania przestrzegania ich zapisów.

Podstawowe informacje i definicje

„Przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

- **zbieranie,**
- **utrwalanie,**
- **organizowanie,**
- **porządkowanie,**
- **przechowywanie,**
- **adaptowanie lub modyfikowanie,**
- **pobieranie,**
- **przeglądanie,**
- **wykorzystywanie,**
- **ujawnianie poprzez przesłanie,**
- **rozpowszechnianie lub innego rodzaju udostępnianie,**
- **dopasowywanie lub łączenie,**
- **ograniczanie,**
- **usuwanie lub niszczenie;**

Podstawowe informacje i definicje

„**Profilowanie**” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

Podstawowe informacje i definicje

„Pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Podstawowe informacje i definicje

„Dane genetyczne” należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji.

Podstawowe informacje i definicje

„Dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

Podstawowe informacje i definicje

„Dane o stanie zdrowia” to wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą, w szczególności:

- informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej);
- numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;
- informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;
- oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

Zgodnie z regułą rozliczalności Administratora, o której mowa w art. 5 ust. 2 RODO Sąd Okręgowy w Radomiu jest zobowiązany zapewnić i wykazać, że przetwarzanie danych osobowych opiera się na następujących zasadach:

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

1. Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą **(„zgodność z prawem, rzetelność i przejrzystość”);**

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

2. Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („**ograniczenie celu**”);

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

3. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**”);

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

4. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane **(„prawidłowość”);**

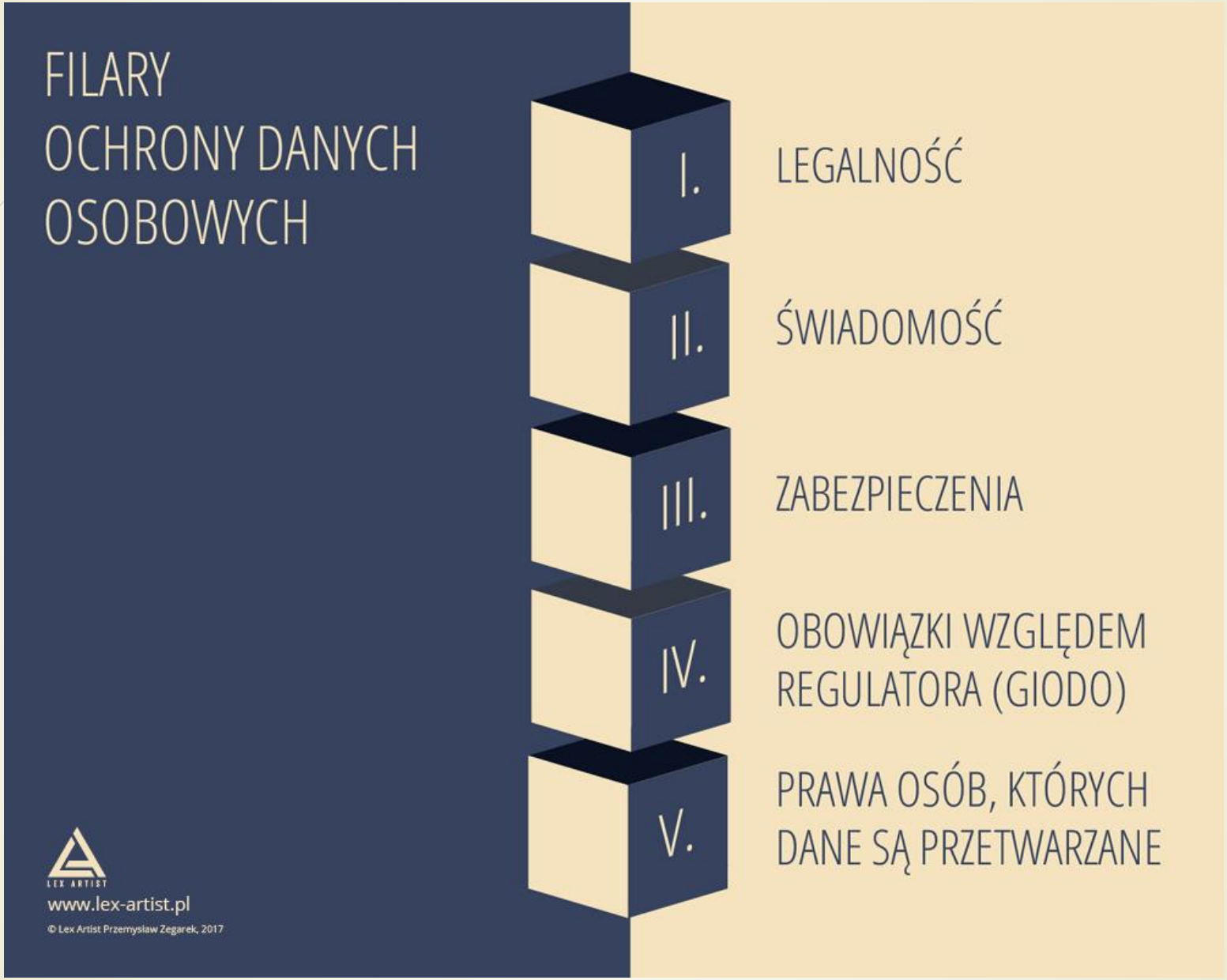
Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

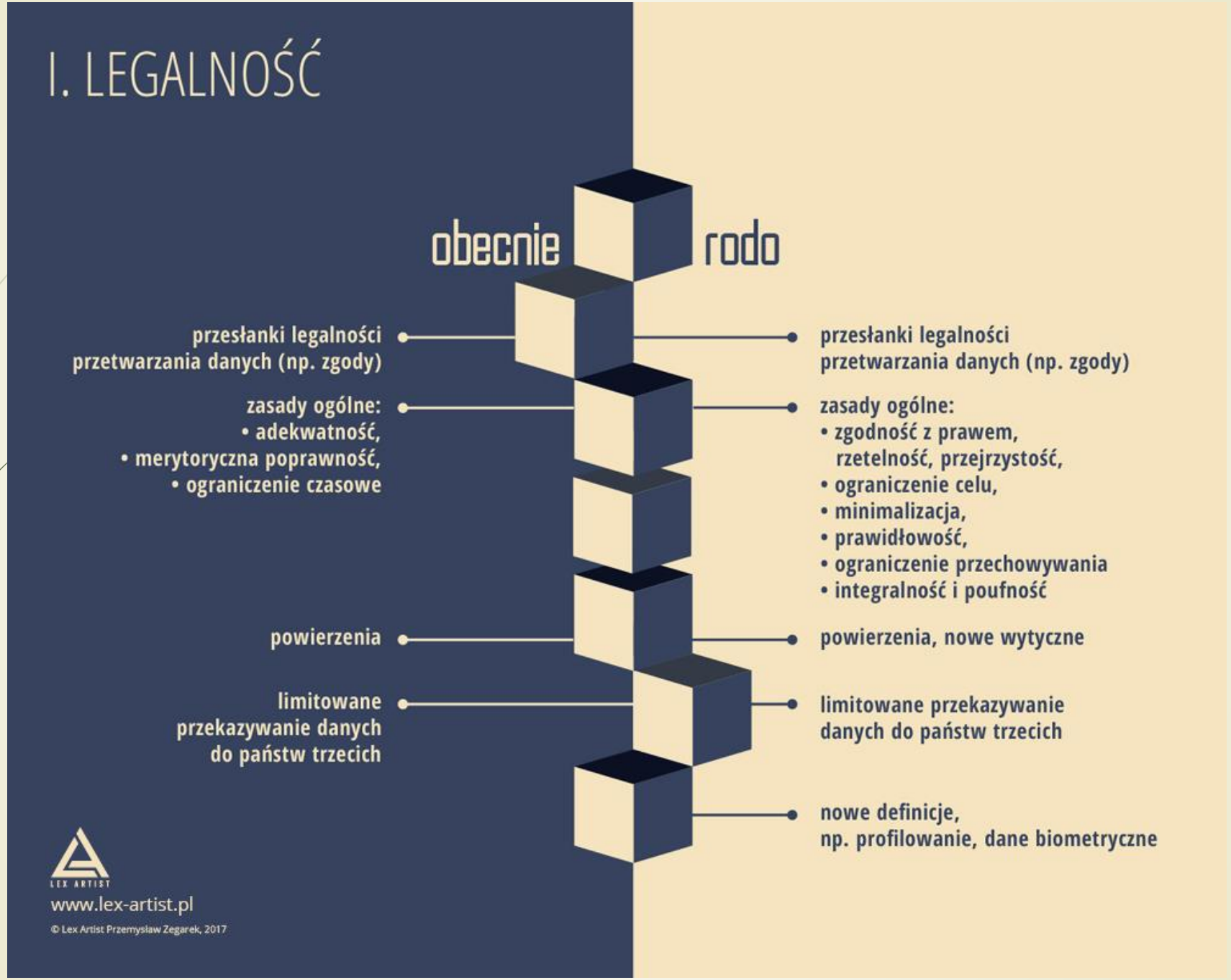
5. Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą **(„ograniczenie przechowywania”);**

Zasady dotyczące przetwarzania danych osobowych, Artykuł 5 RODO

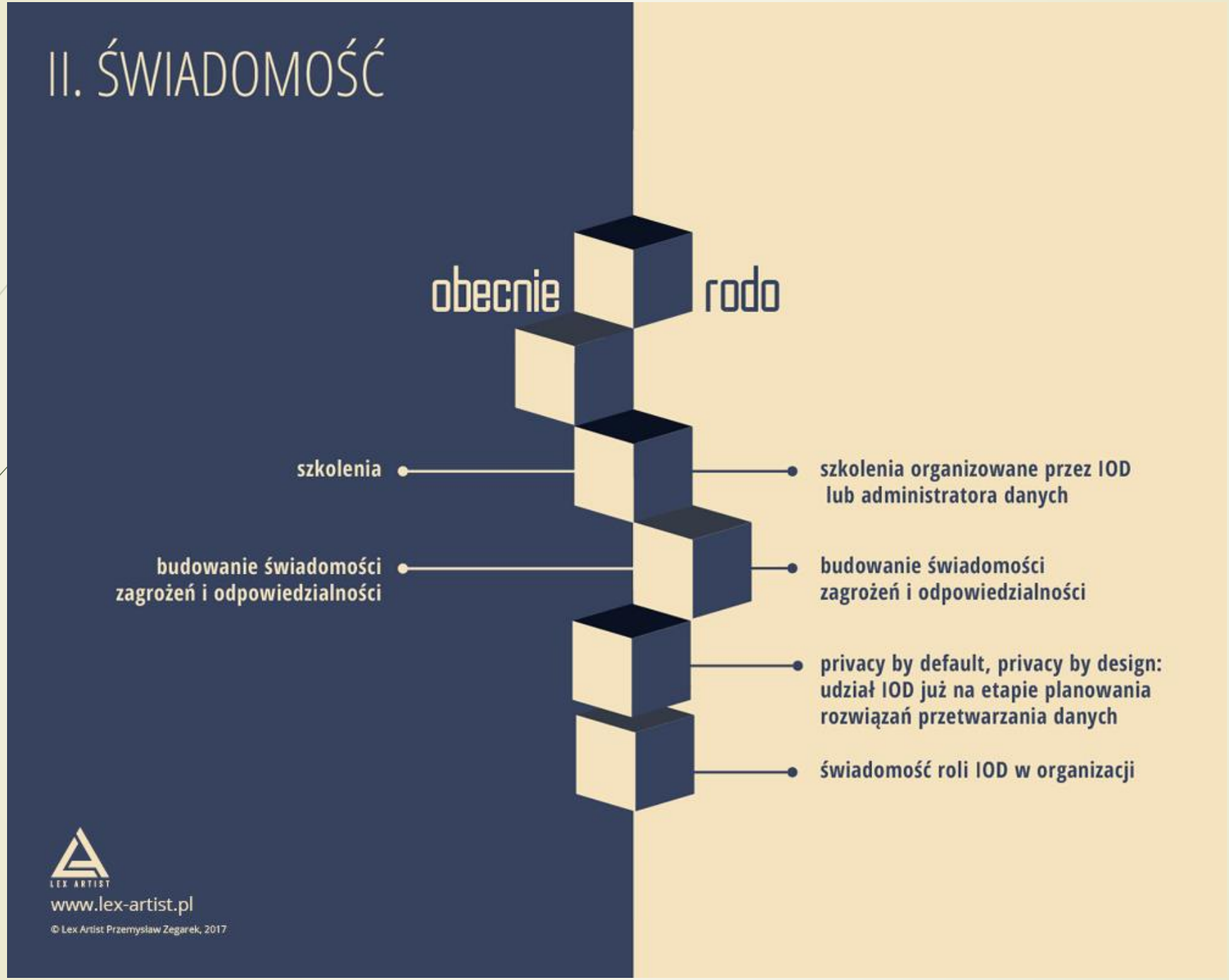
6. Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**„integralność i poufność”).**

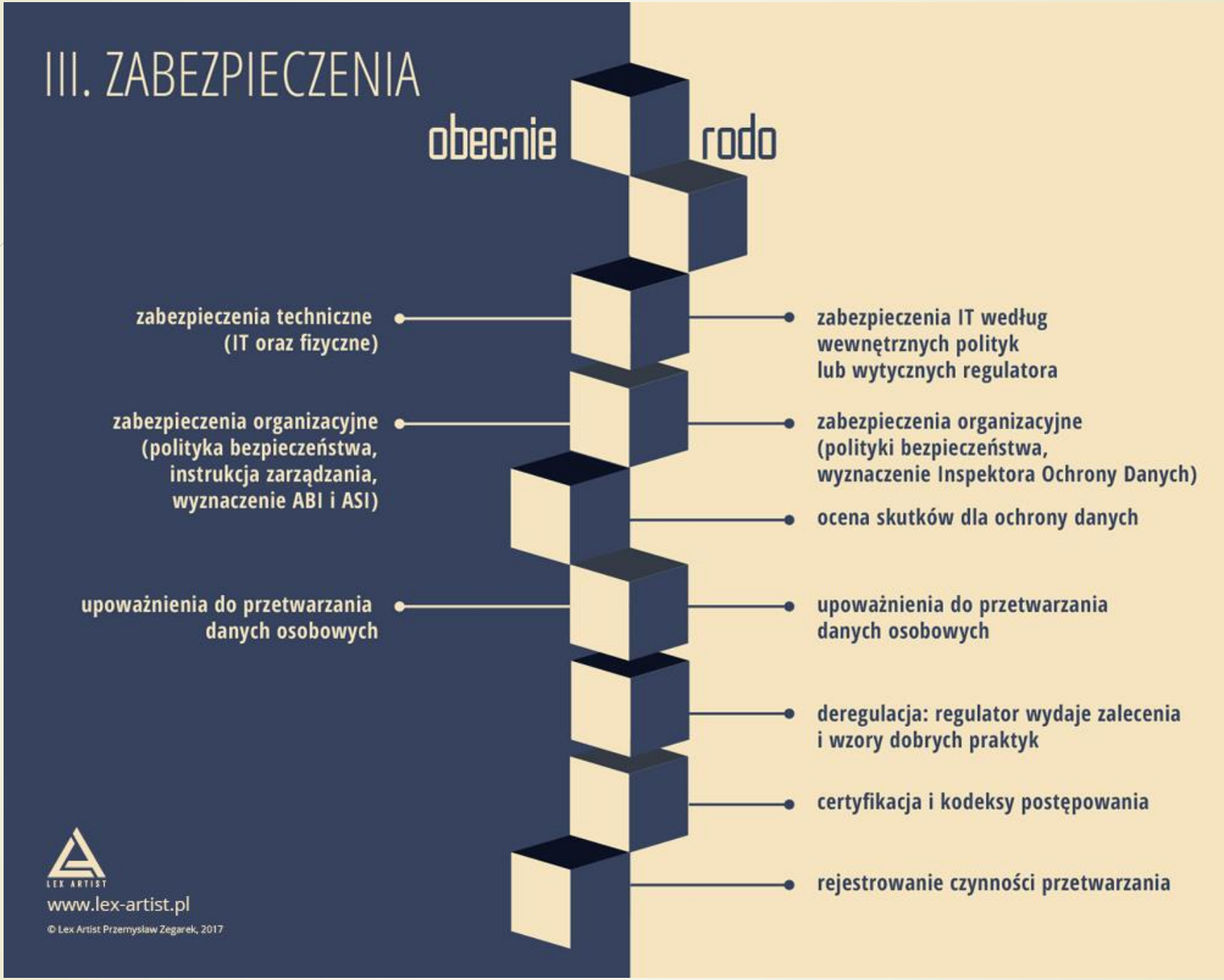
V filarów ochrony danych osobowych


FILARY
OCHRONY DANYCH
OSOBOWYCH
I.
LEGALNOŚĆ
II.
ŚWIADOMOŚĆ
III.
ZABEZPIECZENIA
IV.
OBOWIĄZKI WZGLĘDEM
REGULATORA (GIODO)
V.
PRAWA OSÓB, KTÓRYCH
DANE SĄ PRZETWARZANE
LEX ARTIST
www.lex-artist.pl
© Lex Artist Przemysław Zegarek, 2017

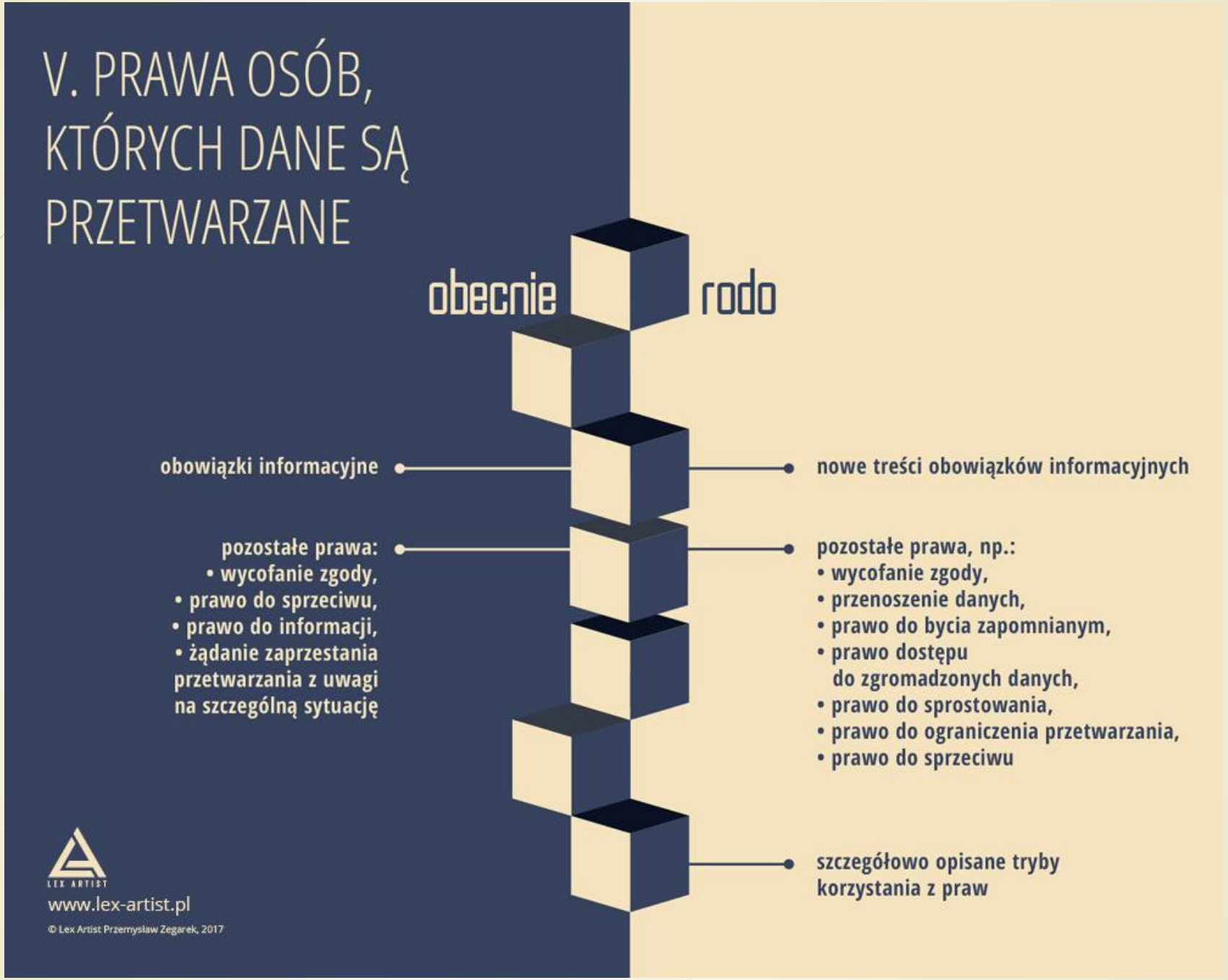

I. LEGALNOŚĆ
obecnie
rodo
przesłanki legalności przetwarzania danych (np. zgody)
zasady ogólne:
• adekwatność,
• merytoryczna poprawność,
• ograniczenie czasowe
powierzenia
limitowane przekazywanie danych do państw trzecich
przesłanki legalności przetwarzania danych (np. zgody)
zasady ogólne:
• zgodność z prawem, rzetelność, przejrzystość,
• ograniczenie celu,
• minimalizacja,
• prawidłowość,
• ograniczenie przechowywania
• integralność i poufność
powierzenia, nowe wytyczne
limitowane przekazywanie danych do państw trzecich
nowe definicje, np. profilowanie, dane biometryczne
LEX ARTIST
www.lex-artist.pl
© Lex Artist Przemysław Zegarek, 2017

II. ŚWIADOMOŚĆ

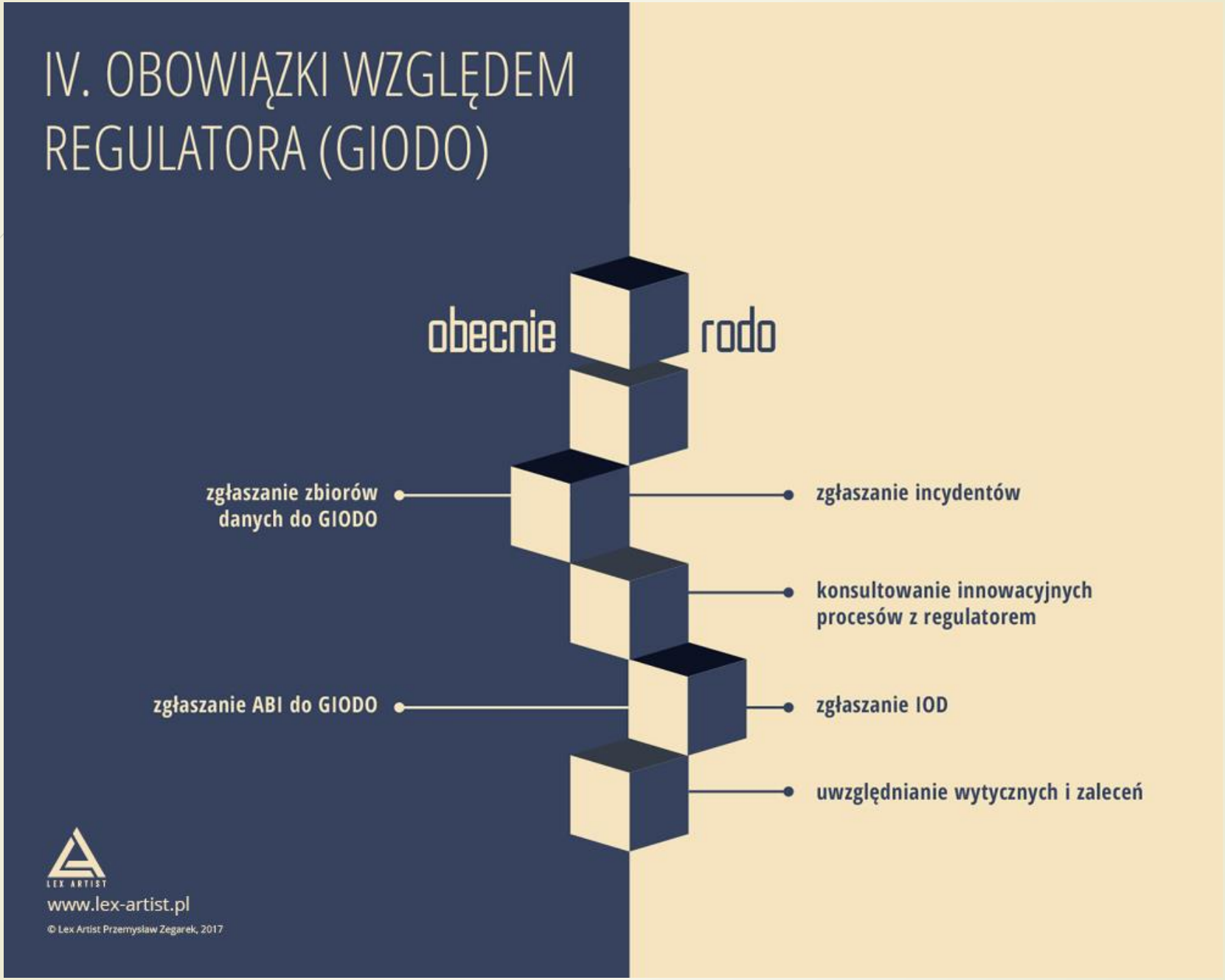



III. ZABEZPIECZENIA
obecnie
rodo
zabezpieczenia techniczne (IT oraz fizyczne)
zabezpieczenia organizacyjne (polityka bezpieczeństwa, instrukcja zarządzania, wyznaczenie ABI i ASI)
upoważnienia do przetwarzania danych osobowych
zabezpieczenia IT według wewnętrznych polityk lub wytycznych regulatora
zabezpieczenia organizacyjne (polityki bezpieczeństwa, wyznaczenie Inspektora Ochrony Danych)
ocena skutków dla ochrony danych
upoważnienia do przetwarzania danych osobowych
deregulacja: regulator wydaje zalecenia i wzory dobrych praktyk
certyfikacja i kodeksy postępowania
rejestrowanie czynności przetwarzania
LEX ARTIST
www.lex-artist.pl
© Lex Artist Przemysław Zegarek, 2017

V. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE



IV. OBOWIĄZKI WZGLĘDEM REGULATORA (GIODO)



Inspektor Ochrony Danych (IOD) i jego zadania

Obowiązki inspektora ochrony danych skupiają się przede wszystkim wokół zadań z zakresu sprawdzania, czy działania Administratora Danych są wykonywane zgodnie z obowiązującym prawem oraz wokół kontaktowania się i współpracowania z organem nadzorczym (PUODO).

Inspektor Ochrony Danych (IOD) i jego zadania

– informowanie administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich, a wynikających z RODO oraz innych przepisów, dotyczących ochrony danych osobowych,
– doradzanie powyższym w metodach wywiązywania się z tych obowiązków,
– monitorowanie przestrzegania rozporządzenia oraz innych przepisów dotyczących ochrony danych osobowych, zwiększanie świadomość pracowników na temat tych zagadnień, przeprowadzanie szkoleń,
– udzielanie na żądanie Administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania,

Inspektor Ochrony Danych (IOD) i jego zadania

– zachowywanie w tajemnicy szczegóły dotyczące swoich zadań

– odpowiadanie na kontakt ze strony osób, które przekazały swoje dane osobowe, a które są zainteresowane prawami, jakie im przysługują po wprowadzeniu RODO oraz szczegółami przetwarzania tych danych,

– współpraca z organem nadzorczym (PUODO) oraz występowanie jako osoba kontaktowa dla niego (na przykład w sytuacji, kiedy dojdzie do naruszenia ochrony tych danych i ich administrator, zgodnie z rozporządzeniem, zgłosi ten fakt do PUODO w obowiązkowym terminie do 72 godzin).

Incydenty bezpieczeństwa danych a obowiązki notyfikacyjne Administratorów danych wobec organu nadzorczego

Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Nie chodzi wyłącznie o przypadki włamań do systemów informatycznych, ale tak prozaiczne zdarzenia, jak np. zgubienie laptopa czy wysłanie e-maila do niewłaściwej osoby (o ile oczywiście prowadzą do nieuprawnionego dostępu do danych osobowych).

Incydenty bezpieczeństwa danych a obowiązki notyfikacyjne Administratorów danych wobec organu nadzorczego

Naruszenia ochrony danych osobowych, które będą powodowały **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, zgodnie z ogólnym rozporządzeniem o ochronie danych, **trzeba będzie zgłaszać zarówno organowi nadzorczemu, jak i osobom, których danych dotyczyło naruszenie.**

Obowiązek notyfikacji jest zatem elementem usuwania skutków incydentów bezpieczeństwa mogących mieć istotny wpływ na interesy osoby fizycznej i wynika z powszechnie akceptowanej i jak się wydaje oczywistej zasady bezpieczeństwa przetwarzania danych.

Incydenty bezpieczeństwa danych a obowiązki notyfikacyjne Administratorów danych wobec organu nadzorczego

Incydenty wynikające z błędu człowieka:

- Ujawnienie informacji osobom nieupoważnionym
- Wyrzucenie do kosza niezniszczonych dokumentów
- Wyrzucenie do kosza sprawnego nośnika danych
- Ujawnienie innym pracownikom lub osobom postronnym haseł dostępu do systemów informatycznych
- Naruszenie merytorycznej poprawności danych przechowywanych w zasobach jednostki
- Utrata lub uszkodzenie dokumentów lub elektronicznego nośnika danych
- Instalowanie programów lub wgrywanie programów typu portable nieautoryzowanych pod kątem bezpieczeństwa przez dział informatyki

Konsekwencje prawne naruszenia zasad przetwarzania danych oraz nowe zasady kontroli

Art. 25 Naruszenie zasad ochrony danych osobowych w fazie projektowania (privacy by design) oraz domyślna ochrona danych (privacy by default)	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 29 Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 30 Rejestrowanie czynności przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 31 Współpraca z organem nadzorczym	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 32 Bezpieczeństwo przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa

Konsekwencje prawne naruszenia zasad przetwarzania danych oraz nowe zasady kontroli

Art. 5 Naruszenie zasad dotyczących przetwarzania danych osobowych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 7 Naruszenie warunków wyrażenia zgody na przetwarzanie danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 15 Naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 16 Naruszenie wykonania prawa do sprostowania i usuwania danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa

Konsekwencje prawne naruszenia zasad przetwarzania danych oraz nowe zasady kontroli

Zgodnie ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych

Art. 101. Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż:
1) jednostka sektora finansów publicznych,
2) instytut badawczy,
3) Narodowy Bank Polski
– w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Art. 102. 1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:
1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
2) instytut badawczy;
3) Narodowy Bank Polski.
2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.
3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679

Dziękuję za uwagę