

*„NOWE EUROPEJSKIE REGULACJE W ZAKRESIE  
PRYWATNOŚCI W FAZIE PROJEKTOWANIA I PRYWATNOŚCI W  
DOMYŚLNYCH USTAWIENIACH”*

*Konferencja  
„NOWE RAMY OCHRONY DANYCH OSOBOWYCH  
W UNII EUROPEJSKIEJ. WYZWANIA DLA POLSKI”*

Dr WOJCIECH WIEWIÓROWSKI  
Generalny Inspektor Ochrony Danych Osobowych / WPiA Uniwersytet  
Gdański

## Nota

Niniejsza prezentacja stanowi uzupełnienie wystąpienia  
podczas konferencji

**„Nowe ramy ochrony danych osobowych w Unii Europejskiej.  
Wyzwania dla Polski”**

zorganizowanej w Krajowej Szkole Administracji Publicznej w Warszawie  
7 marca 2012 r.

Prezentację można kopiować i wykorzystywać w całości lub w części tylko pod  
warunkiem podania pełnej informacji o utworze  
w poniższym brzmieniu:

*W.R. Wiewiórowski, „Nowe europejskie regulacje w zakresie prywatności  
w fazie projektowania i prywatności w domyślnych ustawieniach”,  
GIODO / WPiA Uniwersytet Gdański 2012 (wersja z 1 marca 2012 r.)*

© W.R. Wiewiórowski

THE OLD MODEL STILL WORKS, BUT...



## POJĘCIE PRIVACY BY DESIGN

Nie zaproponowano jak dotąd powszechnie akceptowanego tłumaczenia tego pojęcia na język polski stąd też używane jest ono zamiennie z pojęciem „**ochrona prywatności w fazie projektowania**”, gdyż takie tłumaczenie przyjęto w niektórych oficjalnych tłumaczeniach przygotowanych na potrzeby procesu legislacyjnego w Unii Europejskiej

## NOWY PARADYGMAT OCHRONY DANYCH

Paradygmat – (wg. Thomasa Kuhna)

Zbiór pojęć i teorii tworzących podstawy danej nauki.

Paradygmat jest zestawem teorii i pojęć tworzących jest przyjęty jako konsensus przynajmniej do czasu, kiedy paradygmat jest twórczy poznawczo - tzn. za jego pomocą można tworzyć teorie szczegółowe zgodne z danymi doświadczalnymi, którymi zajmuje się dana nauka.

Paradygmat od tzw. dogmatu odróżnia kilka zasadniczych cech:

- nie jest on dany raz na zawsze - lecz jest przyjęty na zasadzie konsensusu większości badaczy,
- może okresowo ulec zasadniczym przemianom prowadzącym do głębokich zmian w nauce zwanych rewolucją naukową,
- podważa sens absolutnej słuszności.

## NOWY PARADYGMAT OCHRONY DANYCH

Dobry paradygmat posiada kilka cech i m.in. musi:

- być spójny logicznie i pojęciowo,
- być jak najprostszy i zawierać tylko te pojęcia i teorie, które są dla danej nauki rzeczywiście niezbędne,
- dawać możliwość tworzenia teorii szczegółowych zgodnych ze znanymi faktami.

## ŹRÓDŁA KONCEPCJI PRIVACY BY DESIGN

Pojęcie „*privacy by design*” zostało do dyskursu o ochronie prywatności wprowadzone przez *Ann Cavoukian* – rzecznika ds. informacji i prywatności kanadyjskiej prowincji Ontario – jako wynik wieloletnich prac nad wprzęgnięciem zasad ochrony prywatności do nowych projektów infrastrukturalnych realizowanych w Kanadzie.

*Privacy by design* ma stanowić kompleksową odpowiedź na narastające, systemowe efekty zastosowania ICT i rozbudowanej infrastruktury teleinformatycznej. Określenie to zakłada tak filozoficzne, jak i praktyczne podejście do prywatności jako pewnej wartości, której ochrona powinna być częścią rozważań i praktycznych działań podejmowanych przy prowadzeniu wszelkich projektów tak w sferze publicznej jak i prywatnej.

Rozumiana szeroko jako część każdego podejmowanego projektu niezależnie od jego charakteru i celu. Prawidłowe zastosowanie wskazań *privacy by design* może dać bowiem bardzo pozytywne efekty nawet w działaniach na pozór nie związanych z zagadnieniami ochrony prywatności, czy ochrony danych osobowych.



## ŹRÓDŁA KONCEPCJI PRIVACY BY DESIGN

Zasady podstawowe prywatności w fazie projektowania mają umożliwić włączanie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji.

Prawidłowo zastosowane określają bowiem, w jaki sposób proaktywnie uczynić prywatność domyślnym sposobem działania w organizacji przy jednoczesnym utrzymaniu pełnej funkcjonalności – wymaga to podejścia do ochrony prywatności opartego na sumie pozytywnej, nie sumie zerowej.



## ŹRÓDŁA KONCEPCJI PRIVACY BY DESIGN

- Nie należy koncepcji *privacy by design* traktować jako pojęcia wytrycha, które, sugerując głębię tematyczną opartą na wątych acz szeroko akceptowanych hasłach, ma jedynie markować zaangażowanie osoby, używającej tego pojęcia, w ideę ochrony prywatności czy wężiej rozumianą ochronę danych osobowych.
- Istotne jest połączenie dyskusji o *privacy by design* z działaniami podejmowanymi na rzecz upowszechnienia stosowania oceny skutków przedsięwzięć dla ochrony prywatności (*privacy impact assessment* – PIA).

## OD IDEI DO PRAWA STANOWIONEGO

- Rezolucja w sprawie prywatności w fazie projektowania przyjętej przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności, która obradowała w Jerozolimie w dniach 27-29 października 2010 r.
- Zasady opisane w rezolucji stały się w ostatnich miesiącach podstawą do opracowania treści normatywnej w proponowanych przez Komisję Europejską nowych ramach prawnych ochrony danych osobowych w Unii Europejskiej.

## OD IDEI DO PRAWA STANOWIONEGO

- Rezolucja w sprawie prywatności w fazie projektowania przyjętej przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności, która obradowała w Jerozolimie w dniach 27-29 października 2010 r.
- Rzecznicy uznali, że wdrożenie koncepcji jest niezbędnym elementem podstawowej ochrony prywatności, a zasady podstawowe tej koncepcji stanowić powinny wytyczne dla wprowadzania prywatności jako domyślnego sposobu działania każdej organizacji.
- Oderwano koncepcję od teleinformatyki uznając, że dotyczy ona raczej zarządzania organizacją (prywatną lub publiczną) niż zarządzania systemem ICT lub projektem biznesowym. Rzecznicy zapowiedzieli, że będą wspierać włączanie podstawowych zasad prywatności w fazie projektowania w zakres polityki prywatności i ustawodawstwa w poszczególnych porządkach prawnych.

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

Wśród zasad podstawowych *privacy by design* wymieniono:

1. podejście proaktywne, nie reaktywne i zaradcze, nie naprawcze,
2. prywatność jako ustawienie domyślne,
3. prywatność włączoną w projekt,
4. pełną funkcjonalność rozumianą jako osiągnięcie sumy dodatniej, a nie sumy zerowej,
5. ochronę prywatności od początku do końca cyklu życia informacji,
6. transparentność i przejrzystość oraz
7. poszanowanie dla prywatności użytkowników.

Wprowadzenie w życie powyższych siedmiu zasad powinno nastąpić poprzez serię innowacji w procesie przygotowania organizacji do prowadzenia działań w sposób chroniący prywatność użytkowników. Do najważniejszych zadań – obok PIA – należą: prowadzenie analizy ryzyka, analizy luk, ocena zagrożeń, zarządzanie ryzykiem, audyt, certyfikacja i homologacja oraz przygotowywanie materiałów szkoleniowych dla członków organizacji.

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- Podstawą koncepcji *privacy by design* jest **proaktywne podejście** do zagadnienia ochrony prywatności. Zagadnienia ochrony prywatności traktowane są jako składnik zadania nie dlatego, że ich pominięcie może przynieść szkody w postaci incydentów bezpieczeństwa, lecz dlatego, że **są stałą składową zadania**. Tym samym niebezpieczeństwa dla prywatności użytkowników powinny być przewidywane z góry, a systemowo prowadzone zadanie powinno im zapobiegać.
- **Ochrona prywatności włączona (wbudowana) w projekt** co oznacza, że prywatność jest chroniona **nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję tak, że jest po prostu składową projektu**.
- W przypadku systemów teleinformatycznych oznacza to wbudowanie ochrony prywatności tak w architekturę system jak i w procesy biznesowe, które system obsługuje.



## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- Ciekawym wyzwaniem jest **postawienie takiego wymogu projektom legislacyjnym**. Musiałoby bowiem ono oznaczać, że bez ochrony prywatności akt prawny posiadałby nieusuwalne luki uniemożliwiające jego stosowanie. Jakkolwiek trudne się to wydaje, należy uznać, że dla niektórych projektów aktów prawnych taka cecha jest bardzo pożądana. Najlepszym przykładem będą tu akty dotyczące procedur administracyjnych i sądowych. W przypadku prawa polskiego wskazane byłoby wbudowanie ochrony prywatności w konstrukcję instrukcji kancelaryjnych, tak tych które wynikają wprost z aktów prawa stanowionego, jak i tych tworzonych wewnętrznie przez uprawnione do tego instytucje. Osiągnięcie stanu w którym ochrona prywatności byłaby „wbudowana” w proces legislacyjny nie jest jednak możliwe bez włączenia oceny skutków legislacji dla ochrony prywatności do istniejących dziś wytycznych dla przygotowywania oceny skutków regulacji (OSR). Jest oczywiste, że będzie to tylko uzupełnienie wytycznych a nie norm prawnych. Równie oczywiste jest, że rozwiązanie takie będzie krytykowane przez legislatorów jako dodatkowo opóźniające proces tworzenia prawa. Jednak postulat takiej powinien być wysuwany przez polski organ ochrony danych osobowych jako najlepszy sposób realizacji rezolucji jerozolimskiej.
- Patrz np.: *R. Suskind, Koniec świata prawników ? Współczesny charakter usług prawniczych*, Warszawa 2010, s. 141-143.

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- Nie należy mylić założeń **privacy by design** z koncepcją **privacy as the default**, czyli prywatności wynikającej z ustawień serwisu.
  - Prywatność jako ustawienie domyślne jest jedynie jednym z postulatów szerszej idei *privacy by design*.
  - Nie ma wątpliwości, że ustawienia domyślne przygotowane przez twórcę jakiegokolwiek systemu, będą używane przez większość jego użytkowników.
  - Ważnym postulatem jest więc potrzeba uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach domyślnych (początkowych) takiego systemu.
  - Użytkownik chcąc zrezygnować z części swej prywatności powinien podejmować aktywne działania w tym kierunku, a nie poddawać się ingerującym w jego prywatność decyzjom twórców systemu.
  - Użytkownik bierny nie staje się ofiarą swej bierności, lecz beneficjentem decyzji twórcy systemu.



## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- ***Privacy as a the default*** jest jednakże postulatem skierowanym do systemu w jednym określonym momencie. Przyjmuje się bowiem, że „sprawdzenie” następuje w momencie przyłączenia się użytkownika do systemu. Jest to niewątpliwie kluczowy moment dla ochrony prywatności użytkownika (w szczególności klienta zewnętrznego). Tym nie mniej dla całości funkcjonowania danego systemu jest to jedynie jeden z istotnych momentów. Stąd też zasada zachowania prywatności jako ustawienia domyślnego musi być zawsze uzupełniana opisaną niżej zasadą ochrony prywatności od początku do końca cyklu życia informacji.

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- **Wprowadzenie tzw. „pełnej funkcjonalności”.**
- Sformułowanie to niezbyt dobrze poddaje się tłumaczeniu z języka angielskiego i chyba lepiej jest używać tu nieco bardziej obrazowego postulatu „osiągania sumy dodatniej przy ochronie prywatności”.
  - zaprzeczenie tradycyjnym wyobrażeniom, w których ochronę danych osobowych i ochronę prywatności przedstawia się jako przeszkodę dla uzyskania pełnej (swobodnej) funkcjonalności systemu, uznając, że ochrona podstawowych wartości utrudnia działanie twórcom systemu, a czasem wręcz przeszkadza w osiągnięciu rzeczywistych celów tworzenia systemu.
  - Prawidłowe zastosowanie koncepcji prywatności w fazie projektowania umożliwia realizację wszystkich legitymowanych interesów i celów systemu i przeczy fałszywym dychotomiom i swoistemu „miareczkowaniu prywatności”.
  - *Patrz: A. Cavoukian, Biometric Encryption: A Positive-Sum Technology that achieves Strong Authentication, Security and Privacy [w:] A. Cavoukian (red.), 20/20 Access & Privacy Excellence ... 20 Years In the Making. 20th Anniversary Collection, Toronto 2007, s. 1-34.*

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

- **Wymaganie by ochrona prywatności dotyczyła całego „cyklu życia” informacji**
- Dla systemu ICT charakterystyczną cechą jest dążenie do osiągnięcia wymaganego efektu (np. odpowiedniego poziomu ochrony prywatności) w konkretnym momencie na osi czasu (najczęściej w momencie odbioru systemu przez zamawiającego, uruchomienia systemu lub osiągnięcia tzw. pełnej funkcjonalności).

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

**„End-to-end lifecycle protection”** oznacza wymaganie, by ochrona prywatności była integralną częścią procesu:

1. tworzenia systemu (również etapu deweloperskiego i testowego, podczas którego bardzo często dochodzi do rażących przykładów braku dbałości o przetwarzane dane, tylko na podstawie założenia, że „przecież są to jedynie dane testowe”),
2. wdrażania go i łączenia z istniejącymi już rozwiązaniami (konieczność uzyskania odpowiedniej interoperacyjności przy jednoczesnym utrzymaniu zasad ochrony prywatności i poufności danych),
3. rozbudowy, unowocześniania i możliwego łączenia z nieistniejącymi w danej chwili systemami,
4. usuwania danych niepotrzebnych i archiwizowania danych nieaktualnych (procesy te często nie są rozróżniane między sobą) oraz
5. likwidacji systemu jako całości lub całościowego przekształcenia go w inny system nieznany na etapie tworzenia systemu pierwotnego.

## ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA

### ***„End-to-end lifecycle protection”***

Nie należy zapominać, że wymaganie trwałości rozwiązań chroniących prywatność przez cały cykl życia informacji ma również swój sens ekonomiczny. Tylko na pozór śmiesznym zaleceniem jest postulat zapewnienia finansowania procesu utrzymania systemu i finansowania audytu oraz rozwoju ochrony prywatności. Być może jednak warto postawić ten postulat na czele organizacyjnych postulatów kierowanych wobec twórców założeń systemów. Zapewnić należy bowiem nie tylko środki finansowe na uruchomienie systemu, ale też na stałe naprawianie go i usprawnianie. Bez takiego pewnego źródła finansowania stworzymy bowiem „monstrum”, które raz zaczynając działać może przekształcić się w system samosterowalny w najgorszym tego słowa znaczeniu.



## REALIZACJA ZASAD W OGÓLNYM ROZPORZĄDZENIU O OCHRONIE DANYCH

- Proponowane przez Komisję Europejską nowe ramy ochrony danych osobowych w Unii Europejskiej, opierając się na wskazaniach Europejskiej Agendy Cyfrowej oraz Komunikatu Komisji w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności, **uznają, że uwzględnianie ochrony prywatności w fazie projektowania oznaczać powinno, iż kwestie prywatności i ochrony danych uwzględniane są w całym cyklu technologicznym, poczynając od etapu wczesnego projektowania technologii, po ich wdrożenie, wykorzystanie i ostateczne usunięcie.**
- Komisja już wcześniej zwracała uwagę, że prywatność nie była dostatecznie chroniona przez pierwszą generację przepisów o ochronie danych osobowych opartą na dyrektywie z 1995 r. czy na *Fair Information Practice Principles* ustalonych przez amerykańską Federalną Komisję Handlu. **Tym nie mniej proponowane tak w generalnym rozporządzeniu o ochronie danych, które ma zastąpić dyrektywę 95/46, jak i w skierowanej do byłego III filaru dyrektywie rozwiązania prawne nie wychodzą zbyt daleko poza konstrukcje klauzul generalnych.**

## REALIZACJA ZASAD W OGÓLNYM ROZPORZĄDZENIU O OCHRONIE DANYCH

- Preambuła: Ochrona praw i wolności osób fizycznych w zakresie przetwarzania ich danych osobowych wymaga, by „odpowiednie środki techniczne i organizacyjne” zastosowane zostały dla wypełnienia zasad wynikających z rozporządzenia tak na etapie projektowania zasad przetwarzania danych, jak i podczas samego przetwarzania danych. Jednocześnie preambuła przywołuje obowiązek administratora danych wdrożenia odpowiednich polityk i środków celem wypełnienia zasad ochrony danych „*by design*” i „*by default*”. Obie zasady powinny być również respektowane przy tworzeniu przez Komisję Europejską delegowanych aktów wykonawczych do rozporządzenia.



## REALIZACJA ZASAD W OGÓLNYM ROZPORZĄDZENIU O OCHRONIE DANYCH

Zasadam tym poświęcono cały artykuł 23 rozporządzenia i odpowiadający mu art. 21 dyrektywy. W projekcie czytamy:

***„Artykuł 23 Uwzględnienie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna***

1. Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, administrator, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia oraz gwarantowało ochronę praw podmiotu danych.
2. Administrator wdraża mechanizmy służące zapewnieniu, by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla realizacji każdorazowego szczególnego celu przetwarzania oraz by w szczególności nie były one zbierane lub zatrzymywane dłużej niż przez okres niezbędny do realizacji tych celów, zarówno jeśli chodzi o ilość danych, jak i okres ich przechowywania. Mechanizmy te zapewniają w szczególności, by dane osobowe nie były domyślnie udostępniane nieograniczonej liczbie osób.

## REALIZACJA ZASAD W OGÓLNYM ROZPORZĄDZENIU O OCHRONIE DANYCH

***„Artykuł 23 Uwzględnienie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna***

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu określenia dalszych kryteriów i wymogów dotyczących właściwych środków i mechanizmów, o których mowa w ust. 1 i 2, w szczególności wymogów w zakresie uwzględnienia ochrony danych już w fazie projektowania w odniesieniu do sektorów, produktów i usług.
4. Komisja może ustanowić standardy techniczne dotyczące wymogów ustanowionych w ust. 1 i 2. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

## ROLA OCEN SKUTKÓW PRZEDSIĘWZIĘCIA DLA OCHRONY DANYCH

- Przyjmując, że rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest stosowanie oceny skutków projektu dla ochrony prywatności (PIA), należy zauważyć, że ten sam projekt nowych ram prawnych ochrony danych w Unii Europejskiej stawia już znacznie więcej wymagań jeśli chodzi o stosowanie PIA.
- Komisja decydując się na odejście od notyfikacji i rejestracji zbiorów jako zasady, zastępuje ją obowiązkiem przeprowadzania oceny skutków przetwarzania danych dla ochrony prywatności osób fizycznych.
- Komisja nie określa na czym dokładnie ma polegać ocena – wydaje się, że wciąż czeka na propozycje takich testów, które powstają obecnie w środowisku naukowym
- Komisja stwierdza, że po pierwsze wyniki takiej oceny powinny być z zasady (choć dopuszczane są tu wyjątki) dostępne publicznie, a oceną objąć należy przede wszystkim przewidywane środki, mechanizmy i zabezpieczenia, które powinny prowadzić do zgodności przetwarzania danych z wymaganiami prawa Europejskiego.

## ROLA OCEN SKUTKÓW PRZEDSIĘWZIĘCIA DLA OCHRONY DANYCH

- Szczególną rolę PIA spełniał będzie wówczas, gdy jego wyniki wskazywać będą, że przetwarzanie danych w ramach danego projektu może rodzić „wysoki stopień szczególnego ryzyka dla praw i wolności osoby” (*involves a high degree of specific risks to the rights and freedoms of data subjects*). Stanie się on bowiem podstawą do oceny projektu przez organ ochrony danych osobowych.
- Jest tym samym oczywiste, że tego typu ocena musi pojawić się na etapie projektowania. Jej wynik bowiem doprowadzi dopiero do decyzji, czy przetwarzanie danych w projektowany sposób musi podlegać uprzedniej konsultacji i aprobacie ze strony rzecznika ochrony danych osobowych.

## ROLA OCEN SKUTKÓW PRZEDSIĘWZIĘCIA DLA OCHRONY DANYCH

Za operacje mogące rodzić „wysoki stopień szczególnego ryzyka dla praw i wolności osoby” uznano:

- **profilowanie** – (ocena, analiza lub przewidywanie aspektów osobowych w stosunku do osób fizycznych w zakresie zachowania w pracy, zdolności kredytowej (*creditworthiness*), sytuacji ekonomicznej, lokalizacji, zdrowia, osobistych preferencji, wiarygodności (*reliability*) lub zachowania, jeśli takie przewidywanie oparte jest na automatycznym przetwarzaniu danych i może wpływać znacząco na sytuację osoby);
- przetwarzanie danych o życiu seksualnym, zdrowiu, pochodzeniu rasowym i etnicznym lub (**nowa „lista danych wrażliwych”**);
- przetwarzanie danych osobowych na potrzeby **ochrony zdrowia, badań epidemiologicznych lub badań nad chorobami psychicznymi lub zakaźnymi**;
- **monitorowanie publicznie dostępnych miejsc**, a w szczególności wideo nadzór oraz
- - przetwarzanie **w systemach wielkoskalowych danych osobowych dzieci, danych biometrycznych lub genetycznych**.



## ROLA OCEN SKUTKÓW PRZEDSIĘWZIĘCIA DLA OCHRONY DANYCH

- Jednocześnie projektodawcy zwracają uwagę (art. 30 ust. 4) na konieczność konsultowania zamiaru przetwarzania danych osobowych z pomiotami, których dane mają być przetwarzane lub z ich przedstawicielami. Nie wyjaśniono w żaden sposób na czym tego typu konsultacja miałaby polegać, ale widać w tej idei wpływ prawa ochrony konsumentów, gdzie rola stowarzyszeń konsumenckich przy tego typu działaniach jest już od dawna uznawana za oczywistą.
- Warto zwrócić uwagę, że przetwarzanie danych na potrzeby ochrony zdrowia (*for the provision of health care*) odróżniane jest wyraźnie od przetwarzania danych „o zdrowiu”. Ten pierwszy termin ma więc zdaniem projektodawców znacznie szersze znaczenie. Można uznać, że w tym przypadku chodzi o przetwarzanie jakichkolwiek danych osobowych w systemach używanych w ochronie zdrowia, które w jakikolwiek sposób (automatycznie lub manualnie) mogłyby być potencjalnie łączone z danymi osobowymi pacjentów, lekarzy, personelu medycznego i pomocniczego. W każdym z takich przypadków należy przygotować ocenę skutków projektu dla ochrony prywatności i aktualizować takie PIA na każdym etapie tworzenia systemu.

DZIĘKUJĘ ZA UWAGĘ