Jak zmieni się nasze otoczenie prawne?

# Rozporządzenia DORA | implementacja w polskim sektorze bankowym

Paweł Rudolf | Counsel

Forum Technologii Bankowości Spółdzielczej

Warszawa, 1 czerwca 2023 r.

# DORA | Garść faktów

- 28 listopada 2022 r. Rada UE przyjęła nowy akt - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (ang. *Digital Operational Resilience Act*)

- DORA jest odpowiedzią na narastającą potrzebę wypracowania wspólnotowych rozwiązań legislacyjnych w zakresie wzmocnienia cyberbezpieczeństwa usług finansowych. Kładzie nacisk na przeciwdziałanie ryzyku operacyjnemu i zagrożeniom, które pociągają za sobą technologie cyfrowe

- Znajduje bezpośrednie zastosowanie i co do zasady nie wymaga implementacji lub wydania krajowych przepisów służących jej stosowaniu, poza ściśle określonymi wyjątkami, tj. przede wszystkim w zakresie przepisów ustanawiających kary administracyjne czy sankcje karne

- Dla prawidłowego stosowania DORA do 17 stycznia 2024 r. mają zostać wydane przez właściwe unijne organy dodatkowe nadzorcze regulacyjne standardy techniczne (RTS)

- Rozporządzenie weszło w życie 16 stycznia 2023 r. i będzie obowiązywać od 17 stycznia 2025 r.

# DORA skierowana jest głównie do instytucji rynku finansowego, w tym przede wszystkim do:

| | | | | |
|---|---|---|---|---|
| **banków** (instytucji kredytowych) | firm inwestycyjnych | instytucji płatniczych | zakładów ubezpieczeń i reasekuracji | instytucji pieniądza elektronicznego |
| dostawców usług z zakresu kryptoaktywów | zarządzających alternatywnymi funduszami inwestycyjnymi | dostawców usług finansowania społecznościowego (crowdfunding) | repozytoriów sekurytyzacji | administratorów kluczowych wskaźników referencyjnych |
| | kontrahentow centralnych | zewnętrzni dostawcy usług ICT | przewiduje szereg wyłączeń w zakresie jej stosowania, w tym „opcje nardowe” | |

DZP

# DORA

## Zasada proporcjonalności

Podmioty finansowe stosują regulacje w sposób proporcjonalny do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności swoich usług, działań i operacji, jak szczegółowo przewidziano w odpowiednich przepisach tych rozdziałów.*

Nadzór finansowy analizują stosowanie zasady proporcjonalności przez podmioty finansowe przy dokonywaniu przeglądu spójności ram zarządzania ryzykiem związanym z ICT na podstawie przedkładanych na żądanie sprawozdań.

**nie dotyczy wymiany informacji*

# DORA

## Odpowiedzialność korporacyjna

Organ zarządzający podmiotu finansowego określa, zatwierdza i nadzoruje wdrażanie wszystkich ustaleń dotyczących ram zarządzania ryzykiem związanym z ICT oraz ponosi odpowiedzialność za ich wdrażanie (art. 5 ust. 2)

Ostateczna odpowiedzialność organu zarządzającego za zarządzanie w zakresie ryzyka związanego z ICT podmiotu finansowego stanowi nadrzędną zasadę w kompleksowym podejściu do zarządzania ryzykiem ICT, przekładającą się dodatkowo na ciągłe zaangażowanie organu zarządzającego w kontrolę monitorowania zarządzania w zakresie ryzyka związanego z ICT.

# DORA

## Czym są usługi ICT?

Usługi ICT to usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej.

Zewnętrzny dostawca usług ICT to oznacza przedsiębiorstwo świadczące usługi ICT.

# DORA | Główne obszary regulacji

## Zarządzanie ryzykiem związanym z ICT

- wewnętrzne ramy zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z ICT*

## Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i zgłaszanie

- identyfikowanie, śledzenie, rejestrowanie, kategoryzowanie i klasyfikowania oraz zgłaszanie incydentów związanych z ICT według ich priorytetu i dotkliwości oraz krytyczności usług, na które incydenty te mają wpływ

## Testowanie operacyjnej odporności cyfrowej

- ustanowienie i utrzymywanie adekwatnego i kompleksowego programu testowania operacyjnej odporności cyfrowej stanowiącego integralną część ram zarządzania ryzykiem związanym z ICT

## Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT

- zarządzanie ze strony zewnętrznych dostawców usług ICT odbywa się w świetle zasady proporcjonalności, z uwzględnieniem charakteru, skali, stopnia złożoności i znaczenia zależności w zakresie ICT

## Zasady dotyczące wymiany informacji

- podmioty finansowe mogą wymieniać między sobą informacje o cyberzagrożeniu i wyniki analiz takiego cyberzagrożenia, w tym oznaki naruszenia integralności systemu, taktykę, techniki i procedury

**odpowiednie rozdzielenie i niezależność funkcji zarządzania ryzykiem związanym z ICT, funkcji kontroli oraz funkcji audytu wewnętrznego, zgodnie z modelem trzech linii obrony lub wewnętrznym modelem zarządzania ryzykiem i kontroli ryzyka.*

DZP

# DORA | Zarządzanie ryzykiem ICT

## IDENTYFIKACJA

- wszystkie wspierane przez ICT funkcje biznesowe
- źródła ryzyka związanego z ICT, w tym w odniesieniu do innych podmiotów finansowych
- wszystkie zasoby informacyjne i zasoby ICT, w tym zasoby zdalne, zasoby sieciowe i sprzęt komputerowy
- zmiany w infrastrukturze sieci i systemów informatycznych

## OCHRONA I ZAPOBIEGANIE

- bezpieczeństwo przekazywania i przechowywania danych
- zarządzanie siecią i infrastrukturą
- zarządzanie dostępem do zasobów informacyjnych i ICT
- silne mechanizmy uwierzytelniania

## WYKRYWANIE

- Identyfikacja nietypowych działań
- identyfikacja potencjalnych istotnych pojedynczych punktów awarii
- monitorowanie działalności użytkowników

## REAGOWANIE I PRZYWRACANIA SPRAWNOŚCI

- zapewnienie ciągłości funkcji krytycznych i istotnych
- plany awaryjne w zakresie ICT
- działania w zakresie komunikacji i zarządzania kryzysowego
- procedury tworzenia kopii zapasowych oraz przywracania i odzyskiwania danych

## UCZENIE SIĘ I ROZWÓJ

- gromadzenie informacji na temat podatności, cyberzagrożeń oraz incydentów związanych z ICT
- programy szkoleniowe dla personelu
- monitoring zmian technologicznych

## KOMUNIKACJA

- plany działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej
- polityka komunikacyjna dla pracowników i interesariuszy zewnętrznych

DZP

# DORA

## Klasyfikacja i zgłaszanie incydentów ICT

- wprowadzenie wskaźników wczesnego ostrzegania
- procedury identyfikowania, śledzenia, rejestrowania, kategoryzowania i klasyfikowania incydentów związanych z ICT według ich priorytetu i dotkliwości oraz krytyczności usług
- przydzielenie ról i obowiązków, które należy wprowadzić w przypadku różnych rodzajów incydentów
- plany działań informacyjnych skierowanych do pracowników, interesariuszy zewnętrznych i mediów
- procedury reagowania na incydenty związane z ICT
- zgłaszanie poważnych incydentów związanych z ICT nadzorowi
  (wstępne powiadomienie, sprawozdanie śródokresowe, sprawozdanie końcowe)

# DORA

## Testowanie operacyjnej odporności cyfrowej

- kompleksowy program testowania operacyjnej odporności cyfrowej stanowiący integralną część ram zarządzania ryzykiem związanym z ICT
- podejście oparte na analizie ryzyka
- testy były przeprowadzane przez niezależne strony wewnętrzne lub zewnętrzne
- co najmniej raz w roku, przeprowadzenie odpowiednich testów wszystkich systemów i aplikacji ICT wspierających krytyczne lub istotne funkcje

# DORA

## Zaawansowane testowanie z wykorzystaniem TLPT

- obejmuje kilka krytycznych lub istotnych funkcji lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje
- podmioty finansowe oceniają, które krytyczne lub istotne funkcje należy objąć TLPT
- częstotliwość: co do zasady trzy lata, ale KNF może zmniejszyć lub zwiększyć częstotliwość
- właściwy organ może nakazać obowiązkowe testowanie TLPT uwzględniające wskazane elementy
- testerzy wewnętrzni i zewnętrzni, spełniający określone warunki

# DORA | Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT

**Ogólne zasady:**

- strategia dotyczącą ryzyka ze strony zewnętrznych dostawców usług ICT i jej regularny przegląd
- polityka korzystania z usług ICT wspierających krytyczne lub istotne funkcje
- rejestr informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT, z rozróżnieniem na ustalenia wspierające funkcje krytyczne lub istotne, oraz ustalenia, które takich funkcji nie wspierają
- obowiązki przed zawarciem umowy

**Kluczowe obowiązki:**

- strategia wyjścia w odniesieniu do usług ICT wspierających krytyczne lub istotne funkcje
- zapewnienie adekwatnych ustaleń umownych dotyczących korzystania z usług ICT
- ocena ryzyka koncentracji w obszarze ICT

**Postanowienia umowne:**

- gwarantowany poziom usług
- możliwość wypowiedzenia umowy
- ochrona danych, w tym danych osobowych
- prawo dostępu, kontroli i audytu
- współpraca dostawcy z organami (m.in. KNF, BFG)

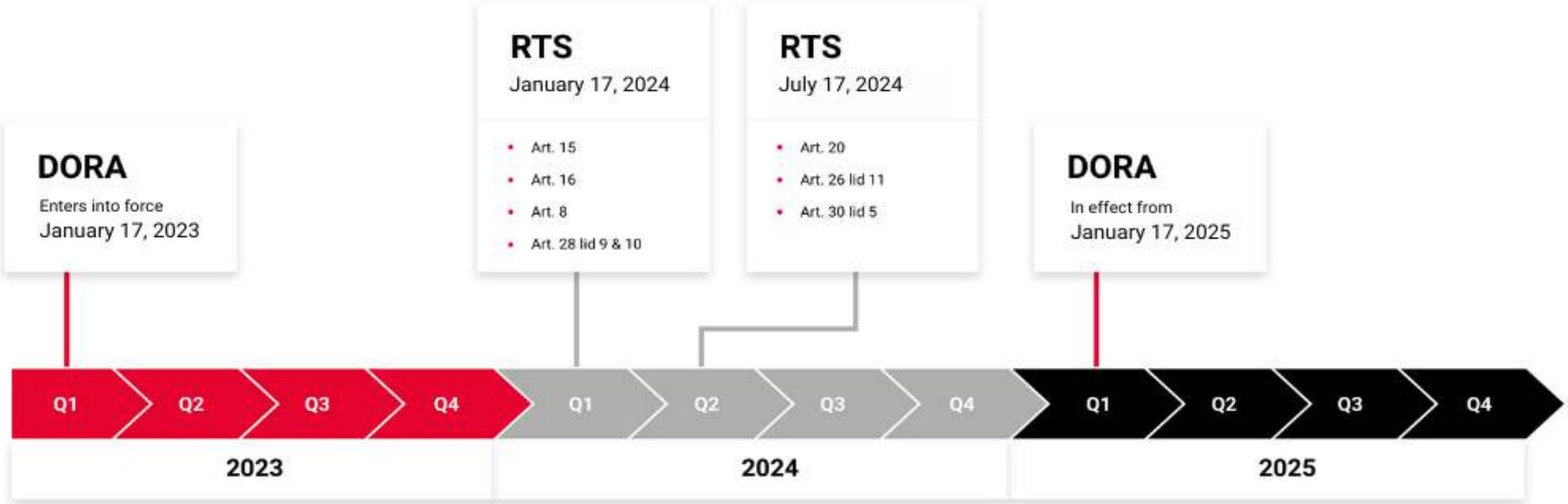
# DORA

## Ustalenia dotyczące wymiany informacji

Możliwa wymiana pomiędzy podmiotami:

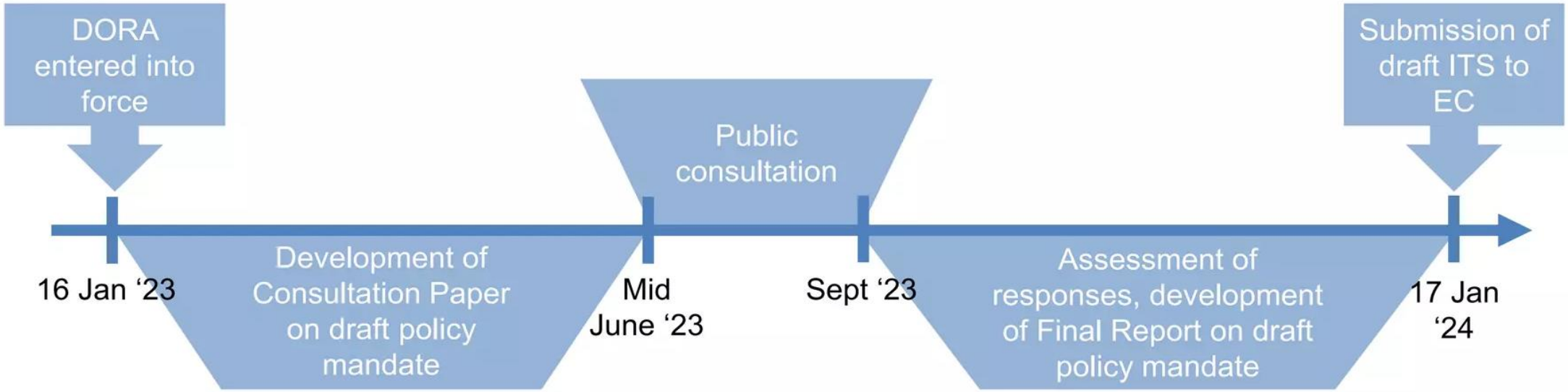
- ma na celu zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych, w szczególności poprzez zwiększanie świadomości w odniesieniu do cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się zdolności do stwarzania cyberzagrożeń
- chroniony jest poufny charakter wymienianych informacji, zgodnie regulacjami dot. zasad prowadzenia działalności, w szczególności w zakresie tajemnicy przedsiębiorstwa, ochrony danych osobowych i innych informacji chronionych

# DORA | RTS-y

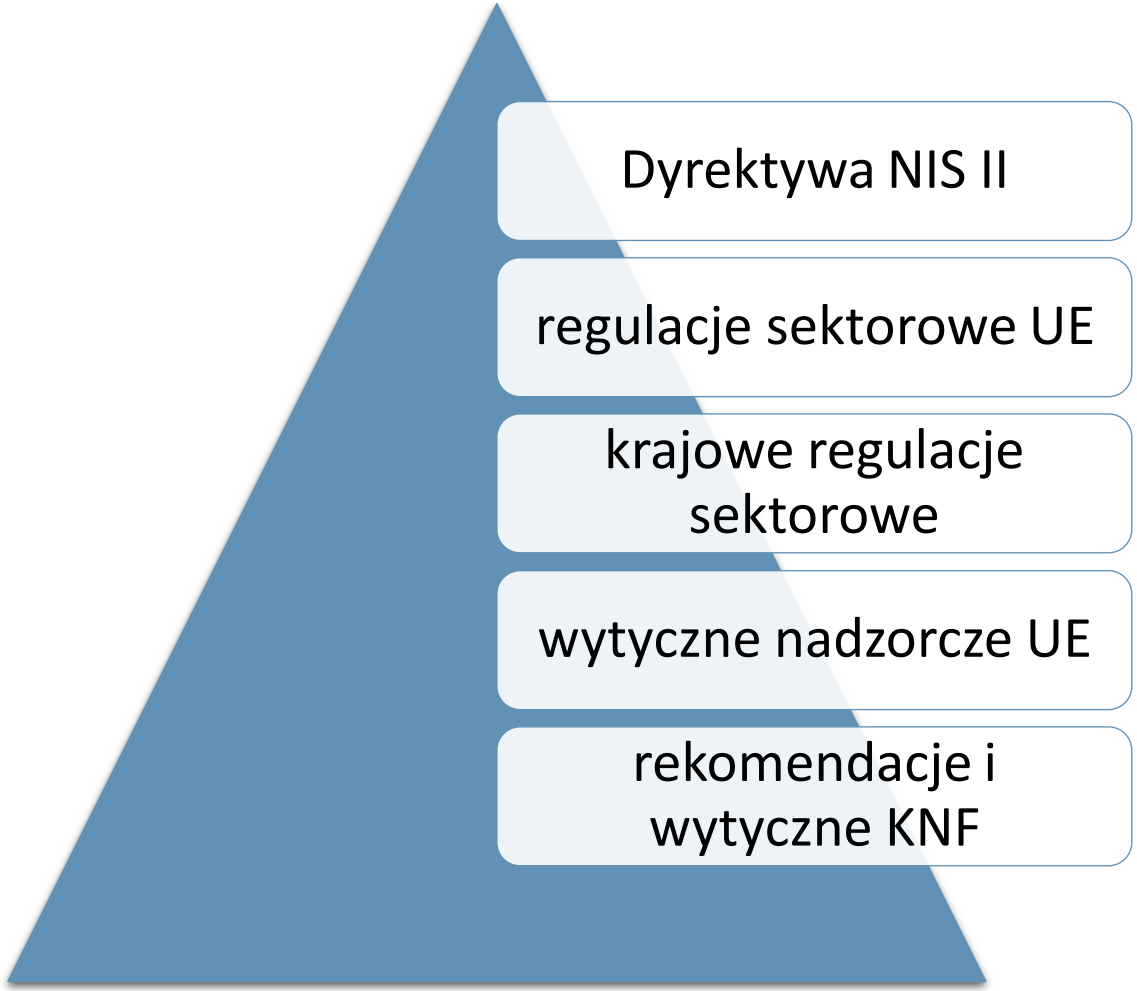

DORA
Enters into force
January 17, 2023
RTS
January 17, 2024
Art. 15
Art. 16
Art. 8
Art. 28 lid 9 & 10
RTS
July 17, 2024
Art. 20
Art. 26 lid 11
Art. 30 lid 5
DORA
In effect from
January 17, 2025
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
2023
2024
2025

# DORA | RTS-y

## Preliminary Timeline for RTSs on RMF and ICT Policy (12 months deadline)



# DORA a regulacje szczególne



# DORA | Wdrożenie

## FAZA I - AUDYT

- analiza dokumentacji i procedur
- opracowanie szczegółowego planu fazy wdrożenia

## FAZA II - IMPLEMENTACJA

- dostosowanie dokumentacji i procedur
- przeprowadzenie klasyfikacji informacji, systemów i procesów biznesowych - przegląd i aktualizacja
- opracowanie procedury testowania operacyjnej odporności cyfrowej
- opracowanie struktury organizacyjnej dostosowanej do wielkości operacji i bezpieczeństwa IT oraz złożoności infrastruktury teleinformatycznej
- przygotowanie opisu zadań na poszczególnych stanowiskach w obszarze zarządzania ryzykiem IT i bezpieczeństwa IT
- przygotowanie opisu procesów w obszarze zarządzania ryzykiem i bezpieczeństwa IT

## FAZA III – UTRZYMANIE I MONITORING

- bieżąca weryfikacja wdrożenia
- zapewnienie zgodności działania z rozporządzeniem DORA

DZP

# DORA | Dlaczego jest tak istotna?

Motyw 12:

*„(…)Przepisy dotyczące ryzyka operacyjnego, jeżeli zostały szerzej rozwinięte w unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do zwalczania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie ukierunkowanym przepisom jakościowym dotyczącym zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania sprawności i odbudowy w odniesieniu do incydentów związanych z ICT lub zdolności w zakresie sprawozdawczości i testowania cyfrowego. (…)”*

DZP

# Dziękuję za uwagę. Zapraszam

**Paweł Rudolf**
**Counsel**

# Jak nas znaleźć w sieci?

Nasze profile w social mediach.

**www.dzp.pl**

**Blogi DZP**: Life Sciences, IP, Prawo pracy, Podatki, Compliance

**LinkedIn**: DZP LinkedIn Profile

**Facebook**: DZP Life Sciences Law Blog

**Youtube**: DZP more than law

DZP


**Biuro w Warszawie**
Rondo ONZ 1
00-124 Warszawa
T + 48 22 557 76 00
F + 48 22 557 76 01

**Biuro w Poznaniu**
ul. Paderewskiego 8
61-770 Poznań
T + 48 61 642 49 00
F + 48 61 642 49 50

**Biuro we Wrocławiu**
ul. Św. Mikołaja 7
50-125 Wrocław
T + 48 71 712 47 00
F + 48 71 712 47 50