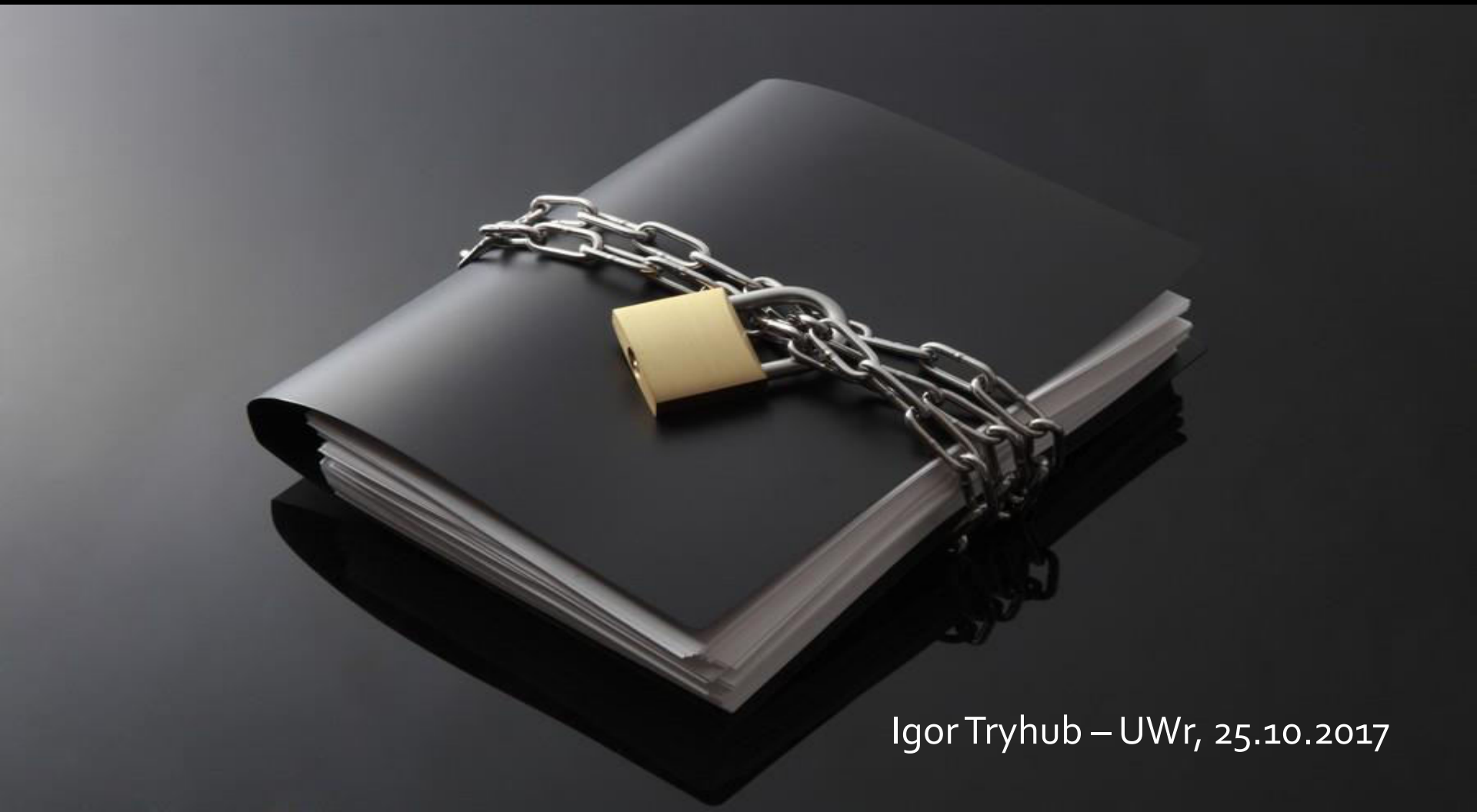
Metodyka zarządzania ryzykiem w ochronie danych osobowych



Igor Tryhub – UWr, 25.10.2017

Cele FBI

- podejmowanie działań na rzecz wspierania bezpieczeństwa informacyjnego i cyberprzestrzeni w Polsce
- budowanie świadomości w zakresie bezpieczeństwa oraz świadomego wykorzystania Internetu
- przegląd skuteczności i efektowności stosowanych zabezpieczeń, w tym projektowanie i propagowanie nowych rozwiązań organizacyjnych i technicznych powodujących wzrost bezpieczeństwa w kraju

Kary finansowe

Niezgodność z wymaganiami RODO może doprowadzić do nałożenia grzywny wysokości do 10 mln EUR, lub do 2% łącznej kwoty światowego rocznego obrotu (wyższa z tych wartości).
Nałożenie grzywny może wynikać z:

- a) niepodjęcia oceny skutków dla ochrony lub
- b) przeprowadzania oceny skutków dla ochrony danych w niewłaściwy sposób lub
- c) niezasięgnięcia opinii właściwego organu nadzoru w razie potrzeby

Cele procesu

- bieżące zapewnienie adekwatnych oraz skutecznych środków organizacyjnych i technicznych minimalizujących ryzyko naruszenia praw i wolności osób fizycznych
- zapewnienie ochrony przed nieuprawnionym dostępem do danych osobowych i aktywów służących ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych osobowych i aktywów
- zapewnienie rozliczalności (nie tylko spełnienie wymagań RODO, ale także wykazanie, że zostały podjęte odpowiednie środki w celu zapewnienia zgodności)

Ocena skutków dla ODO

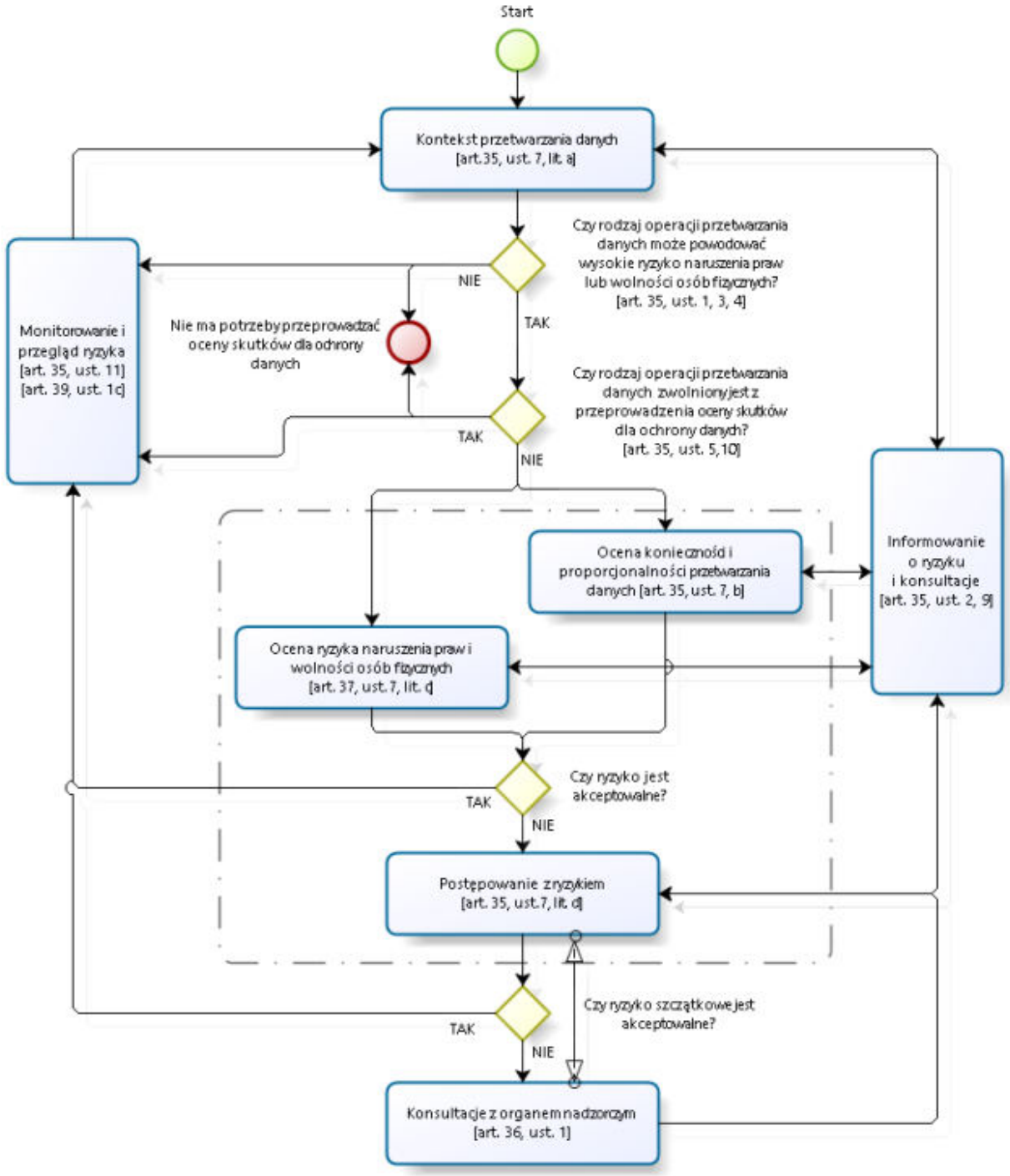
- ocena skutków dla ochrony danych osobowych jest mechanizmem, który pomaga administratorom danych w zachowaniu zgodności z prawem
- jest obowiązkowe jedynie wtedy, gdy przetwarzanie "może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”
- jest to szczególnie ważne w przypadku wprowadzenia nowych technologii lub rozwiązań dotyczących przetwarzania danych

Operacje o potencjalnie wysokim ryzyku naruszenia praw i wolności

- Systematyczne monitorowanie
- Dane osobowe wrażliwe
- Dane przetwarzane na dużą skalę
- Zestawy danych, które zostały dopasowane lub połączone
- Pozbawienie osób fizycznych przysługujących praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi
- Innowacyjne wykorzystanie lub stosowanie rozwiązań technologicznych lub organizacyjnych
- Przesyłanie danych poza granice Unii Europejskiej
- Uniemożliwienie osobie fizycznej korzystania z prawa lub korzystania z usługi lub umowy

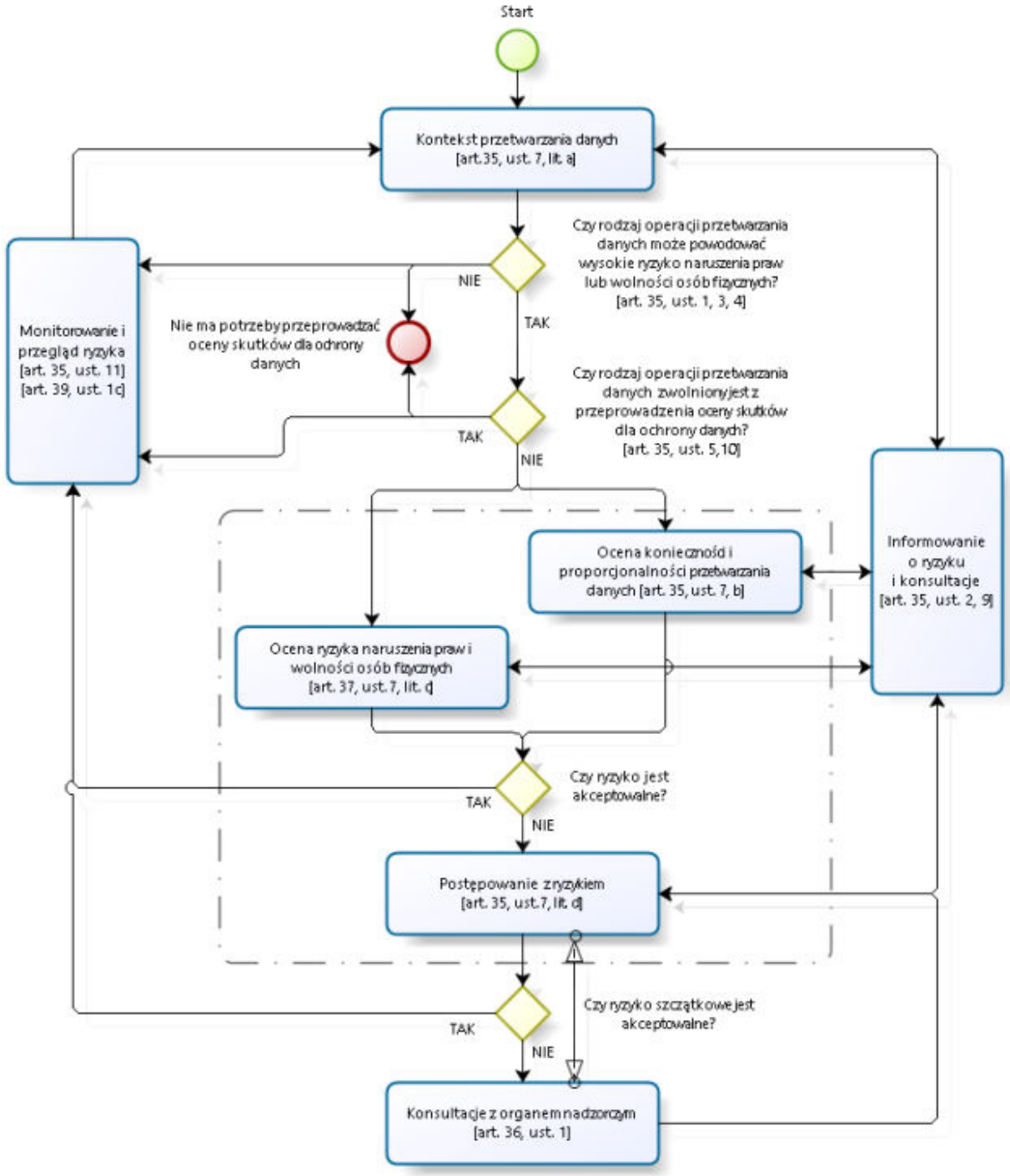
Skutki przeprowadzenia analizy i oceny ryzyka

- Podjęcie działań korygujących lub zapobiegawczych
- Poinformowanie lub/i podjęcie konsultacji z organami nadzorczymi
- Poinformowanie lub/i podjęcie konsultacji z Klientami
- Poinformowanie osób fizycznych, których dane osobowe dotyczą
- Przeprowadzenie kontroli lub/i audytów wewnętrznych, zewnętrznych (w tym testów penetracyjnych) w organizacji lub dostawców/wykonawców (procesorów danych)
- Potwierdzenie aktualności kontekstu przetwarzania danych, w szczególności inwentaryzacji aktywów.
- Unikanie przetwarzania
- Przeniesienie przetwarzania danych osobowych
- Zdefiniowanie wymagań bezpieczeństwa dla systemów informatycznych lub usług IT


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

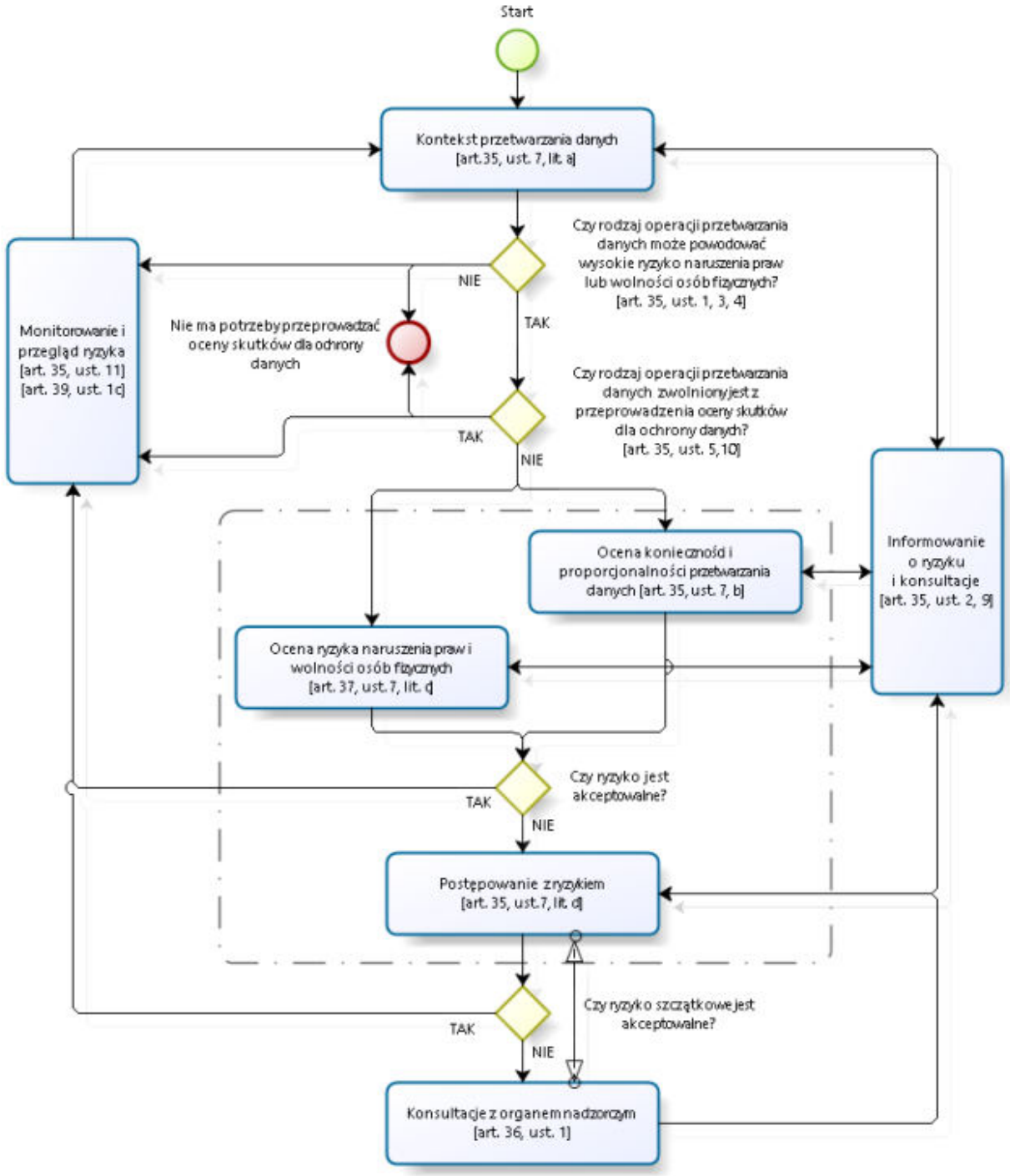
Opis procesu zarządzania ryzykiem

1. Określenie kontekstu przetwarzania
2. Ocena, czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych
3. Ocena, czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych
4. Ocena konieczności i proporcjonalności przetwarzania danych
5. Ocena ryzyka naruszenia praw i wolności osób fizycznych
6. Ocena, czy ryzyko jest akceptowalne
7. Przeprowadzenie postępowania z ryzykiem
8. Ocena, czy ryzyko szczątkowe jest akceptowalne
9. Informowanie o ryzyku lub/i przeprowadzenie konsultacji
10. Przeprowadzenie konsultacji z organem nadzorczym
11. Nie ma potrzeby przeprowadzenia oceny skutków dla ochrony danych osobowych
12. Monitorowanie i przegląd ryzyka


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

1-3: Kontekst przetwarzania danych

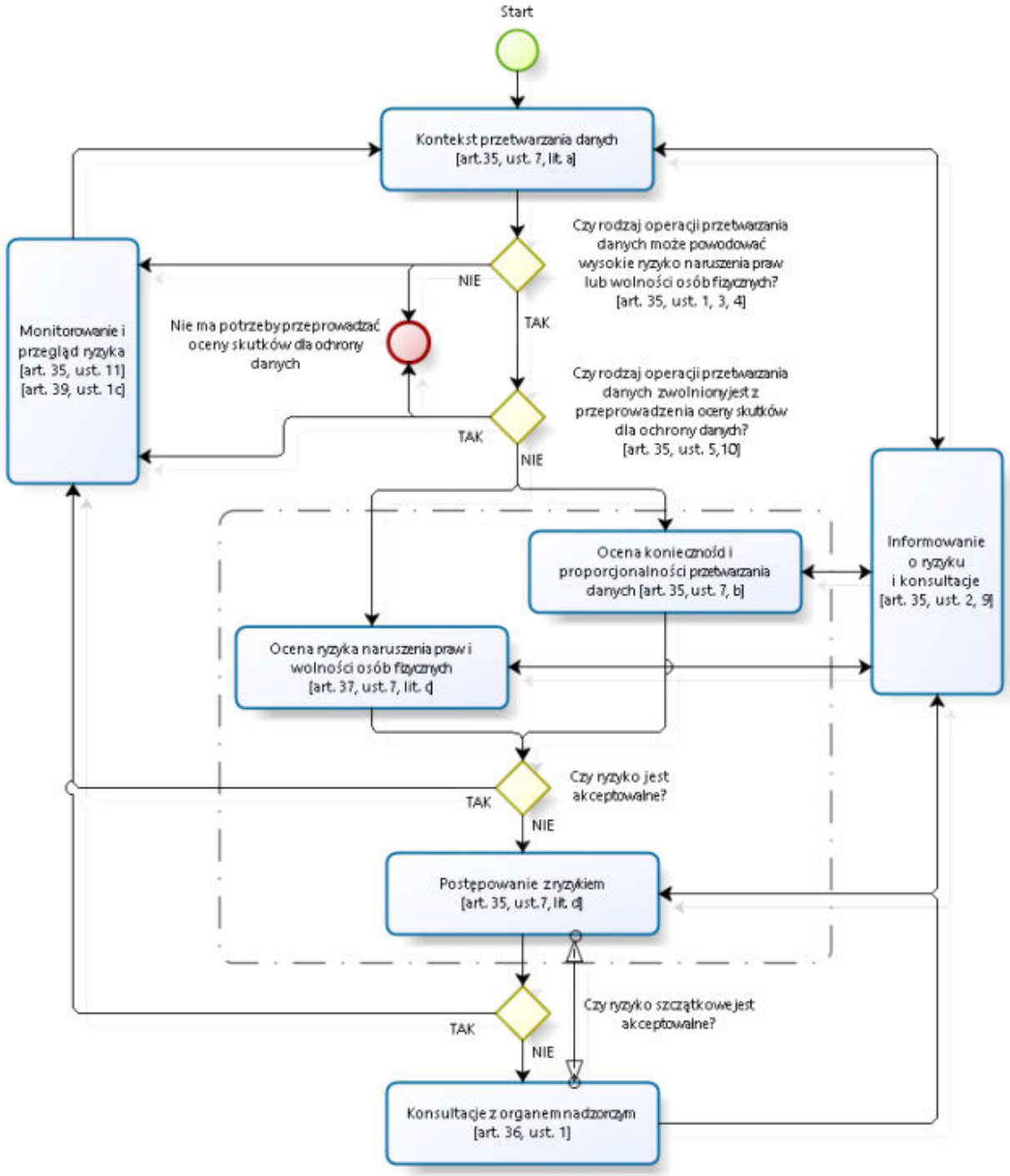
1. charakter danych osobowych
2. zakres przetwarzania
3. cel w którym zebrano dane osobowe
4. odbiorcy i przetwarzający dane osobowe
5. okres przechowywania danych


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

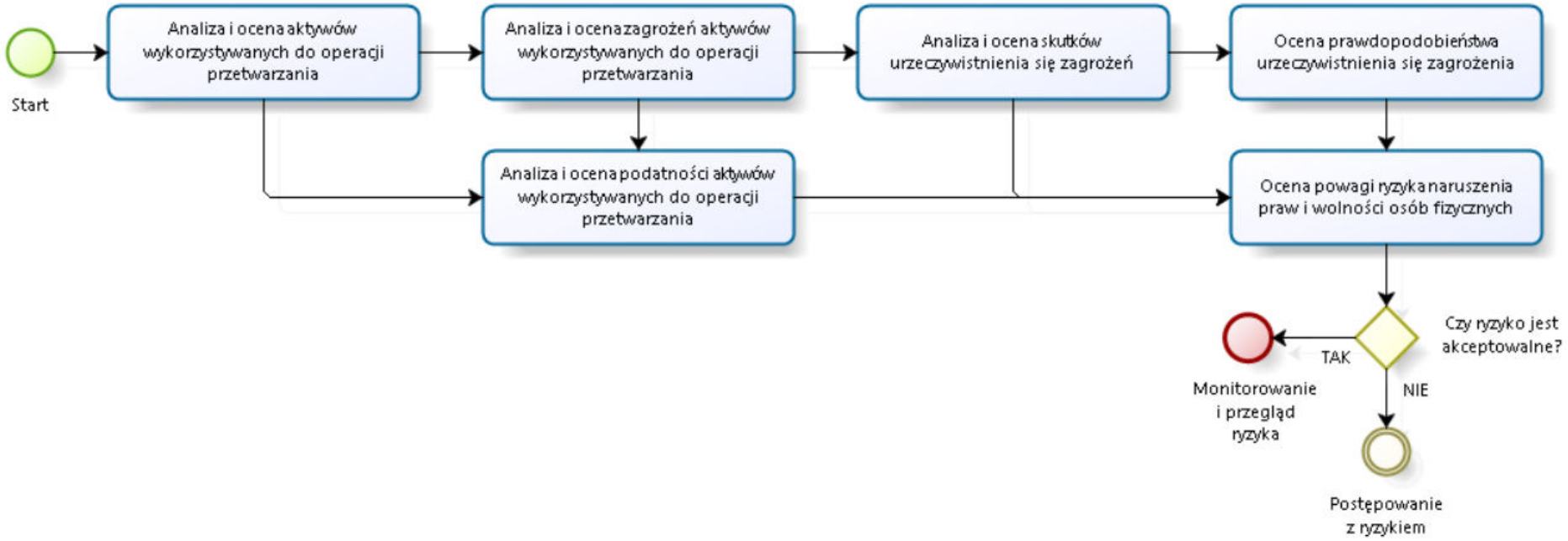
4: Ocena konieczności i proporcjonalności przetwarzania

Należy zweryfikować i udokumentować czy:

1. DO zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach
2. DO przetwarzane są zgodnie z prawem
3. DO są adekwatne, stosowne oraz ograniczone do celów
4. został ograniczony czas przechowywania danych
5. zapewnione są środki dla udzielenia informacji osobie, której dane dotyczą


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

5: Ocena ryzyka naruszenia praw i wolności osób fizycznych



5.1: Aktywy wykorzystywane do operacji przetwarzania

Należy zidentyfikować i zinwentaryzować aktywa – zasoby niezbędne do realizacji czynności związanych z operacjami przetwarzania danych osobowych:

- Procesy i działania biznesowe
- Personel
- Sprzęt
- Siedziba
- Oprogramowanie
- Sieć
- Organizacja
- Informacje

5.2: Zagrożenia aktywów do przetwarzania

- Dla zidentyfikowanych aktywów należy przypisać zagrożenia, które mogą oddziaływać na naruszenie praw i wolności osób fizycznych
- Zagrożenie – potencjalna przyczyna niepożądanego incydentu, która może wywołać naruszenie praw i wolności osób fizycznych

5.2: Przykłady zagrożeń aktywów

- Zniszczenia fizyczne
- Utrata podstawowych usług
- Naruszenie praw i wolności osób fizycznych
- Naruszenie bezpieczeństwa informacji
- Awarie techniczne
- Nieautoryzowane działania
- Naruszenie bezpieczeństwa funkcji
- Zagrożenia osobowe

5.3: Skutki urzeczywistnienia się zagrożeń

Dla każdego zagrożenia zidentyfikowanego w ramach aktywa należy przeanalizować wpływ (skutki) na zmaterializowanie się zagrożeń w kontekście naruszenia praw i wolności osób fizycznych

5.3: Skutki naruszenia

Lp.	Katalog skutków naruszenia praw i wolności osób fizycznych
1	Dyskryminacja
2	Kradzież tożsamości lub oszustwo dotyczące tożsamości
3	Strata finansowa
4	Naruszenie dobrego imienia
5	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową
6	Nieuprawnione odwrócenie pseudonimizacji
7	Wszelka inna znacząca szkoda gospodarcza lub społeczna

5.4: Podatności aktywów do przetwarzania

- Dla każdego zagrożenia zidentyfikowanego w ramach aktywa należy przypisać podatności
- Podatność – źródło zagrożenia, słabość lub luka aktywa lub zabezpieczania, która może być wykorzystana do urzeczywistniania się zagrożenia

5.5: Prawdopodobieństwa urzeczywistnienia się zagrożenia

Każde zagrożenie zidentyfikowane w ramach aktywa, przy uwzględnieniu zidentyfikowanych podatności i istniejących zabezpieczeń, należy ocenić w kontekście prawdopodobieństwa urzeczywistnienia się zagrożenie

6: Powagi ryzyka naruszenia praw i wolności osób fizycznych

$$R = S * P_{Pod} * P_{Pb}$$

gdzie:

- R – Ocena powagi ryzyka naruszenia praw i wolności osób fizycznych
- S – Ocena skutków naruszenia praw i wolności osób fizycznych
- $PPod$ - Ocena podatności aktywów wykorzystywanych do operacji przetwarzania
- PPb – Ocena prawdopodobieństwa urzeczywistnienia się zagrożenia

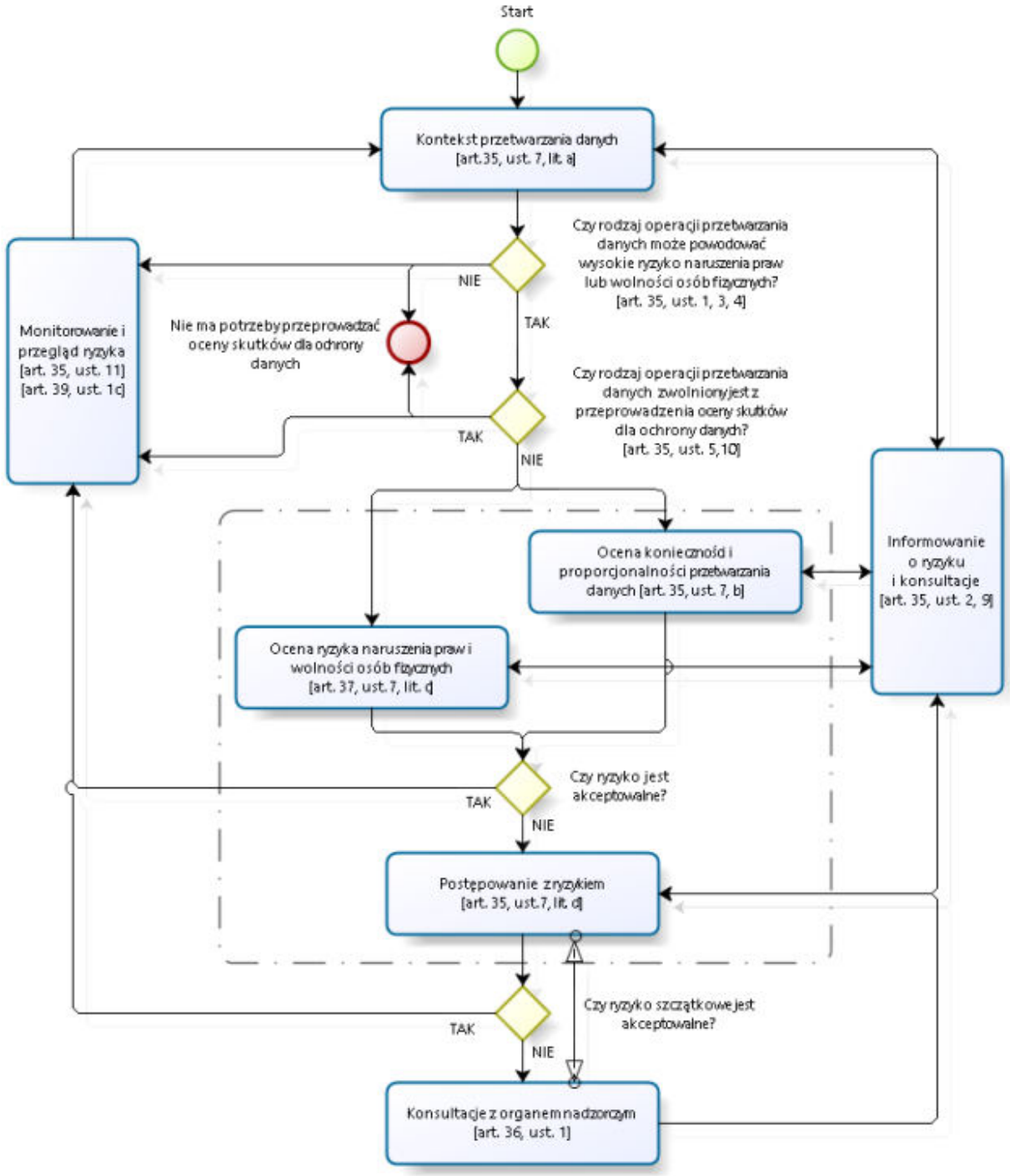
6: Rozkład ryzyka

Ocena prawdopodobieństwa		Ocena skutków x Ocena podatności					
		1	**2**	**3**	**4**	**6**	**9**
	1	1	2	3	4	6	9
	2	2	4	6	8	12	18
	3	3	6	9	12	18	27

Tabela 7. Macierz rozkładu oceny ryzyka naruszeniem praw i wolności osób fizycznych

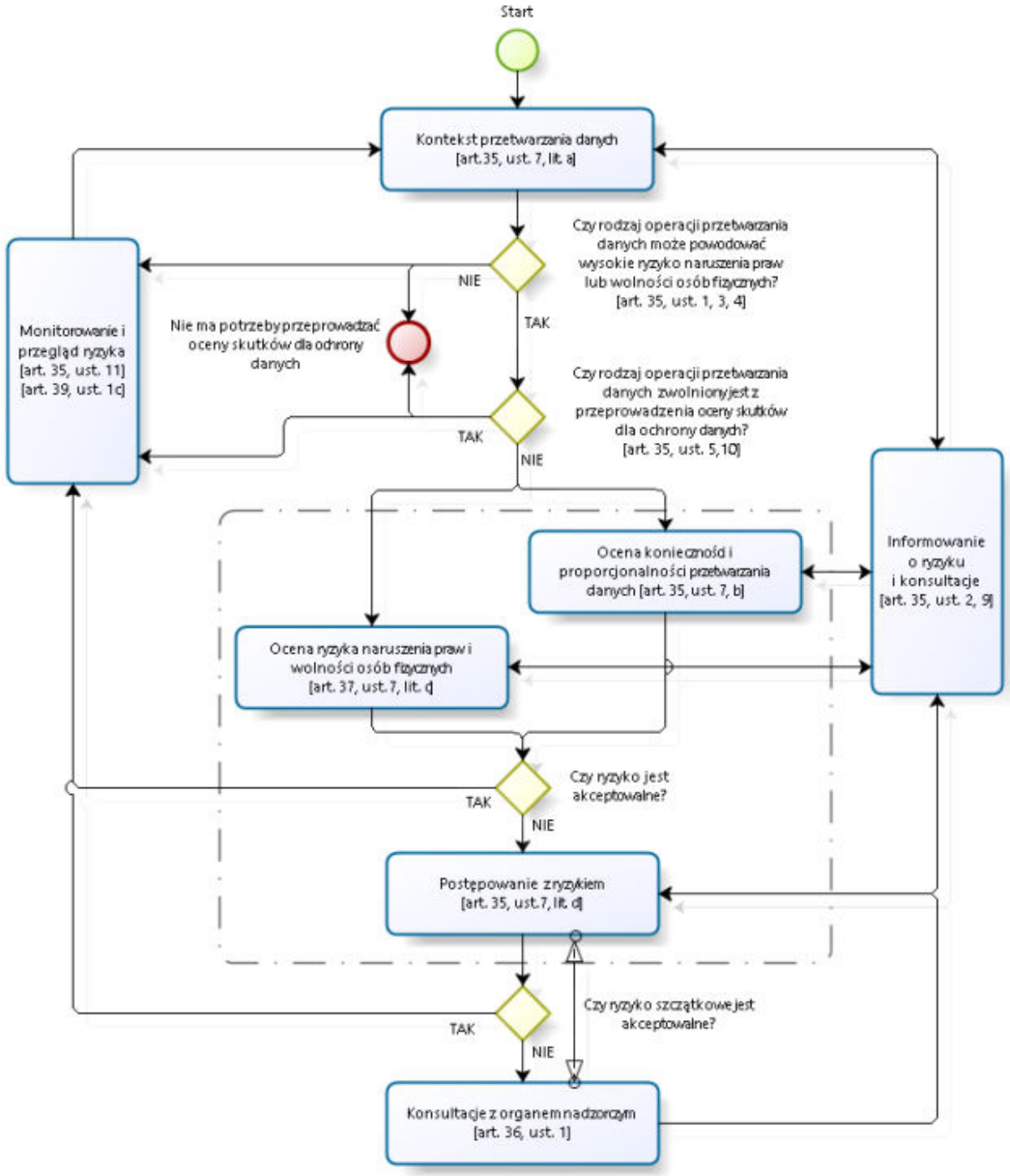
Poziom	Skala wartości	Opis
Niskie ryzyko	od 1 do 8	Ryzyka akceptowane, niewymagające dalszego postępowania.
Wysokie ryzyko	od 9 do 27	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem

Tabela 8. Poziom akceptacji ryzyka naruszeniem praw i wolności osób fizycznych


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

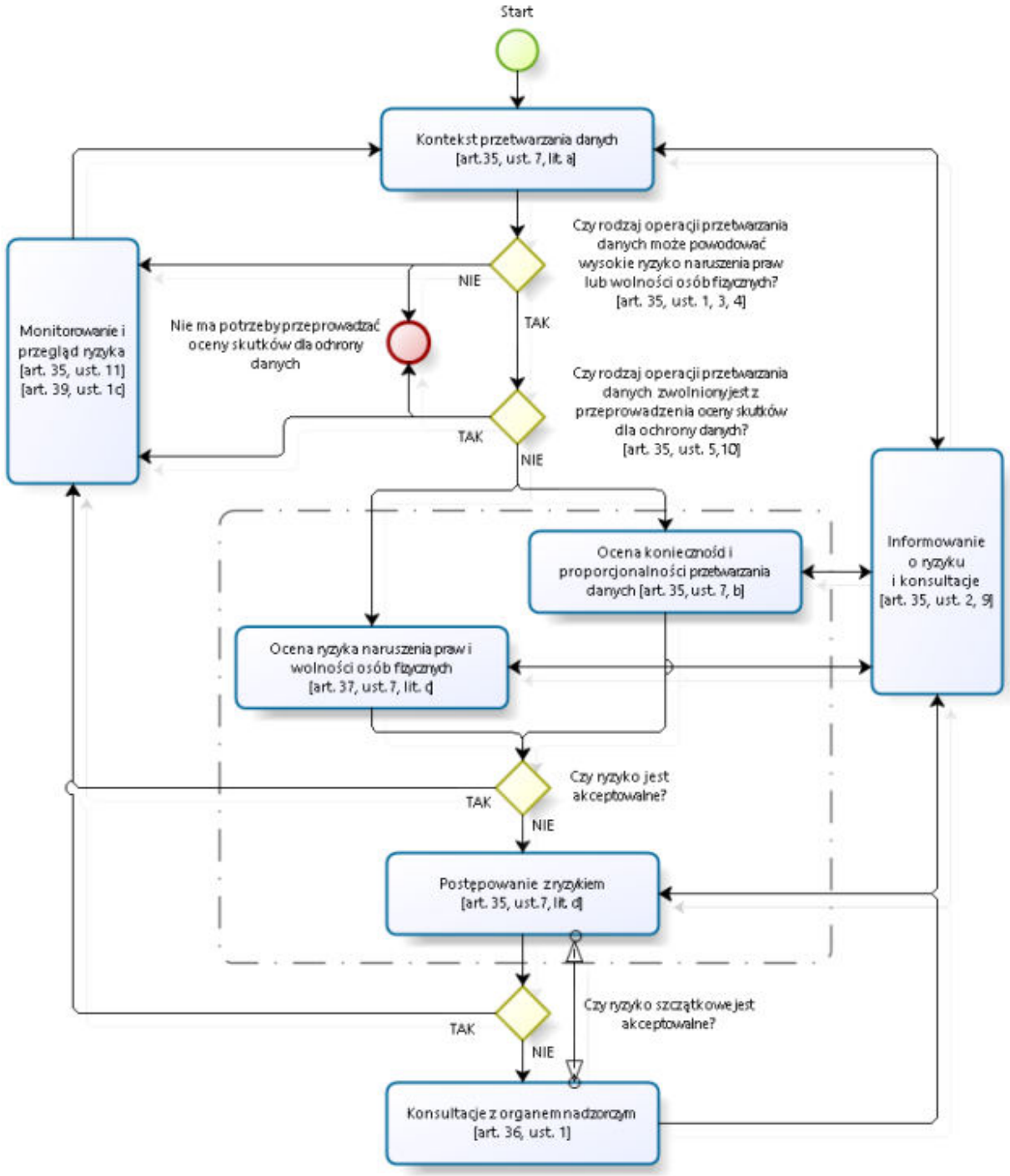
7: Postępowanie z ryzykiem

- Cel – dokonanie wyboru wariantu postępowania z ryzykiem oraz zaplanowanie zabezpieczeń organizacyjnych i technicznych:
  - minimalizacja ryzyka
  - unikanie ryzyka
  - transfer ryzyka
  - akceptacja ryzyka
- Wynik – dokument „Plan postępowania z ryzykiem”, na podstawie którego każda odpowiedzialna osoba powinna definiować sposób osiągania deklarowanego efektu w zadeklarowanym terminie.


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

8: Konsultacje z organem nadzorczym

- Jeżeli po przeprowadzeniu postępowania z ryzykiem nadal nie ma możliwość zmitygowania ryzyka do poziomu akceptowalnego i zapewnienia zgodności z wymaganiami RODO, to przed rozpoczęciem przetwarzania administrator musi skonsultować się z organem nadzorczym
- Uwaga: są przypadki, gdzie może być wymagane, aby administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednią zgodę na przetwarzanie danych osobowych, w tym związanych z ochroną socjalną i zdrowiem publicznym

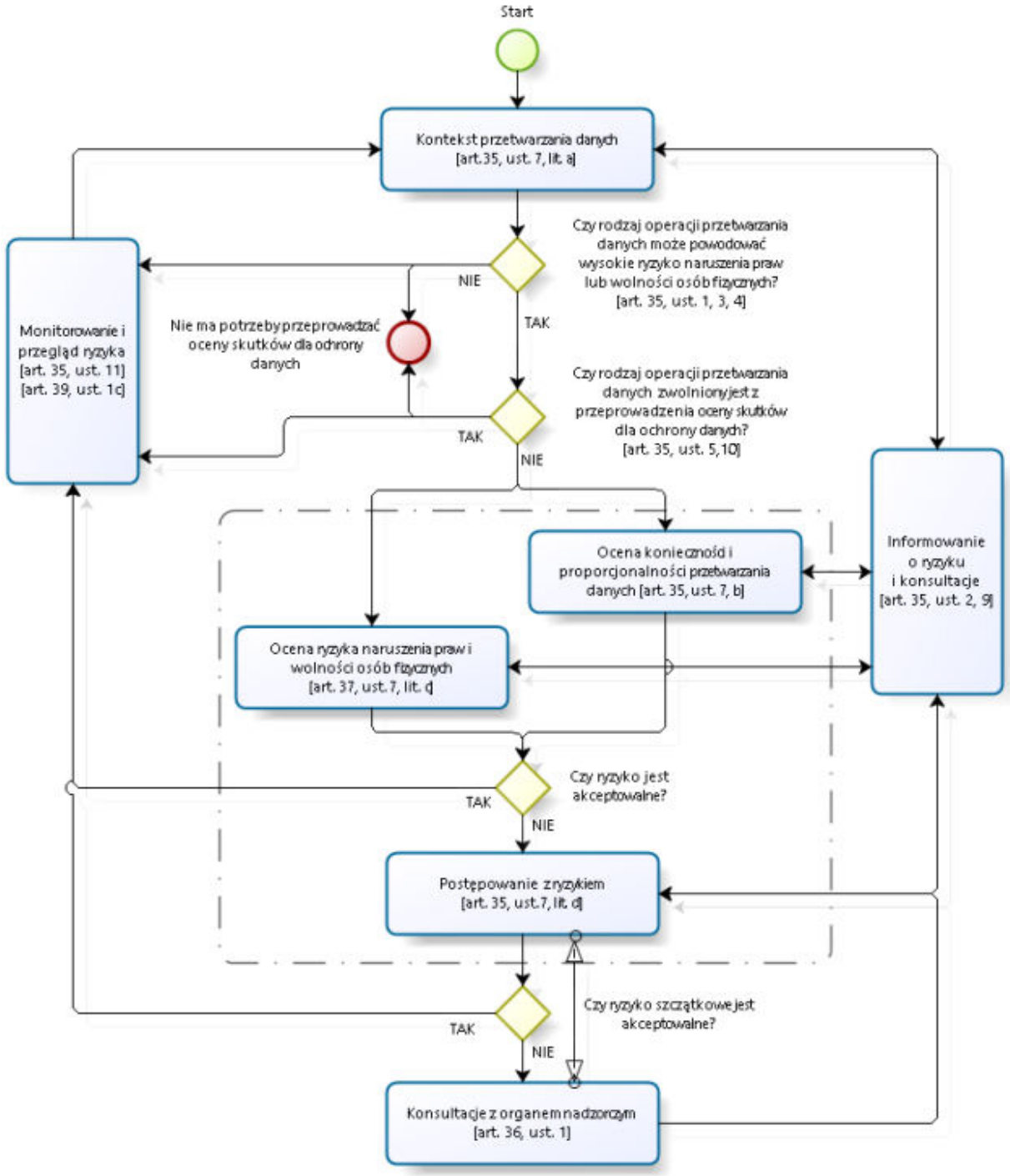

Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

9-10: Informowanie o ryzyku i konsultacje

- Powinny być zaangażowane wszystkie strony zainteresowane na każdym etapie procesu zarządzania ryzykiem ODO
- W stosownych przypadkach zaleca się zasięganie opinii niezależnych ekspertów różnych zawodów, tj. prawników, informatyków, ekspertów ds. bezpieczeństwa
- Informowanie o ryzyku powinno być realizowane zgodnie z zasadą "need to know"

9-10: Role i odpowiedzialności

- Podział osób na podstawie modelu RACI:
  - Responsible – odpowiedzialna za realizację zadań
  - Approver – nadzorująca i zatwierdzająca realizację zadań
  - Consulted – konsultująca i doradzająca w realizacji zadań
  - Informed – informowana o prowadzonych działaniach oraz niewpływająca na realizację zadań


Start
Kontekst przetwarzania danych [art.35, ust. 7, lit. a]
Czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? [art. 35, ust. 1, 3, 4]
NIE
TAK
Nie ma potrzeby przeprowadzać oceny skutków dla ochrony danych
Monitorowanie i przegląd ryzyka [art. 35, ust. 11] [art. 39, ust. 1c]
Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? [art. 35, ust. 5,10]
TAK
NIE
Informowanie o ryzyku i konsultacje [art. 35, ust. 2, 9]
Ocena konieczności i proporcjonalności przetwarzania danych [art. 35, ust. 7, b]
Ocena ryzyka naruszenia praw i wolności osób fizycznych [art. 37, ust. 7, lit. c]
Czy ryzyko jest akceptowalne?
TAK
NIE
Postępowanie z ryzykiem [art. 35, ust.7, lit. d]
Czy ryzyko szczątkowe jest akceptowalne?
TAK
NIE
Konsultacje z organem nadzorczym [art. 36, ust. 1]

11-12: Monitorowanie i przegląd ryzyka

- Powinien być realizowany na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych
- Proces monitorowania powinien być realizowany na bieżącą
- Weryfikacja powinna być przeprowadzona co najmniej raz w roku lub częściej w przypadku modyfikacji lub planowania modyfikacji kontekstu przetwarzania danych
- Wyniki procesu monitorowania i przeglądu powinny być dokumentowane, w tym zgłaszane i obsługiwane nieprawidłowości i słabości mechanizmów ochrony danych osobowych, w celach dowodowych

Dziękuję!