URZĄD OCHRONY DANYCH OSOBOWYCH

WYZWANIA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH W DZIAŁALNOŚCI JEDNOSTEK SAMORZĄDU TERYTORIALNEGO

UODO RUSZA W KRAJ

Gdańsk, 31.01.2025 r.

Personal Data Protection Office
2 Stawki st., 00-193 Warsaw, POLAND
www.uodo.gov.pl/en
tel. +48 22 531 03 00

UODO RUSZA W KRAJ

Rozpoczęliśmy cykl **ogólnopolskich spotkań** z mieszkańcami, organami administracji samorządowej i rządowej w poszczególnych województwach.

W ramach tej inicjatywy priorytetowo traktujemy problematykę ochrony danych osobowych w jednostkach samorządu terytorialnego (JST).

Podobne spotkania prezesa i pracowników Urzędu Ochrony Danych Osobowych odbywać się będą w kolejnych województwach w ramach i w miarę uzgodnień dokonywanych z władzami wojewódzkimi, powiatowymi i gminnymi.

WSPÓŁPRACA UODO Z JST

Spotkania z organizacjami zrzeszającymi JST

- ✓Unia Metropolii Polskich (24.06.2024 r.),
- ✓Związek Miast Polskich (6.09.2024 r.),
- ✓Związek Gmin Wiejskich RP (26.09.2024 r.),
- ✓Związek Powiatów Polskich (19.11.2024 r.).

Spotkanie ze Związkiem Województw RP (24.11.2024 r.)

Spotkanie z Narodowym Instytutem Samorządu Terytorialnego (25.11.2024 r.)

Współpraca z organizacjami zrzeszającymi Inspektorów Ochrony Danych

Cykl spotkań „UODO RUSZA W KRAJ” [redacted]

Możliwe inicjatywy

Opracowanie **kodeksów postępowania dla JST** w określonych obszarach (np. oświata, opieka przedszkolna, sport, opieka społeczna itd.). W kodeksie należy wyraźnie opisać role i wskazać, kto jest kim w procesie ochrony danych, kto będzie odpowiadał za naruszenie, jaki jest jego zakres odpowiedzialności.

URZĄD OCHRONY DANYCH OSOBOWYCH

Aktualizacja Poradników UODO

- Obowiązki administratorów związane ze zgłaszaniem naruszeń ochrony danych osobowych
- Poradnik dla pracodawców
- Poradnik dotyczący monitoringu wizyjnego

PROGRAM EDUKACYJNY „TWOJE DANE – TWOJA SPRAWA”

URZĄD OCHRONY DANYCH OSOBOWYCH

Program **skierowany do szkół podstawowych, ponadpodstawowych oraz placówek doskonalenia nauczycieli** jest największym systemowym projektem edukacyjnym realizowanym od 2009 roku w celu propagowania wiedzy o ochronie danych osobowych w społeczeństwie, ze szczególnym uwzględnieniem dzieci.

Obecnie realizowana jest jego XV edycja.

Szansa dla uczniów i nauczycieli na rozwijanie praktycznych umiejętności i kompetencji cyfrowych w zakresie ochrony prywatności i danych osobowych.

W ramach Programu organizowane są:
szkolenia, konferencje, webinaria, konkursy, zajęcia lekcyjne, pozalekcyjne i wydarzenia tematyczne skierowane do uczniów, nauczycieli i dyrektorów szkół, a także rodziców.

Nabór do każdej edycji programu rozpoczynamy we wrześniu!

XV EDYCJA PROGRAMU
„TWOJE DANE - TWOJA SPRAWA"

URZĄD OCHRONY DANYCH OSOBOWYCH

Inicjatywa, ma na celu systematyczne podnoszenie świadomości uczniów i nauczycieli w zakresie ochrony danych osobowych. W obliczu dynamicznego rozwoju technologii, zagadnienie to nabiera coraz większego znaczenia, stając się jednym z filarów współczesnego społeczeństwa informacyjnego.

HARMONOGRAM 2024/2025

- **2 WRZEŚNIA -24 PAŹDZIERNIKA 2024** — Rekrutacja
- **10 PAŹDZIERNIKA 2024** — Konferencja inaugurująca
- **24 - 25 PAŹDZIERNIKA 2024** — Szkolenie online dla koordynatorów
- **LISTOPAD 2024 - MAJ 2025** — Webinaria dla uczniów i nauczycieli
- **10 GRUDNIA 2024** — Ogłoszenie Konkursów
- **GRUDZIEŃ 2024 MAJ 2025** — Konkurs dla placówek na najlepsze inicjatywy, konkurs dla uczniów
- **28 STYCZNIA 2025** — Dzień Ochrony Danych Osobowych
- **31 MAJA 2025** — Raporty końcowe
- **CZERWIEC 2025** — Spotkanie podsumowujące, wręczenie nagród

CAŁY OKRES

Inicjatywy edukacyjne, lekcje i wydarzenia tematyczne

Patroni honorowi: Ministerstwo Edukacji i Nauki, Rzecznik Praw Dziecka

Patroni medialni: TVP2, PNŚ, głosnauczycielski, TIK w edukacji, Portal Oświatowy, Polskie Radio dzieciom

DZIAŁALNOŚĆ INSPEKTORÓW OCHRONY DANYCH (IOD) W JST

Gdy dochodzi do naruszenia przepisów dotyczących Inspektorów Ochrony Danych Prezes UODO podejmuje działania **na podstawie art. 58 RODO**

Prezes UODO reagował w razie:

- niewyznaczenia inspektora pomimo takiego obowiązku,
- nieopublikowania na stronie internetowej administratora imienia i nazwiska inspektora lub nieaktualizowania tych informacji,
- obciążania inspektora obowiązkami, które należą do administratora,
- zapisania w regulaminie organizacyjnym, że IOD może być odwołany w każdym czasie,
- nieprawidłowego usytuowania IOD w strukturze organizacyjnej administratora, gdy IOD nie podlegał bezpośrednio najwyższemu kierownictwu,
- niezapewnienia inspektorowi wystarczającej ilości czasu oraz innych zasobów niezbędnych do wykonywania jego zadań,
- niezapewnienia inspektorowi zasobów na podnoszenie wiedzy fachowej,
- pomijania inspektora w sprawach dotyczących przetwarzania danych osobowych (w tym takich, w których administratorzy prosili o opinię UODO nie zwracając się wcześniej o opinię do inspektora).

DZIAŁALNOŚĆ INSPEKTORÓW OCHRONY DANYCH W JSTA

W marcu 2022 r została sformułowana i opublikowana lista 27 pytań obejmująca kluczowe obowiązki administratorów odnoszące się do zagwarantowania IOD prawidłowego statusu i wykonywania zadań **(art. 37 – 39 RODO).**

Prezes UODO przesłał je do ponad 20 administratorów z sektora publicznego i prywatnego. Jeśli wyjaśnienia były niekompletne, lakoniczne lub niepoparte konkretnymi dowodami (rozwiązaniami) – wszczynane były postępowania. Niekiedy konieczne było przeprowadzenie kontroli w siedzibie administratora.

Przykładowe pytania:

- W jaki sposób administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (np. czy zostały opracowane zasady dotyczące tego, jakie sprawy mają być konsultowane z IOD, kto i w jakich sytuacjach powinien zgłaszać się w celu uzyskania konsultacji IOD, czy i na jakich zasadach IOD bierze udział w naradach kierownictwa)?
- W jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?
- Czy administrator przyjął jakiekolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (w szczególności w celu zapewnienia poszanowania gwarancji jego niezależności oraz jego uprawnień w zakresie dostępu do danych osobowych i operacji przetwarzania, włączania we wszystkie sprawy dotyczące ochrony danych osobowych, unikania konfliktu interesów), a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?

DZIAŁALNOŚĆ INSPEKTORÓW OCHRONY DANYCH W JST

URZĄD OCHRONY DANYCH OSOBOWYCH

W 2023 r. w ramach EROD przeprowadzono działanie skoordynowanego egzekwowania prawa (Coordinated Enforcement Framework - CEF), dotyczące pozycji i wyznaczania inspektorów ochrony danych (CEF DPO). W inicjatywie tej uczestniczyło 25 organów ochrony danych z Europejskiego Obszaru Gospodarczego (w tym UODO).

Sprawozdanie z tego działania opublikowano w styczniu 2024 r.

W sprawozdaniu z działania CEF DPO znaczenie niezależności IOD jest wielokrotnie podkreślane:

- rola IOD musi być rozwijana w niezależny sposób, a zarówno organy nadzorcze, jak i wewnętrznie same organizacje muszą prowadzić więcej działań uświadamiających i egzekucyjnych dotyczących niezależności IOD;
- inspektorzy ochrony danych powinni mieć możliwość gromadzenia dowodów w przypadku ingerencji w ich niezależność;
- istnieje ciągle aktualna potrzeba właściwego rozumienia roli IOD i jego znaczenia w zapewnianiu zgodności przetwarzania z prawem.
- przestrzeganie tych wymogów jest szczególnie ważne wobec przepisów UE w dziedzinie cyfrowej (zarówno tych jeszcze procedowanych, jak i tych, które weszły już w życie lub niedawno weszły w życie).

PROBLEMY DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH W JST

URZĄD OCHRONY DANYCH OSOBOWYCH

Kontrola NIK luty 2024 r.:

- Korzystanie z adresów mailowych utworzonych w domenach komercyjnych bez zawarcia wymaganych RODO umów powierzenia przetwarzania danych osobowych.
- Nieprawidłowe przetwarzanie w skrzynkach pocztowych danych osobowych, w tym danych o stanie zdrowia, informacji o korzystaniu ze świadczeń pomocy społecznej.
- Udostępnianie na stronach BIP oświadczeń majątkowych po upływie okresu ich publikacji.
- Nieprawidłowości przy transmisji i publikowaniu posiedzeń organów stanowiących.

Problemy pojawiające się w praktyce UODO:

- **Najważniejsze zagadnienia sygnalizowane w skargach do UODO:** udostępnianie danych osobowych w BIP, w nagraniach z sesji rady w Internecie, w transmisjach na żywo, udostępnienie danych osobowych sygnalisty, itd.
- **Tematyka zgłaszanych do UODO naruszeń ochrony danych:** omyłkowe wysłanie korespondencji, udostępnienie dokumentacji nieuprawnionej osobie, bezpodstawne traktowanie innych podmiotów jako zaufanych odbiorców, zagubienie korespondencji przez operatora pocztowego, wysłanie pod niewłaściwy adres, uszkodzenie/otwarcie przesyłki, zagubienie/kradzież dokumentacji, laptopa, pendrive'a, ransomware.
- **Kontrole:** nieprawidłowe klauzule informacyjne (np. nie wiadomo, kto jest administratorem), brak umów powierzenia, nieprawidłowo wydzielone stanowiska do obsługi interesantów, przechowywanie dokumentacji przez czas dłuższy, niż wskazują przepisy, brak analizy ryzyka, oceny skutków dla ochrony danych.

WYZWANIA TECHNOLOGICZNE W JST

URZĄD OCHRONY DANYCH OSOBOWYCH

Wyzwania technologiczne związane z ochroną danych osobowych:

Cyberzagrożenia

ataki hakerskie, phishing, ransomware to zagrożenia dla bezpieczeństwa danych

Przechowywanie danych w chmurze

ryzyko związane z bezpieczeństwem

Zgodność z regulacjami

zgodność z RODO oraz innymi regulacjami, w tym przede wszystkim w zakresie cyberbezpieczeństwa

Ochrona danych osobowych a sztuczna inteligencja:

Problemy etyczne i prawne

profilowanie, automatyczne decyzje, przejrzystość algorytmów

Ryzyka związane z jakością danych

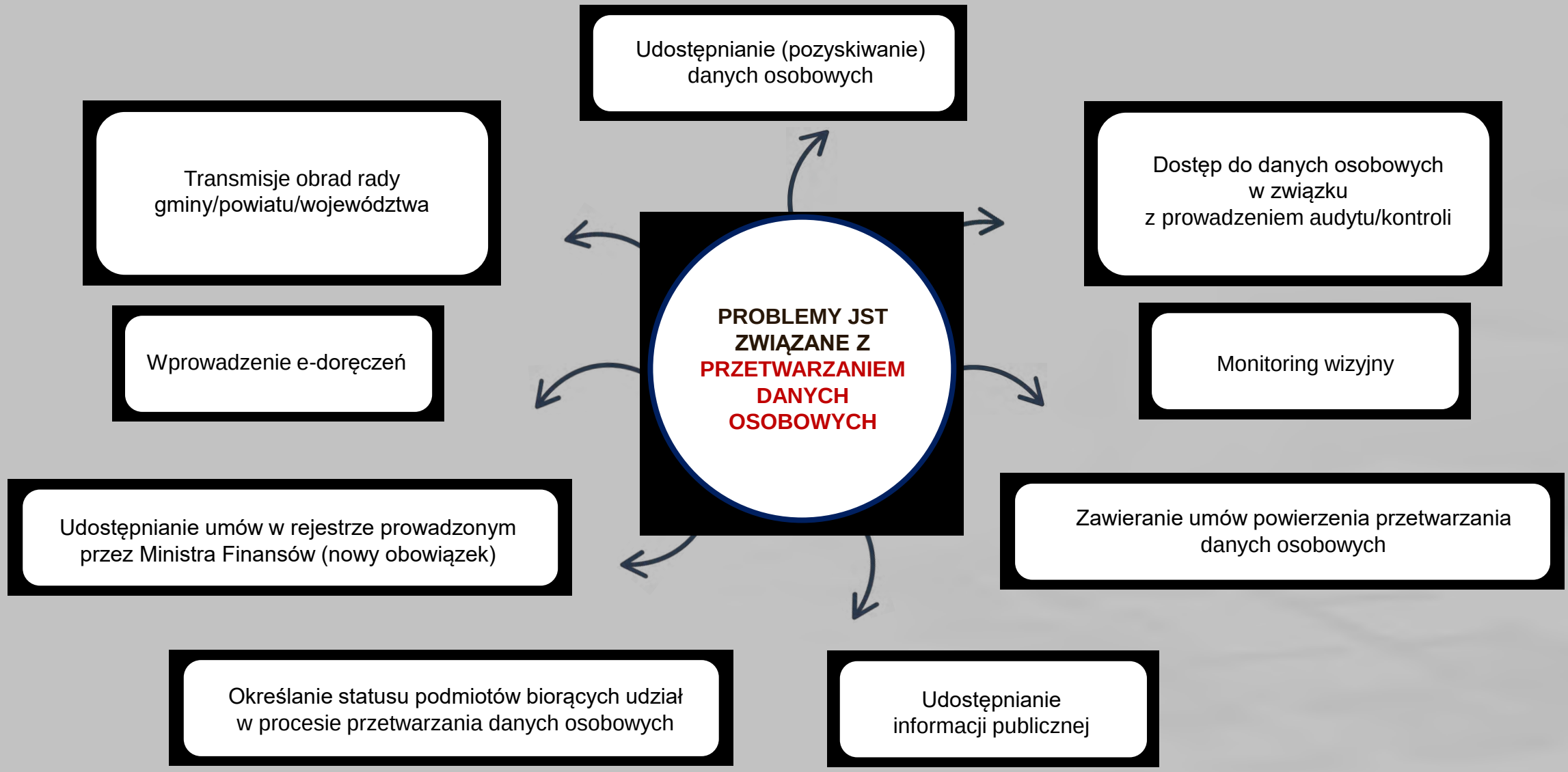
błędy w algorytmach oraz „zanieczyszczone dane mogą prowadzić do nieprawidłowych decyzji

Wyzwania w zapewnieniu anonimowości

zapewnienie anonimowości i prywatności danych jest kluczowe

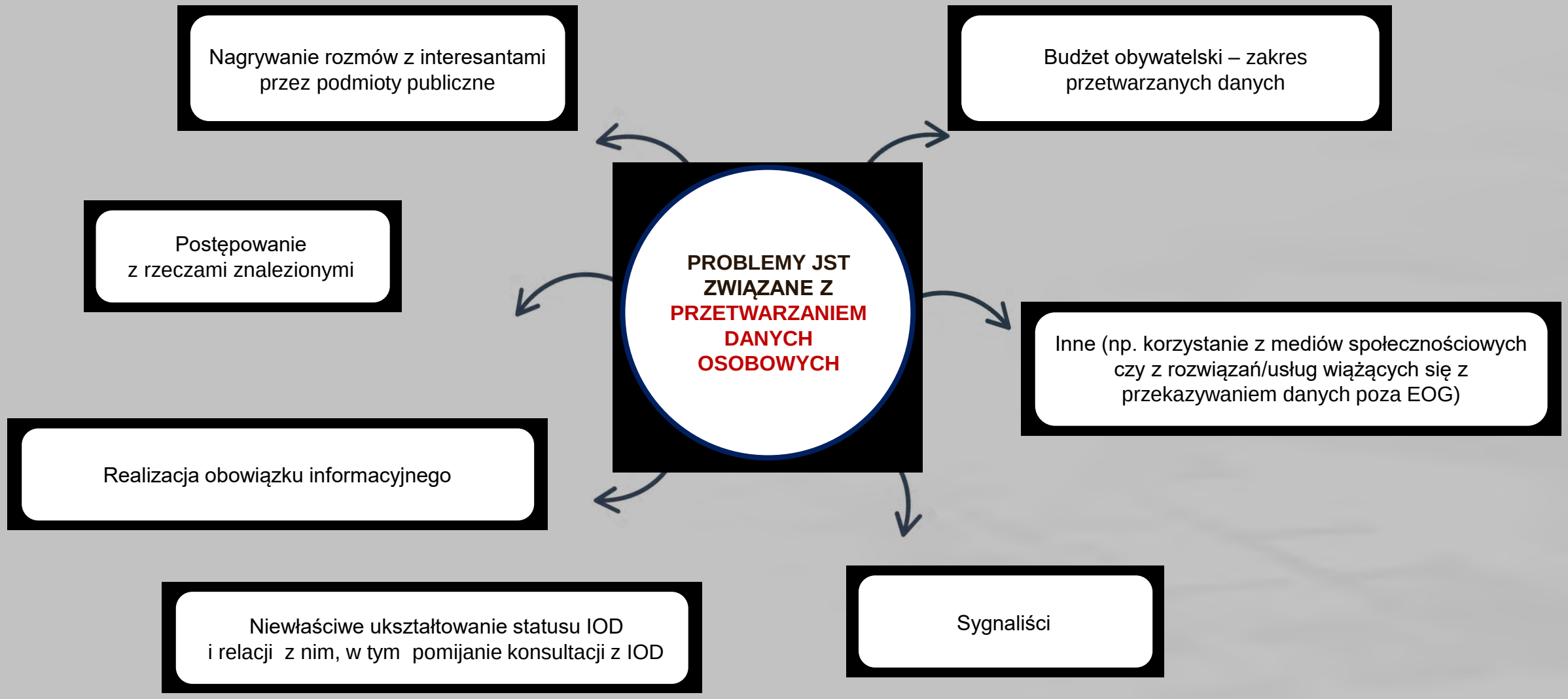
OGÓLNY WYKAZ NAJISTOTNIEJSZYCH PROBLEMÓW JEDNOSTEK SAMORZĄDU TERYTORIALNEGO ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH

URZĄD OCHRONY DANYCH OSOBOWYCH



OGÓLNY WYKAZ NAJISTOTNIEJSZYCH PROBLEMÓW JEDNOSTEK SAMORZĄDU TERYTORIALNEGO ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH

URZĄD OCHRONY DANYCH OSOBOWYCH



PRZYKŁADOWE NIEPRAWIDŁOWOŚCI STWIERDZONE W TOKU KONTROLI JST

URZĄD OCHRONY DANYCH OSOBOWYCH

- Klauzule informacyjne nie zawierają kompletnych informacji dotyczących poszczególnych administratorów, celu przetwarzania i podstawy prawnej, odbiorców danych, czy okresu przechowywania danych.
- Umowa powierzenia przetwarzania danych nie zawiera wszystkich postanowień wynikających z art. 28 ust. 3 RODO, w tym w szczególności zobowiązania podmiotu przetwarzającego do wspierania administratora w wypełnianiu jego obowiązków wynikających z RODO.
- Stanowiska obsługi interesantów nie są od siebie w żaden sposób oddzielone, tak że poszczególni klienci z łatwością mogą się zapoznać z danymi osób obsługiwanych przy innych stanowiskach.

PRZYKŁADOWE NIEPRAWIDŁOWOŚCI STWIERDZONE W TOKU KONTROLI W JST

URZĄD OCHRONY DANYCH OSOBOWYCH

- Udostępnienie dokumentacji z archiwum zakładowego. Nie zostały wdrożone wystarczające środki organizacyjne mające na celu zapewnienie odpowiedniego bezpieczeństwa udostępnianych danych, gdyż nie było możliwości ustalenia, komu, w jakim zakresie oraz w jakim czasie zostały udostępnione dane z archiwum.
- Przechowywanie dokumentów (np. związanych ze sprawami meldunkowymi) przez okres dłuższy niż wskazany w przepisach (rozporządzenia Rady Ministrów, instrukcja kancelaryjna i inne).
- Brak oceny skutków dla ochrony danych w związku z miejskim monitoringiem wizyjnym (kamery w przestrzeni miejskiej).
- Brak wskazania w dokumentacji analizy ryzyka działań naprawczych, a także brak przeprowadzenia oceny ryzyka dla wszystkich zagrożeń.

SKARGI NA JST

Od 01.01.2023 r. zostało wydanych **70 decyzji administracyjnych** w sprawach, w których stronami były organy JST (wójtowie, burmistrzowie, prezydenci miast, rady gmin lub miast) albo organy związków międzygminnych.

Decyzje te dotyczyły najczęściej skarg na:

- udostępnienie danych osobowych w BIP (np. w treści uchwał w sprawie skarg, w odpowiedzi na interpelację, w petycji, w protokole, w oświadczeniu majątkowym),
- udostępnienie danych osobowych podczas sesji rady,
- udostępnienie danych osobowych podczas transmisji na żywo z sesji rady,
- udostępnienie danych osobowych w zamieszczonym w Internecie nagraniu z sesji rady,
- udostępnienie danych osobowych osoby zawiadamiającej o nieprawidłowościach (sygnalisty) na rzecz osoby mającej dopuścić się nieprawidłowości.

NARUSZENIA OCHRONY DANYCH OSOBOWYCH W JST

URZĄD OCHRONY DANYCH OSOBOWYCH

Naruszenia ochrony danych osobowych w JST stanowią istotną część naruszeń zgłaszanych do organu nadzorczego przez szeroko rozumiane podmioty sektora publicznego.

Zidentyfikowaliśmy obszary przetwarzania danych w JST, w których ryzyko wystąpienia naruszeń ochrony danych osobowych jest wyjątkowo duże. Dlatego wymagają one prewencyjnego wdrożenia adekwatnych środków technicznych lub organizacyjnych w celu zabezpieczenia procesu przetwarzania danych osobowych.

Wśród nich można wymienić:

- Przypadkowe wysłanie korespondencji (tradycyjnej lub elektronicznej) do nieuprawnionych osób trzecich w wyniku omyłkowego działania pracowników JST.
- Udostępnienie danych nieuprawnionej osobie.
- Omyłkowe wysłanie korespondencji do innego podmiotu sektora JST.
- Nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja.
- Zagubienie korespondencji przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem jej do nadawcy.
- Nieuprawniony dostęp do baz danych.
- Zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej.
- Zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji nośnika danych.
- Wykorzystanie złośliwego oprogramowania ingerującego w poufność, integralność lub dostępność danych osobowych.

URZĄD OCHRONY DANYCH OSOBOWYCH

DZIĘKUJEMY ZA UWAGĘ!

Personal Data Protection Office
2 Stawki st., 00-193 Warsaw, POLAND
www.uodo.gov.pl/en
tel. +48 22 531 03 00