Projekt pt. „Rozwój kompetencji specjalistów ochrony zdrowia z zakresu realizacji badań naukowych”, nr FERS.01.13-IP.07-0004/24, realizowany w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus, Priorytet FERS.01 Umiejętności, Działanie FERS.01.13 Umiejętności w sektorze zdrowia.

TYTUŁ: Akty prawne i podstawy prawne dot. danych w ochronie zdrowia cz. I

Akty prawne i podstawy prawne dot. bezpieczeństwa danych cz. II

PROWADZĄCY: adw. Oskar Platta

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Dane osobowe – zagadnienia ogólne

AGENCJA BADAŃ MEDYCZNYCH

Stan prawny

- RODO - Ogólne Rozporządzenie o ochronie danych (Rozporządzenie UE 2016/679) –
- Obowiązuje bezpośrednio we wszystkich krajach UE;
- Polska ustawa o ochronie danych osobowych ma zastosowanie tylko w bardzo ograniczonym zakresie, np. co do organizacji urzędu nadzorującego ochronę danych osobowych, wyznaczenia inspektora ochrony danych czy postępowania w sprawach o naruszenia przepisów o ochronie danych.

Czym są dane osobowe?

- informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie której dane dotyczą)
- wszelkie informacje, ale wyłącznie w przypadku, gdy możliwa jest identyfikacja – odniesienie do konkretnej osoby (pewne informacje mogą być danymi osobowymi w zależności od tego, czy możliwe jest zidentyfikowanie osoby, do której te informacje się odnoszą)
- pojęcie nie obejmuje danych dotyczących osób prawnych i jednostek organizacyjnych niebędących osobami fizycznymi (np. spółek), ale…
- w aktualnym stanie prawnym ochronie podlegają dane osobowe przedsiębiorców – osób fizycznych (np. wpisane do CEIDG)

AGENCJA BADAŃ MEDYCZNYCH

Czy stosujemy RODO?

Informacja, że osoba z najdłuższym nazwiskiem na tym callu lubi oglądać komedie romantyczne	Informacja, że pracownicy firmy XYZ sp. z o.o. zarabiają średnio 40 zł za godzinę pracy
Zdjęcie, na którym można kogoś rozpoznać	Jan Paweł II był pierwszym papieżem z Polski
Numer telefonu, adres email, w służbowym telefonie	Lista kontaktów w prywatnym telefonie komórkowym

Dane osobowe – szczegóły

- odnoszą się wyłącznie do **żyjącej osoby fizycznej**
- ważny jest kontekst informacji
- RODO nie zna kategorii „danych wolnych”, czyli powszechnie dostępnych informacji o osobie fizycznej, obejmujących np.: imię, nazwisko, tytuł i stopień naukowy, datę urodzenia, zawód, określenie branży i dziedziny handlowej, w których działa, adres, numer telefonu
- informacje ze sfery publicznej i prywatnej są w równym stopniu danymi osobowymi.

Szczególna kategoria – dane sensytywne (wrażliwe) – dodatkowe wymogi

Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

- Pochodzenie rasowe lub etniczne
- Przekonania religijne
- Dane genetyczne
- Dane biometryczne
- Dane dotyczące zdrowia
- Poglądy polityczne
- Seksualność lub orientacja seksualna
- Przynależność do związków zawodowych

AGENCJA BADAŃ MEDYCZNYCH

Co to jest przetwarzanie danych osobowych?

- operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, porządkowanie, organizowanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie
- gromadzenie danych na zlecenie podmiotu trzeciego

Podmioty w procesie przetwarzania danych osobowych

- Administrator danych osobowych
- Przetwarzający dane osobowe
- Osoba, której dane dotyczą
- Personel upoważniony do przetwarzania danych
- Inspektor ochrony danych

Podmioty w procesie przetwarzania danych na przykładzie badania klinicznego

Administrator	Podmiot przetwarzający	Personel upoważniony do zbierania danych	Osoby, których dane dotyczą
Spółka X – Sponsor badania klinicznego	**Ośrodek badawczy** – podmiot, który faktycznie będzie prowadził badanie kliniczne	**Badacze –** pracownicy Ośrodka, którzy będą faktycznie przetwarzać dane osobowe	**Pacjenci, uczestnicy badania klinicznego**

Kiedy można przetwarzać dane osobowe?

- Podstawa prawna przetwarzania danych osobowych
- Zgodne z wyznaczonym celem (nie naruszającym prawa)
- Dane adekwatne do celu przetwarzania
- Spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą
- Wdrożenie odpowiednich środków technicznych i organizacyjnych dotyczących przetwarzania danych

Podstawa prawna przetwarzania danych osobowych

- Administrator danych **musi mieć podstawę prawną**, aby przetwarzać dane osobowe.

- Zgoda
- Realizacja umowy
- Ochrona żywotnych interesów
- Prawnie uzasadniony interes
- Interes publiczny
- Obowiązek prawny

Prawnie uzasadniony interes

Przetwarzanie danych na podstawie prawnie uzasadnionego interesu, jest dopuszczalne, ale wymaga **łącznego** zaistnienia następujących okoliczności:

1) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,
2) nie zachodzą sytuacje, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych

Zgoda na przetwarzanie danych osobowych

- zgoda dotyczy określonych danych osobowych i określonego celu przetwarzania
- musi być wyraźna, a zapytanie o udzielenie zgody jednoznacznie sformułowane, zrozumiałe
- zgoda – tylko dobrowolna; od jej udzielenia nie można np. uzależniać wykonania umowy (jeśli te dane osobowe nie są konieczne dla wykonania umowy)
- forma – dowolna, ale obowiązek administratora wykazania, że została udzielona
- może być w dowolnym momencie odwołana!

Klauzule informacyjne

- Obowiązek przekazania informacji o przetwarzaniu danych dla osoby, której dane dotyczą (podczas pozyskiwania danych) – klauzule informacyjne
- Informacje dotyczące m.in.:
  - Danych administratora
  - Celu i podstawy przetwarzania
  - Przysługujących praw
  - Odbiorców danych
  - Czasu przetwarzania

Możliwość „rozdzielania” informacji

- Informacja o przetwarzaniu danych może być rozdzielana – np. aby zachować większa przejrzystość lub gdy jest ograniczona ilość miejsca (np. strona internetowa)

- **Pierwszy poziom informacji**: Kto jest administratorem, w jakim celu przetwarzana dane osobowe oraz informacja o przysługujących prawach i gdzie je znaleźć (link do dalszej części informacji).

- **Drugi poziom informacji:** Podstawa przetwarzania, czas, prawa osoby, której dane dotyczą, odbiorcy danych, dobrowolność/obowiązek podania danych, profilowanie – jeżeli dotyczy.

Przekazywanie danych poza UE

- Dopuszczalne tylko w przypadkach przewidzianych prawem – m.in.:
  - Decyzja Komisji Europejskiej co do zapewniania przez państwo trzecie odpowiedniego poziomu ochrony
  - Zastosowanie standardowych klauzul umownych
  - Zgoda osoby, której dotyczą dane

Powierzenie przetwarzania danych – współpraca z innymi podmiotami

- Przetwarzanie „w imieniu administratora”, tj. podmiot przetwarzający nie decyduje o celach przetwarzania, a jedynie dokonuje czynności przetwarzania ściśle określonych przez administratora
- Przykłady – dostawcy usług (np. usługi hostingowe)
- Konieczność zweryfikowania dostawcy oraz podpisania umowy powierzenia przetwarzania.

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Wewnętrzne dokumenty i procedury ochrony danych osobowych

AGENCJA BADAŃ MEDYCZNYCH

Agencja Badań Medycznych, ul. Chmielna 69, 00-801 Warszawa, e-mail: kancelaria@abm.gov.pl, tel. + 48 22 270 70 69, NIP: 5252783949 REGON: 382836515

Polityka ochrony danych – zagadnienia ogólne

- Wdrożenie odpowiednich środków technicznych i organizacyjnych dla ochrony danych osobowych – art. 24 ust. 2 RODO;
- Przewodnik po zagadnieniach i sposobach postępowania w sytuacjach związanych z danymi osobowymi;
- Powinna odnosić się do innych procedur związanych z danymi osobowymi w firmie;
- Wskazuje osoby odpowiedzialne za dane osobowe w firmie.

Rejestr czynności przetwarzania

- Rejestr czynności przetwarzania jest zbiorem wszystkich procesów związanych z przetwarzaniem danych osobowych prowadzonych w firmie;
- **Kto musi prowadzić rejestr** – art. 30 ust. 1 RODO - Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają
- Jakie dane zawiera rejestr:
    - określenie tożsamości administratora/podmiotu przetwarzającego oraz jego danych kontaktowych,
    - cele przetwarzania,
    - opis kategorii osób, których dane dotyczą oraz kategorii przetwarzanych danych,
    - określenie państw spoza UE, do których przekazywane są dane oraz dokumentacja zabezpieczeń,
    - terminy usunięcia poszczególnych kategorii danych,
    - ogólny opis stosowanych środków bezpieczeństwa.

AGENCJA BADAŃ MEDYCZNYCH

Nazwa Procesu	Rodzaj podmiotu danych	Cel przetwarzania	Kategorie przetwarzania danych	Kategorie odbiorców danych	Przesyłanie danych do podmiotów w państwach trzecich poza EOG	Czas retencji danych dla każdego rodzaju danych	Ogólny opis podstawowych środków organizacyjnych i technicznych zapewniających bezpieczeństwo	Współadministratorzy	Podstawa prawna przetwarzania	Osoba odpowiedzialna za nadzór nad zbiorem
Rekrutacja Pracowników	Kandydaci do pracy	Przetwarzanie danych osobowych w celach rekrutacji pracowników	Dane dot. wykształcenia, dane kontaktowe, dane dot. doświadczenia zawodowego, wizerunek	Podmioty świadczące usługi na rzecz [xxx]., przetwarzające dane wyłącznie na polecenie i zgodnie z instrukcjami Administratora., Upoważnione organy władzy publicznej – gdy obowiązek taki wynika z przepisów prawa. W szczególności:	NIE	Dane przechowywać zgodnie z harmonogramem retencji. W przypadku wszczęcia sporu sądowego lub istnienia podwyższonego ryzyka wystąpienia roszczeń - nie usuwać przed uzyskaniem zgody działu prawnego.	Dane przechowywane w zabezpieczonym hasłem komputerze,	BRAK	Zgoda wyrażona w CV przesłanym przez kandydata	
Windykacja należności	Dłużnicy Spółki	Windykacja należności	Dane kontaktowe, kwota zaległości	Podmioty świadczące usługi na rzecz [xxx], przetwarzające dane wyłącznie na polecenie i zgodnie z instrukcjami Administratora, Upoważnione organy władzy publicznej – gdy obowiązek taki wynika z przepisów prawa	NIE	Do momentu spełnienia bądź przedawnienia wszelkich roszczeń	Dane przechowywane w zabezpieczonej na klucz szafie, elektroniczne kopie dokumentacji w zabezpieczonym hasłem komputerze	BRAK	Prawnie uzasadniony interes Spółki jakim jest ochrona interesów Spółki poprzez windykację należności	

Procesy	Czas przechowania
REKRUTACJA PRACOWNIKÓW	
Aplikacje osób zatrudnionych (CV, listy motywacyjne i inne dane pozyskane podczas rekrutacji)	Pracownik zatrudniony przed 1 stycznia 2019 r.: 51 lat od zakończenia stosunku pracy, Pracownik zatrudniony po 1 stycznia 2019 r.: 11 lat od zakończenia stosunku pracy.
Aplikacje osób odrzuconych (CV, listy motywacyjne i inne dane pozyskane podczas rekrutacji)	Jeżeli nie wyraziły zgody na dalsze rekrutacje: 3 lata od zakończenia rekrutacji (dowód przy zarzucie dot. dyskryminacji); jeżeli kandydat wyraził zgodę na dalsze przetwarzanie danych przy następnych rekrutacjach - tak długo jak CV będzie wykorzystywane w procesach rekrutacyjnych.
PROWADZENIE AKT OSOBOWYCH	
Dokumentacja pracownicza: umowy o pracę, listy płac, karty wynagrodzeń, ewidencja czasu pracy, raporty szkód lub inne dokumenty związane z ponoszeniem odpowiedzialności porządkowej przez pracownika , akta medyczne, akta dotyczące niepełnosprawności, opis stanowiska, szkolenia BHP, umowy zakupu akcji pracowniczych, rejestry pracy, akta degradacji, listy obecności, umowy zbiorowe, instrukcje dla pracowników, plany motywacyjne, program równych szans w zatrudnieniu, plan pozytywnych działań etc.)	Pracownik zatrudniony przed 1 stycznia 2019 r.: 51 lat od zakończenia stosunku pracy, Pracownik zatrudniony po 1 stycznia 2019 r.: 11 lat od zakończenia stosunku pracy.
Dokumentacja związana z wypadkiem w pracy lub w drodze do pracy, w tym: raporty z obrażeń, rejestr wypadków i obrażeń, raport powypadkowy, etc.	10 lat od sporządzenia dokumentacji (art. 234 § 3 k.p.)
Akta dotyczące ekspozycji na promieniowanie, akta dotyczące bezpieczeństwa, akta dotyczące ekspozycji na substancje	40 lat od daty ostatniego wpisu (§18 ust. 4 rozporządzenia MZ ws. badań i pomiarów czynników szkodliwych [...])
WSPÓŁPRACA NA PODSTAWIE UMOWY CYWILNOPRAWNEJ	
Umowy dot. współpracy zleceniobiorców/usługodawców ze Spółką	10 lat od zakończenia współpracy
Dokumentacja związana z wykonywaniem zlecenia z wyłączeniem dokumentacji podatkowej (rejestry przepracowanych godzin, dokumenty związane z ponoszeniem odpowiedzialności przez zleceniobiorcę, wszelkie dokumenty określające relacje między zleceniobiorca i Spółką nieokreślone w Umowie).	10 lat od zakończenia współpracy

Naruszenie ochrony danych osobowych

- Naruszenie ochrony danych oznacza 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:

Przykłady:

- zgubienie/kradzież laptopa zawierającego dane osobowe, który nie był zabezpieczony hasłem;
- omyłkowe wysłanie maila do niewłaściwego adresata z danymi osobowymi;
- zgubienie teczki z dokumentacją zawierającą dane osobowe.

Najczęstsze naruszenia ochrony danych osobowych

- Wysyłka na nieprawidłowy adres e-mail, lub brak weryfikacji rzeczywistego odbiorcy.
- Hasła dostępu na „żółtych karteczkach” (źle konstruowane hasła, brak wymuszania zmiany hasła)
- Brak odpowiedniego zarządzania uprawnieniami (dostępy użytkowników do zasobów informacyjnych firmy, które nie powinny być dla nich dostępne z uwagi na zakres obowiązków).
- Wynoszenie z firmy niezaszyfrowanych nośników z informacjami.
- Udostępnianie haseł dostępowych osobom nieupoważnionym.
- Niewłaściwe ustawienie monitora komputera.
- Wybieranie złej drukarki, pozostawianie na wierzchu wydruków.
- Telefoniczne udostępnienie danych osobom niezidentyfikowanym, brak procedury weryfikacji.
- Zagubienie firmowego sprzętu (laptopy).
- Zgubienie telefonu ze skonfigurowanym służbowym mailem.
- Zawirusowanie komputera.

Art. 33 ust.1 RODO

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

W przypadku naruszenia ochrony danych osobowych, ***administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*** *- zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55,* ***chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych****. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.*

- **Obowiązek zgłoszenia**. W przypadku stwierdzenia naruszenia ochrony danych osobowych, administrator zgłasza je właściwemu organowi nadzorczemu
- Według Grupy Roboczej Art. 29 **administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu**, które doprowadziło do naruszenia ochrony danych.
- **Wyjątek od obowiązku notyfikacji**. Jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Zawiadamianie osoby, której dane dotyczą – obowiązek z RODO

Art. 34 ust. 1 RODO

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Administrator zawiadamia osobę, **JASNYM I PROSTYM JĘZYKIEM** opisuje charakter naruszenia ochrony danych osobowych.

Czy jeżeli naruszenie ochrony danych osobowych dotyczy tylko jednej osoby –to należy uznać, że takie naruszenie może powodować wysokie ryzyko naruszenia?

- TAK, może – należy badać cały kontekst.

Wnioski/żądania osób, których dane dotyczą

- Każda osoba, której dane dotyczą ma złożyć żądanie/wniosek w zw. z:
  - prawem dostępu do informacji, w tym prawa do kopii danych (art. 15 RODO);
  - prawem do sprostowania danych (art. 16 RODO);
  - prawem do usunięcia danych osobowych (art. 17 RODO);
  - prawem do ograniczenia przetwarzania (art. 18 RODO);
  - prawem do przenoszenia danych (art. 20 RODO);
  - prawem do sprzeciwu (art. 21 RODO);
  - prawem do niepodlegania profilowaniu (art. 22 RODO).

Podstawa przetwarzania danych osobowych wyznacza zakres przysługujących nam praw!

Wnioski/żądania osób, których dane dotyczą

- Każda osoba, której dane dotyczą ma złożyć żądanie/wniosek w zw. z:
  - prawem dostępu do informacji, w tym prawa do kopii danych (art. 15 RODO);
  - prawem do sprostowania danych (art. 16 RODO);
  - prawem do usunięcia danych osobowych (art. 17 RODO);
  - prawem do ograniczenia przetwarzania (art. 18 RODO);
  - prawem do przenoszenia danych (art. 20 RODO);
  - prawem do sprzeciwu (art. 21 RODO);
  - prawem do niepodlegania profilowaniu (art. 22 RODO).

Podstawa przetwarzania danych osobowych wyznacza zakres przysługujących nam praw!

Jak rozpatrzyć wniosek?

- Wniosek należy rozpatrzeć w terminie 30 dni od dnia wpłynięcia wniosku – jeżeli z jakichś powodów nie można odpowiedzieć w terminie 30 dni należy skontaktować się z działem prawnym lub kancelarią prawniczą.
- Na każdy wniosek należy odpowiedzieć, nawet na te niezasadne.
- Procedura odpowiadania na wniosek wygląda następująco:
    1. Informujemy odpowiednią osobę o przyjściu żądania/wniosku;
    2. Weryfikujemy tożsamość osoby (np. kontakt na inny zapisany e-mail, nr telefonu);
    3. Wysyłamy e-mail do osoby, której dane dotyczą z prośbą o wypełnienie formularza (nie jest to obowiązkowe);
    4. Po otrzymaniu formularza lub dalszych wyjaśnień osoba odpowiedzialna ocenia czy żądanie/wniosek jest uzasadnione;
    5. Udzielenie odpowiedzi na żądanie zgodnie z prośbą osoby lub informacja o przyczynach odmowy;
    6. Żądanie należy ewidencjonować w rejestrze wniosków, osób których dane dotyczą;

Dzień dobry.

Dostałam na skrzynkę mailową wiadomość SPAM - wysłaną przez firmę [redacted] na zlecenie [redacted] W związku z tym poproszę o informację do których mam prawo na podstawie przepisów GDPR:

1. w jaki sposób Państwo weszliście w posiadacie moich danych
2. Jakie dokładnie dane mnie dotyczące posiadacie
3. Dlaczego wysyłacie mi treści marketingowe bez uprzedniego uzyskania ode mnie zgody na marketing bezpośredni

Wg przepisów GDPR mam prawo do wglądu i usunięcia moich danych. Proszę zatem o kopię moich danych będących w Państwa posiadaniu, lub w posiadaniu innych podmiotów na Państwa zlecenie.

W przypadku braku odpowiedzi na powyższe zgłoszenie w ciągu 7 dni, sprawa zostanie zgłoszona do UOKiK i GIODO, z podejrzeniem kradzieży oraz nieuprawnionego przetwarzania danych osobowych przez [redacted]

Pozdrawiam
[redacted]

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Dane osobowe w ochronie zdrowia - badania kliniczne

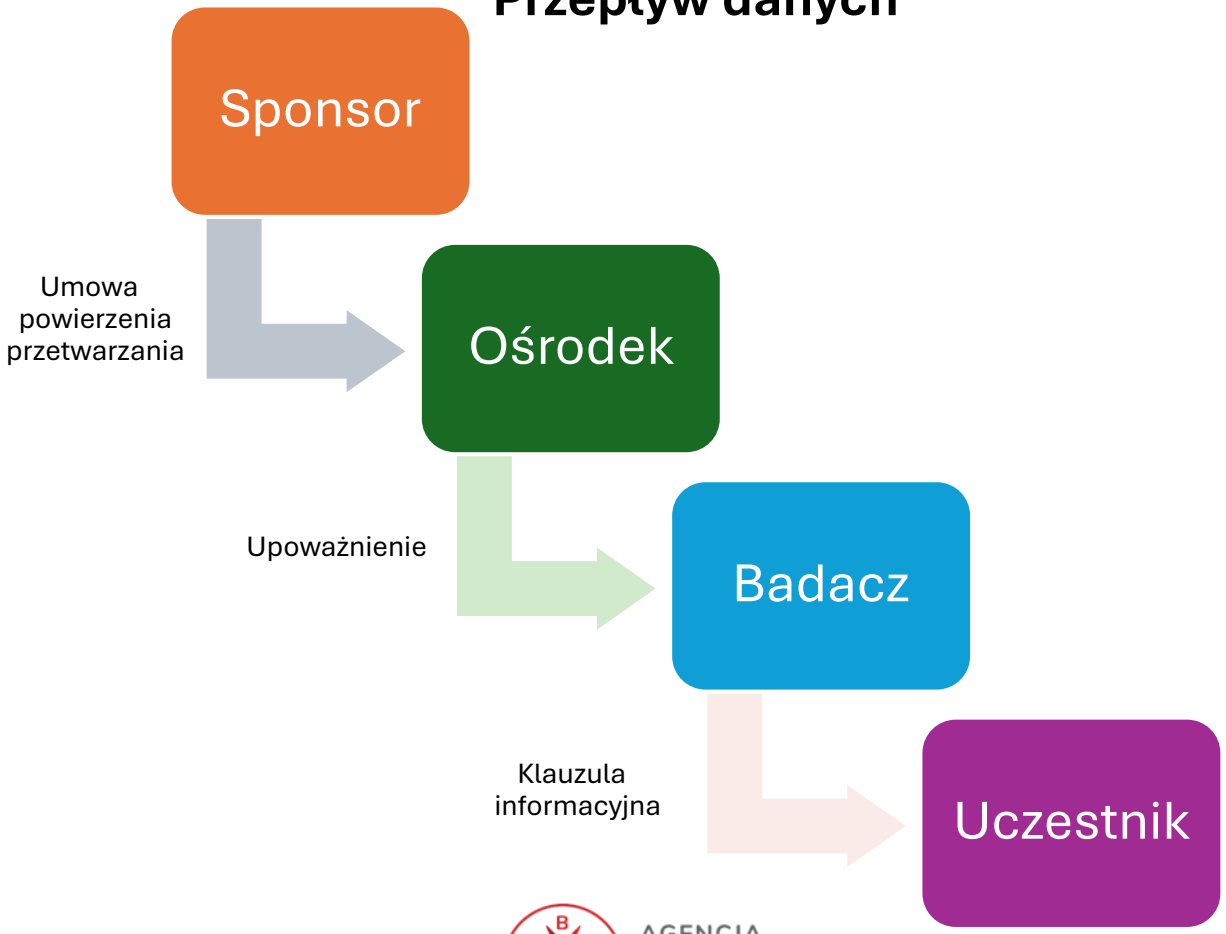
AGENCJA BADAŃ MEDYCZNYCH

Agencja Badań Medycznych, ul. Chmielna 69, 00-801 Warszawa, e-mail: kancelaria@abm.gov.pl, tel. + 48 22 270 70 69, NIP: 5252783949 REGON: 382836515

Identyfikacja ról przetwarzania danych w badaniu klinicznym

Administrator	Podmiot przetwarzający	Personel upoważniony do zbierania danych	Osoby, których dane dotyczą
Spółka X – Sponsor badania klinicznego	**Ośrodek badawczy** – podmiot, który faktycznie będzie prowadził badanie kliniczne	**Badacze –** pracownicy Ośrodka, którzy będą faktycznie przetwarzać dane osobowe	**Pacjenci, uczestnicy badania klinicznego**

Przepływ danych



AGENCJA BADAŃ MEDYCZNYCH

Umowa przetwarzania z Ośrodkiem badawczym

Kluczowe aspekty do ustalenia w umowie z ośrodkiem badawczym:

- Zabezpieczenie danych;
- Odpowiedzialność;
- Przekazywanie informacji o przetwarzaniu danych pacjentom;
- Pseudonimizacja lub anonimizacja danych

Upoważnienie dla Badacza

Bardzo prosty dokument wskazujący najczęściej:

- Zakres upoważnienia (do jakich danych, zbiorów ma dostęp);
- Oświadczenie, że pracownik/współpracownik zna zasady przetwarzania danych

Informacja (zgoda?) dla Uczestnika

Wytyczne EROD dot. podstawy prawnej:

- odstąpienie od zgody jako podstawy;
- Właściwsze podstawy to:

  W zakresie bezpieczeństwa i wiarygodności:

  - Art. 6 ust. 1 lit. c RODO - obowiązek prawny w zakresie np. bezpieczeństwa
  - Art. 9 ust. 2 lit. i RODO - przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego;

  W zakresie badawczym:

  - Art. 6 ust. 1 lit. e RODO – tj. interes publiczny;
  - Art. 6 ust. 1 lit. f RODO – tj. prawnie uzasadniony interes
  - Art. 9 ust. 2 lit i lub j RODO (interes publiczny)

Wtórne wykorzystanie danych osobowych

Czy wtórne wykorzystanie danych zebranych podczas badania jest możliwe?

<u>Tak, ale:</u>

- Anonimizacja to też jest przetwarzanie danych;
- Konieczne jest wyodrębnienie tej kwestii w informacji o przetwarzaniu danych osobowych;
- Anonimizacja vs. Pseudonimizacja
- EHDS!

Polski problem z dokumentacją medyczną

- Brak podstawy prawnej do przekazania dokumentacji medycznej firmie (sponsorowi).
- Czym jest dokumentacja medyczna?
- Jak otrzymać dostęp do dokumentacji medycznej i czy jest to konieczne?

Konieczność przeprowadzenia DPIA

- Data Protection Impact Assessment („DPIA”);
- Dokonywana przed rozpoczęciem przetwarzania, gdy ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
- kiedy obowiązkowa? np.:
    - przetwarzanie na dużą skalę danych sensytywnych,
    - systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie,
    - dany rodzaj operacji został objęty wykazem obowiązkowego DPIA.

Inne problemy z danymi osobowymi w ochronie zdrowia

- Badania obserwacyjne na nakietach oddziałowych – czy lekarz może publikować artykuły na „własnych” lub „szpitalnych” pacjentach?
- Biobanki tkanek – jak działają w zw. z danymi osobowymi?

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

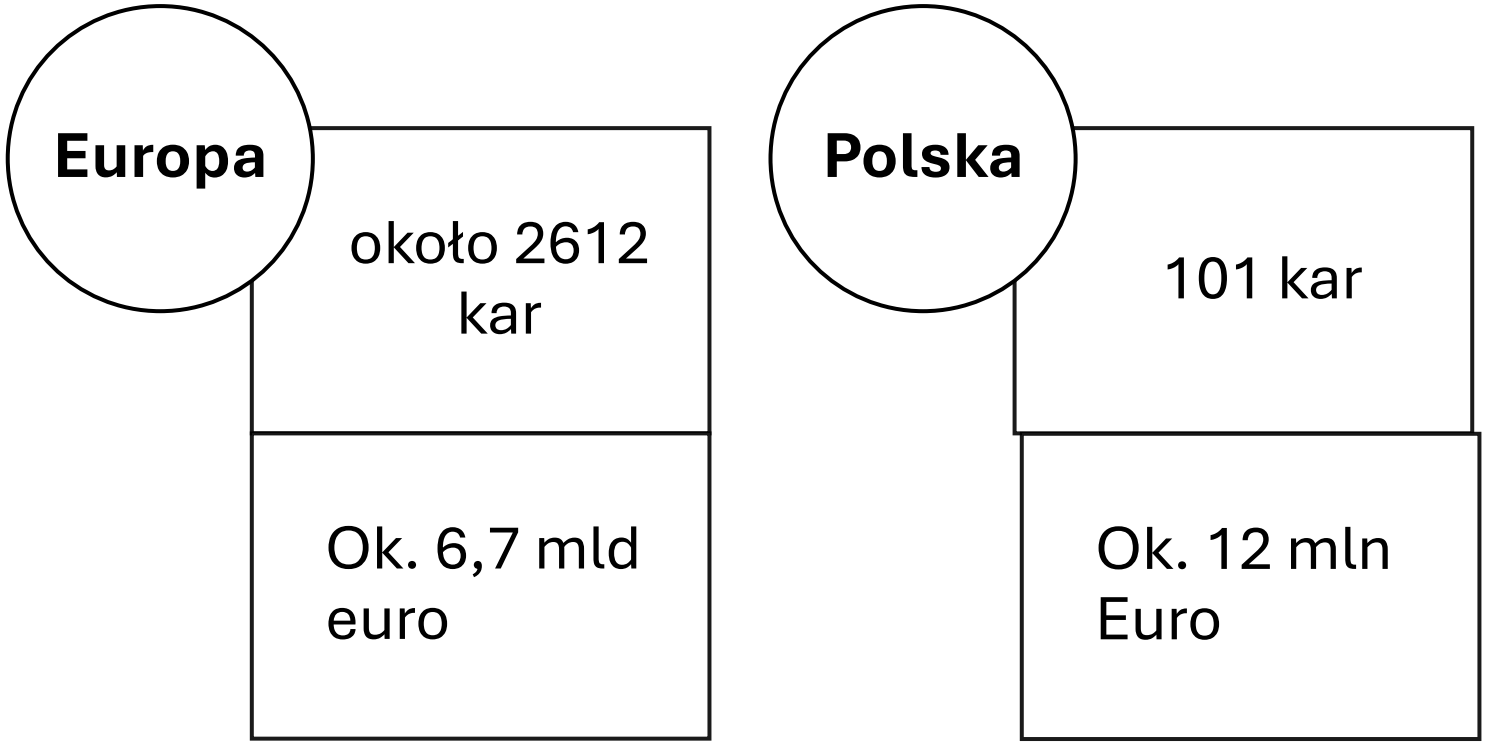
Prezes Urzędu Ochrony Danych Osobowych i kary

AGENCJA BADAŃ MEDYCZNYCH

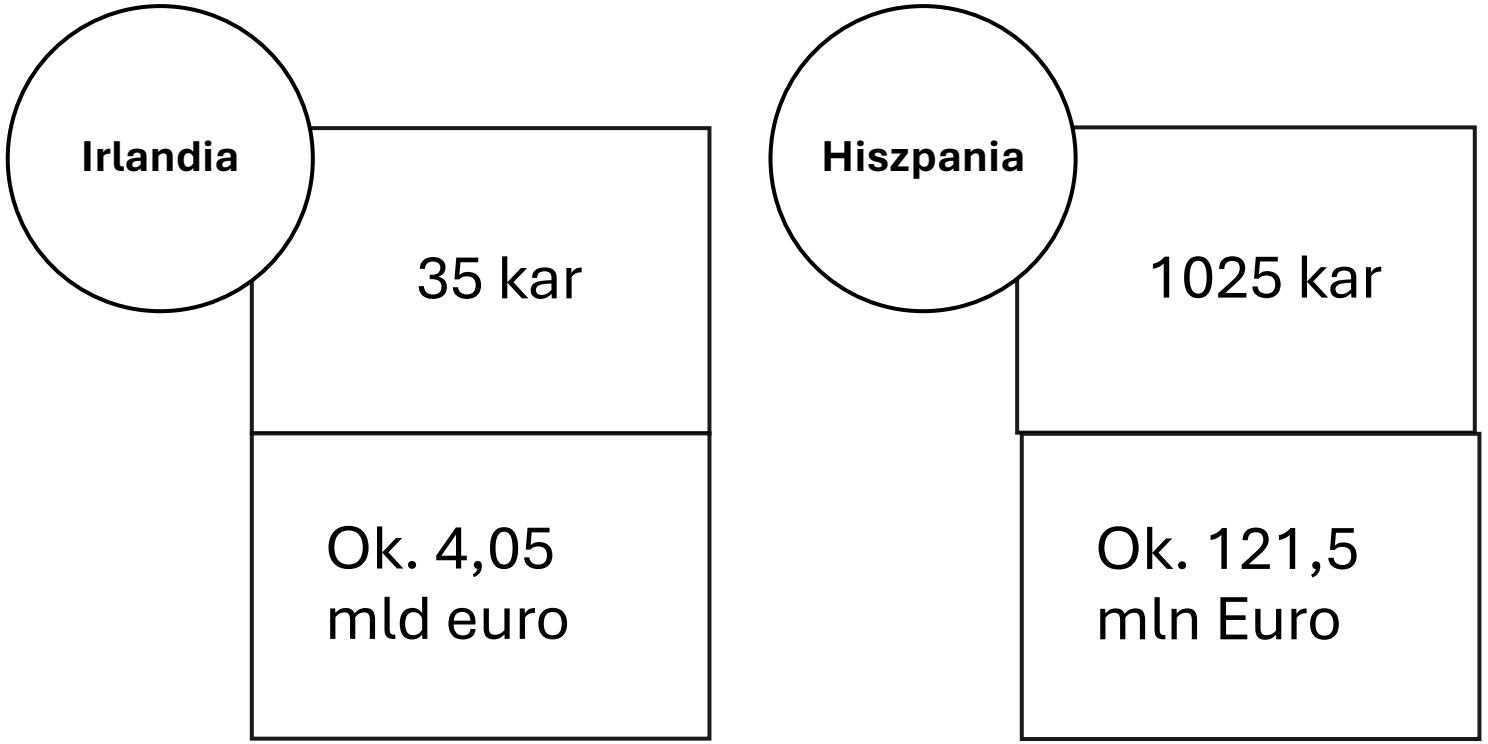
Kary za „nieprzestrzeganie RODO”

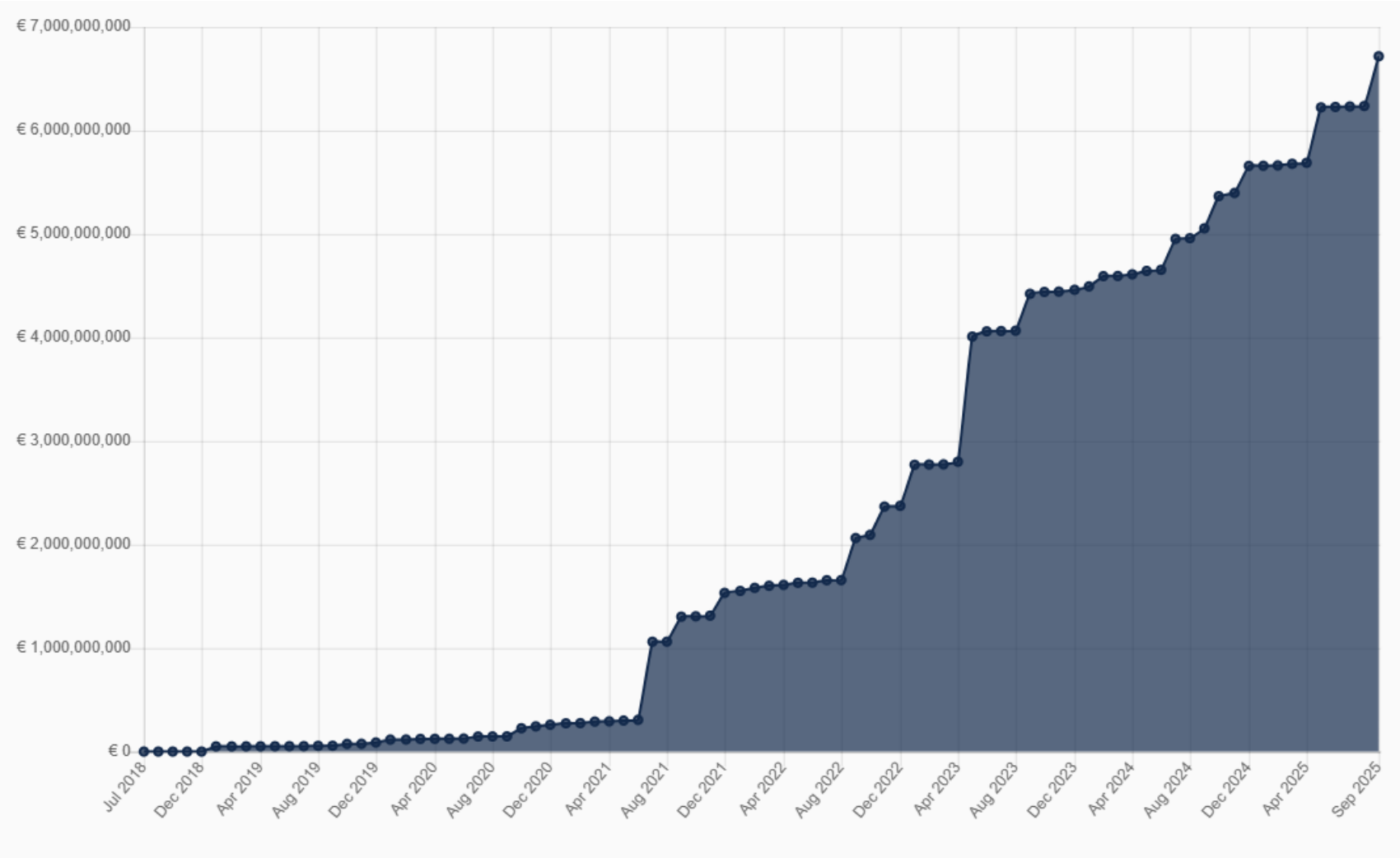
- Bardzo wysokie kary administracyjne były jednym z powodów „zamieszania” przy wejściu w życie RODO
- Zgodnie z art. 83 RODO, organ nadzorczy za naruszenie rozporządzenia może nałożyć karę – do 20.000.000 Euro lub 4% całkowitego rocznego światowego obrotu
- Kary m.in. za naruszenie praw osób, których dane dotyczą, naruszenie obowiązków administratora czy podmiotu przetwarzającego, ale też niewykonanie nakazu organu nadzorczego

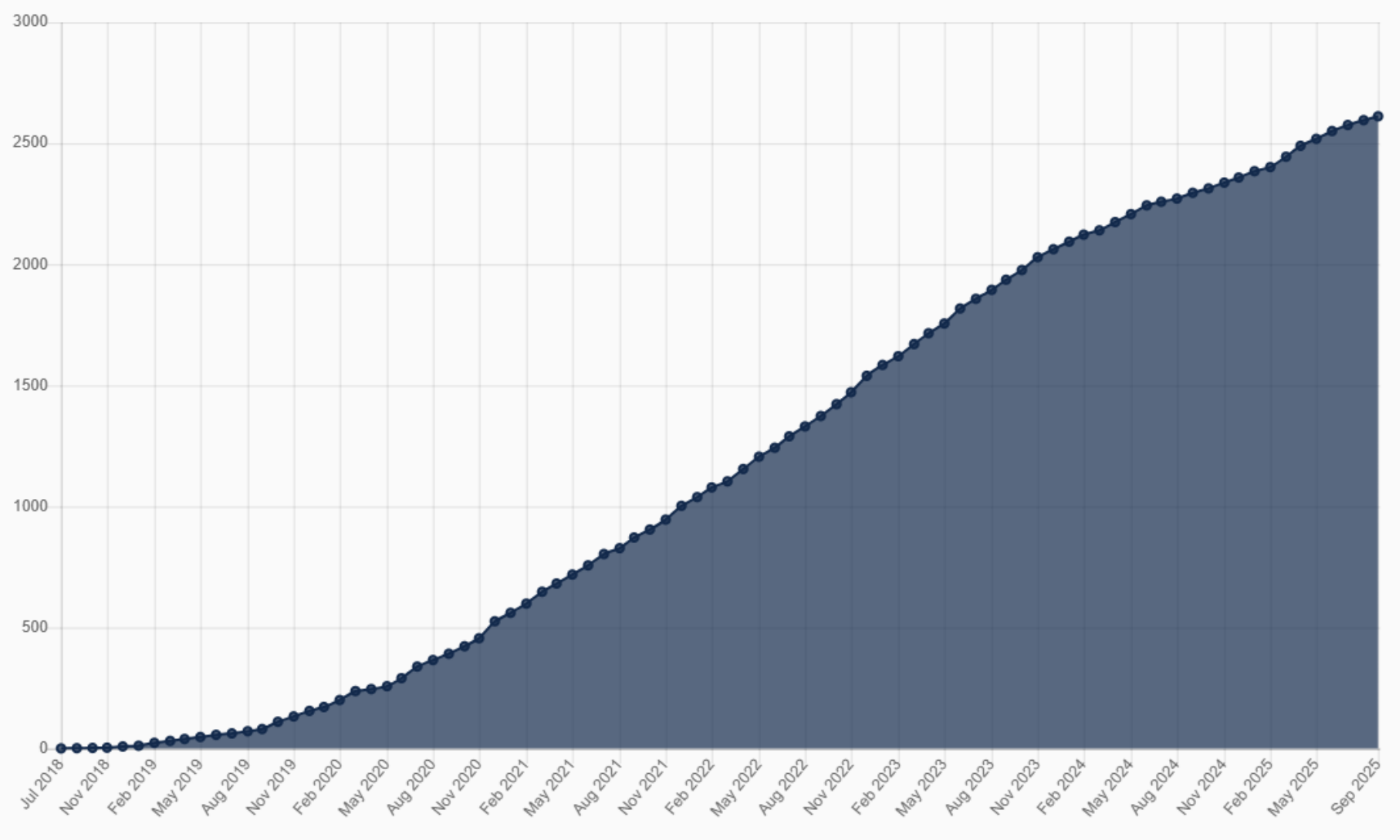
Kary Statystyki



Kary Statystyki




€ 7,000,000,000
€ 6,000,000,000
€ 5,000,000,000
€ 4,000,000,000
€ 3,000,000,000
€ 2,000,000,000
€ 1,000,000,000
€ 0
Jul 2018
Dec 2018
Apr 2019
Aug 2019
Dec 2019
Apr 2020
Aug 2020
Dec 2020
Apr 2021
Aug 2021
Dec 2021
Apr 2022
Aug 2022
Dec 2022
Apr 2023
Aug 2023
Dec 2023
Apr 2024
Aug 2024
Dec 2024
Apr 2025
Sep 2025


3000
2500
2000
1500
1000
500
0
Jul 2018
Nov 2018
Feb 2019
May 2019
Aug 2019
Nov 2019
Feb 2020
May 2020
Aug 2020
Nov 2020
Feb 2021
May 2021
Aug 2021
Nov 2021
Feb 2022
May 2022
Aug 2022
Nov 2022
Feb 2023
May 2023
Aug 2023
Nov 2023
Feb 2024
May 2024
Aug 2024
Nov 2024
Feb 2025
May 2025
Sep 2025

Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
POLAND	2025-03-17	6,300,000	Poczta Polska SA (Polish Post)	Art. 6 (1) GDPR	Insufficient legal basis for data processing	link link
POLAND	2025-08-26	4,323,250	ING Bank Śląski	Art. 5 (1) a), b), c) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing	link
POLAND	2025-07-21	3,955,000	McDonald's Polska Sp. z o.o.	Art. 5 (1) c) GDPR, Art. 25 (1) GDPR, Art. 28 (1) GDPR, Art. 38 (1) GDPR	Non-compliance with general data processing principles	link link
POLAND	2022-01-19	1,000,000	Fortum Marketing and Sales Polska S.A.	Art. 5 (1) f) GDPR, Art. 24 (1) GDPR, Art. 25 (1) GDPR, Art. 28 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link link
POLAND	2024-08-20	940,000	mBank	Art. 34 (1), (2) GDPR	Insufficient fulfilment of data breach notification obligations	link link
POLAND	2019-09-10	660,000	Morele.net	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
POLAND	2020-12-14	443,000	Virgin Mobile Polska	Art. 5 (1) f), (2) GDPR, Art. 25 (1) GDPR, Art. 32 (1) b), d), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
POLAND	2024-11-20	358,000	Unknown	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 25 (1) GDPR, Art. 28 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
POLAND	2024-12-23	357,000	Panek SA	Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link link link
POLAND	2024-05-20	336,000	Company	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link

Fundusze Europejskie dla Rozwoju Społecznego

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Serdecznie dziękuję za uwagę!

Adw. Oskar Platta

FAIRFIELD

oskar.platta@fairfield.pl

0048 22 616 41 41

AGENCJA BADAŃ MEDYCZNYCH