ROZPORZĄDZENIE DORA

GŁÓWNE ZAŁOŻENIA I WPŁYW NA DZIAŁALNOŚĆ PODMIOTÓW FINANSOWYCH

Październik 2024 r.

SPCG

KANCELARIA
ADWOKATÓW
I RADCÓW
PRAWNYCH

Szanowni Państwo,

od dnia 16 stycznia 2023 r. obowiązuje w UE rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (ang. *Digital Operations Resilience Act*; „Rozporządzenie DORA"), a obowiązek jego stosowania rozpocznie się z dniem **17 stycznia 2025 r., a więc już niedługo**.

Akt ten jest jednym z elementów unijnego pakietu legislacyjnego dotyczącego finansów cyfrowych, którego celem jest aktualizacja otoczenia regulacyjnego w obszarze technologii finansowych, a także zharmonizowanie procesów i standardów odporności cyfrowej w całym sektorze finansowym.

W niniejszym opracowaniu przedstawiam podstawowe informacje związane z Rozporządzeniem DORA w kontekście niezbędnych procesów dostosowawczych oraz obszary wsparcia, jakiego w tym zakresie udzielić może Państwu nasz zespół prawny. Chętnie rozwinę ten temat podczas spotkania lub w drodze konsultacji, do czego niniejszym Państwa zapraszam.

Z wyrazami szacunku,

Ewa Mazurkiewicz
Partner

CEL	Celem Rozporządzenia DORA jest ustanowienie jednolitych wymogów dotyczących bezpieczeństwa informatycznego sektora finansowego na rynku UE oraz kluczowych dostawców technologii informacyjno-telekomunikacyjnych („ICT”). Rozporządzenie DORA jest częścią pakietu unijnych aktów prawnych dla sektora finansowego, na który składają się: 1) rozporządzenia w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych w oparciu o technologię rozproszonego rejestru; 2) rozporządzenie o rynkach kryptoaktywów (MiCA); 3) rozporządzenie DORA.
KOGO DOTYCZY?	Rozporządzenie będzie miało zastosowanie do podmiotów finansowych wymienionych w art. 2 Rozporządzenia DORA, w szczególności do: (i) instytucji sektora finansowego: organizatorów obrotu, centralnych depozytów i CCP, instytucji kredytowych, firm inwestycyjnych, spółek zarządzających, a więc towarzystw funduszy inwestycyjnych i ZASI działających na podstawie zezwolenia, zakładów ubezpieczeń i reasekuracji, (ii) podmiotów z obszaru cyfrowych finansów: dostawców usług w zakresie kryptoaktywów, instytucji płatniczych i instytucji pieniądza elektronicznego, (iii) dostawców technologii, w tym dostawców usług chmury obliczeniowej i innych dostawców usług ICT. Należy podkreślić, że nie wszystkie podmioty finansowe będą objęte tymi samymi obowiązkami w tym samym stopniu (obowiązki nałożone na poszczególne podmioty różnią się w zależności od rozmiaru, zakresu działalności i profilu ryzyka podmiotu finansowego).
OD KIEDY?	Rozporządzenie DORA weszło w życie w dniu 16 stycznia 2023 r., a jego **przepisy będą miały zastosowanie od dnia 17 stycznia 2025 r.**

GŁÓWNE ZAŁOŻENIA

Rozporządzenie DORA opiera się na **pięciu filarach**. W ramach każdego z filarów DORA nakłada na podmioty finansowe różne obowiązki w zakresie odporności cyfrowej. Zakres obowiązków nałożonych na dany podmiot jest pochodną **zasady proporcjonalności**, tzn. obowiązki różnią się w zależności od rozmiaru, profilu działalności oraz profilu ryzyka podmiotu finansowego.

Wspomniane powyżej filary obejmują:

1) **zarządzanie ryzykiem związanym z ICT (art. 5-14 Rozporządzenia DORA)**: Rozporządzenie DORA wprowadzi m.in. obowiązek utworzenia i utrzymania odpornych systemów i narzędzi ICT, środków ochrony i zapobiegania ryzykom, opracowania polityk bezpieczeństwa informacji, monitorowania incydentów ICT, wprowadzenia strategii ciągłości działania oraz planów przywrócenia gotowości do pracy, a także obowiązek identyfikowania, klasyfikowania i prowadzenia dokumentacji funkcji biznesowych związanych z ICT. Dodatkowo, instytucje finansowe są zobowiązane do zapewnienia obowiązkowych szkoleń dla personelu;

2) **zgłaszanie incydentów związanych z ICT (art. 17-23 Rozporządzenie DORA)**: adresaci omawianego aktu będą zobowiązani do ustanowienia oraz wdrożenia procesu zarządzania incydentami związanymi z ICT, klasyfikowania ich i zgłaszania do odpowiednich organów nadzorów (Rozporządzenie DORA reguluje proces zarządzania incydentami ICT, w tym klasyfikację zdarzeń według priorytetu i dotkliwości oraz krytyczności usług, na które incydenty mają wpływ). Co ważne, ujednoliceniu ulegną procedury zgłaszania incydentów ICT w związku z różnymi procedurami określonymi w dyrektywie NIS czy PSD2;

3) **testowanie operacyjnej odporności cyfrowej (art. 24-27 Rozporządzenia DORA)**: Rozporządzenie DORA zobowiąże poszczególne podmioty m.in. do przeprowadzania okresowych testów odporności cyfrowej, przygotowania i dokonywania przeglądów programu testowania odporności cyfrowej. Program testowania powinien obejmować różne aspekty, takie, jak analiza *open source*, ocena bezpieczeństwa sieci i testowanie scenariuszy. Rozporządzenie DORA określi również wymogi dla testerów oraz zasady uznawania wyników testów penetracyjnych (TLPT) w przypadku podmiotów działających w kilku państwach UE. Co istotne, testy penetracyjne będą przeprowadzane na działających systemach produkcyjnych wspierających krytyczne lub istotne funkcje danego podmiotu;

GŁÓWNE ZAŁOŻENIA **cd.**	**4)** **zarządzanie ryzykiem ze strony zewnętrznych dostawców ICT (art. 28-39 Rozporządzenia DORA)**: Rozporządzenie DORA wprowadza obowiązek monitorowania ryzyka ze strony zewnętrznych dostawców ICT, w tym na etapie wykonywania umowy i zakończenia współpracy (m.in.: wprowadzenie strategii, dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT, polityki korzystania z usług ICT wspierających krytyczne lub istotne funkcje, dokonywanie przeglądów strategii oraz ryzyk zidentyfikowanych w odniesieniu do ustaleń umownych dot. korzystania z usług ICT wspierających krytyczne lub istotne funkcje) oraz ustanawia minimalne wymogi dla umów z zewnętrznymi dostawcami ICT (szerzej poniżej). Ponadto Rozporządzenie DORA wprowadza nadzór właściwych organów nad kluczowymi zewnętrznymi dostawcami ICT (wybranymi zgodnie z art. 31 Rozporządzenia DORA); **5)** **wymiana informacji (art. 45 Rozporządzenia DORA)**: Rozporządzenie DORA wprowadza regulacje w zakresie wymiany informacji zarówno pomiędzy samymi podmiotami, jak i w relacji z właściwymi organami. Rozporządzenie DORA umożliwia zwłaszcza podmiotom wymianę informacji o cyberzagrożeniu i wyniki analiz takiego cyberzagrożenia.
ROLA ZARZĄDU	Głównym założeniem Rozporządzenia DORA jest **pełna odpowiedzialność organu zarządzającego** (tj. zarządów spółek) za określenie, zatwierdzenie oraz nadzorowanie wdrożenia ram zarządzania ryzykiem związanym z ICT (art. 5 ust. 2 Rozporządzenia DORA). W motywie 45 podkreśla się m.in. konieczność ciągłego angażowania organu zarządzającego w kierowanie i dostosowywanie ram zarządzania ryzykiem związanym z ICT. Przykładowo, zgodnie z art. 5 ust. 4 Rozporządzenia DORA członkowie zarządu powinni regularnie odbywać szkolenia w celu zdobycia i aktualizacji wiedzy oraz umiejętności wystarczających do zrozumienia i oceny ryzyka związanego z ICT, a także jego wpływu na operacje danego podmiotu.

UMOWY Z DOSTAWCAMI ICT

Rozporządzenie DORA określa **minimalne postanowienia umowne**, które powinny zostać uwzględnione w umowie z dostawcą ICT (art. 30 Rozporządzenia DORA):

- jasny i kompletny opis wszystkich funkcji i usług ICT;
- postanowienia dotyczące podwykonawstwa tzw. kluczowej lub ważnej funkcji lub jej istotnych części, w tym – jeżeli podwykonawstwo jest dozwolone – warunki jakie mają zastosowanie do podwykonawstwa;
- wskazanie lokalizacji, w których będą świadczone funkcje i usługi ICT i w których będą przetwarzane dane;
- postanowienia dotyczące dostępności, autentyczności, integralności i poufności w związku z ochroną danych, w tym danych osobowych oraz zwrotu danych osobowych i nieosobowych na wypadek zakończenia współpracy;
- opisy gwarantowanych poziomów usług, w tym ich aktualizacje i zmiany;
- zapewnienie podmiotowi finansowemu przez dostawcę ICT pomocy w przypadku wystąpienia incydentu związanego z ICT (bez dodatkowych opłat lub w ramach opłaty uiszczonej z góry);
- obowiązek zewnętrznego dostawcy usług ICT do pełnej współpracy z właściwymi organami oraz organami przymusowej restrukturyzacji podmiotu finansowego, w tym z osobami przez nie wyznaczonymi;
- prawo wypowiedzenia umowy z dostawcą ICT, w tym odpowiednio długie okresy wypowiedzenia umowy przez dostawcę ICT;
- obowiązki sprawozdawcze dostawcy ICT wobec podmiotu finansowego;
- prawo dostępu, kontroli i audytu dostawcy ICT przez podmiot finansowy lub wyznaczoną osobę trzecią;
- strategie wyjścia (tj. *exit plan*).

KONSEKWENCJE NARUSZENIA ROZPORZĄ-DZENIA DORA

Państwa członkowskie są zobowiązane do powierzenia właściwym organom uprawnienia do stosowania względem **zobowiązanych podmiotów finansowych, które naruszą przepisy Rozporządzenia DORA**, kar administracyjnych lub środków naprawczych, obejmujących m.in.:

- wydanie nakazu zaprzestania postępowania naruszającego Rozporządzenie DORA oraz powstrzymania się od ponownego podejmowania takich działań;
- wymaganie tymczasowego lub stałego zaprzestania wszelkich praktyk, które właściwy organ uważa za sprzeczne z Rozporządzeniem DORA, oraz niedopuszczenie do ponownego ich podejmowania;
- podejmowanie wszelkiego rodzaju środków, w tym o charakterze pieniężnym, mających zapewnić dalsze przestrzeganie wymogów prawnych;
- wydanie publicznych ogłoszeń, w tym podanie do wiadomości publicznej informacji wskazującej tożsamość osoby fizycznej lub prawnej oraz charakter naruszenia.

KONSEKWENCJE NARUSZENIA ROZPORZĄ-DZENIA DORA **cd.**	Z kolei w przypadku częściowego lub całkowitego **niezastosowania się przez kluczowego zewnętrznego dostawcę usług ICT do środków, które zostały podjęte przez organy nadzorcze** (np. nieprzekazanie wszystkich stosownych informacji i dokumentów, niezłożenie sprawozdań po zakończeniu działań nadzorczych) organ nadzorczy nad rynkiem finansowym może nałożyć okresową karę pieniężną do 1% średniego dziennego światowego obrotu w poprzedzającym roku obrotowym za każdy dzień trwania naruszenia. Okresowa kara pieniężną jest nakładana za każdy dzień do czasu zastosowania się do środków podjętych przez organ nadzorczy i nie dłużej niż przez 6 miesięcy od dnia zawiadomienia o decyzji nakładającej tę karę. Informacja o nałożeniu kary może zostać podana do wiadomości publicznej (art. 35 Rozporządzenia DORA).
AKTY WYKONAWCZE	Europejskie Urzędy Nadzoru (EUN), tj. Europejski Urząd Nadzoru Bankowego (EBA), Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA) oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) opublikowały dotychczas dwa pakiety aktów wykonawczych do Rozporządzenia DORA. **Pierwszy pakiet:** przyjęty przez Komisję Europejską w lutym i marcu 2024 r. doprecyzowuje regulacje Rozporządzenia DORA w zakresie: (i) ram zarządzania ryzykiem ICT oraz uproszczonych ram zarządzania ryzykiem ICT (art. 15, art. 16 ust. 3 Rozporządzenia DORA), doprecyzowujących m.in. elementy polityk oraz procedur wewnętrznych w zakresie zarządzania ryzykiem ICT (RTS); (ii) kryteriów klasyfikacji incydentów ICT (art. 18 ust. 3 Rozporządzenia DORA), doprecyzowujących m.in. kryteria klasyfikacji poważnych incydentów związanych z ICT, podejście do klasyfikacji poważnych incydentów oraz próg istotności każdego kryterium klasyfikacji (RTS); (iii) wzorów na potrzeby rejestru informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT (art. 28 ust. 9 Rozporządzenia DORA) (ITS) oraz polityki dotyczącej usług ICT wspierających krytyczne lub istotne funkcje, świadczonych przez zewnętrznych dostawców usług ICT (art. 28 ust. 10 Rozporządzenia DORA) (RTS).

AKTY WYKONAWCZE **cd.**	**Drugi pakiet:** projekty RTS oraz wytyczne opublikowane w dniu 17 lipca 2024 r., doprecyzowują regulacje Rozporządzenia DORA w zakresie: (i) przeprowadzania testów penetracyjnych (TLPT) (RTS); (ii) raportowania incydentów ICT (RTS); (iii) harmonizacji warunków umożliwiających prowadzenie działań nadzorczych (RTS); (iv) wykonywania nadzoru przez właściwe organy nadzoru (RTS); (v) szacowania kosztów i strat spowodowanych incydentami (wytyczne); (vi) współpracy w zakresie nadzoru i wymiany informacji między EUN a właściwymi organami (wytyczne). Projekty RTS oraz wytycznych z drugiego pakietu zostały już przyjęte przez EUN i przekazane Komisji Europejskiej w celu dalszych prac. Ponadto, w dniu 18 kwietnia 2024 r. na stronie Rządowego Centrum Legislacji zamieszczono projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego wdrażający do prawa krajowego oraz zapewniający stosowanie Rozporządzenia DORA oraz towarzyszącej mu dyrektywy 2022/2556. **Zgodnie z założeniami projektowana ustawa ma wejść w życie w dniu 17 stycznia 2025 r., czyli w terminie, od którego stosuje się przepisy Rozporządzenia DORA.** Projekt przewiduje m.in. wyznaczenie KNF jako organu nadzoru właściwego w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego. Zgodnie z projektowanymi regulacjami **KNF będzie mogła w drodze decyzji nakazać zaprzestanie danego zachowania oraz powstrzymanie się od takiego zachowania w przyszłości, zakazać pełnienia funkcji członka zarządu lub rady nadzorczej albo innej funkcji kierowniczej tego podmiotu** przez okres nie krótszy niż miesiąc i nie dłuższy niż rok, a także **nałożyć karę pieniężną** do wysokości 20,869,500 zł lub 10% rocznego przychodu (w przypadku osoby prawnej) i karę pieniężną do wysokości 3,042,410 zł (w przypadku osoby fizycznej). KNF będzie mogła również wydać publiczne oświadczenie, w którym wskaże imię i nazwisko osoby fizycznej albo firmę lub nazwę osoby prawnej, odpowiedzialnych za dane naruszenie wraz ze wskazaniem jego charakteru.
PRZEPISY ODRĘBNE	Ponieważ Rozporządzenie DORA reguluje powierzanie podmiotom trzecim wykonywania czynności z zakresu szeroko pojmowanych technologii informatycznych (IT) przez podmioty prowadzące działalność regulowaną, należy pamiętać o konieczności dalszego stosowania zarówno obowiązujących w danym zakresie wymogów sektorowych dla danej branży (outsourcing), gdyż Rozporządzenie DORA tych wymogów nie uchyla. Co więcej, dodatkowym obszarem, na który należy zwrócić uwagę wdrażając Rozporządzenie DORA, są wymogi tzw. trzeciego poziomu, a więc wytyczne i stanowiska wydawane przez właściwe organy na podstawie przepisów sektorowych (tu w szczególności wskazujemy na Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej).

WSPARCIE SPCG

W związku z nadchodzącym terminem rozpoczęcia stosowania Rozporządzenia DORA **oferujemy**:

1) weryfikację dotychczas zawartych umów pod kątem ustalenia zakresu umów, do których zastosowanie znajdują przepisy Rozporządzenia DORA;
2) audyt prawny w zakresie zgodności z Rozporządzeniem DORA umów z dostawcami ICT np. umów wdrożeniowych, utrzymaniowych, rozwojowych, licencyjnych, body leasingowych, czy umów na przeprowadzenie testów penetracyjnych, z uwzględnieniem właściwych przepisów odrębnych;
3) audyt prawny w zakresie zgodności z Rozporządzeniem DORA procedur i dokumentów wewnętrznych, w tym procedur zarządzania ryzykiem ICT, incydentów ICT czy testowania odporności operacyjnej, z uwzględnieniem właściwych przepisów odrębnych;
4) dostosowanie – w ramach zaleceń poaudytowych – zawartych umów z dostawcami ICT oraz procedur wewnętrznych do wymogów Rozporządzenia DORA, z uwzględnieniem właściwych przepisów odrębnych;
5) przygotowanie wzorów umów z dostawcami ICT zgodnych wymogami Rozporządzenia DORA, z uwzględnieniem właściwych przepisów odrębnych;
6) negocjowanie umów z dostawcami usług ICT;
7) stałe doradztwo w regulacyjnych aspektach cyberbezpieczeństwa, w tym w szczególności w zakresie wypełniania obowiązków wynikających z Rozporządzenia DORA;
8) wsparcie w wypełnianiu obowiązków raportowych i sprawozdawczych np. sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT;
9) reprezentację przed organami nadzoru i sądami administracyjnymi w postępowaniach dotyczących wykonania obowiązków określonych w Rozporządzeniu DORA;
10) szkolenia i warsztaty przygotowujące podmiot do rozpoczęcia stosowania Rozporządzenia DORA/ułatwiające wdrożenie nowych rozwiązań w organizacji.

Ewa Mazurkiewicz
radca prawny
Partner

e.mazurkiewicz@spcg.pl

ul. Złota 59, bud. Skylight
00-120 Warszawa

tel.: +48 22 244 83 00
m.: +48 604 949 854

Więcej informacji o kancelarii: https://spcg.pl/

Opinie i analizy prawne w różnych dziedzinach prawa: https://spcgblog.pl/

Śledź nas na LinkedIn: https://www.linkedin.com/company/spcg-law-firm/

Siedziba Kancelarii:
ul. Jabłonowskich 8
31-114 Kraków
tel.: +48 12 427 24 24
faks: +48 12 427 23 33
e-mail: spcg@spcg.pl

Oddział w Warszawie:
ul. Złota 59, bud. Skylight
00-120 Warszawa
tel.: +48 22 244 83 00
faks: +48 22 244 83 01
e-mail: warszawa@spcg.pl

Oddział w Katowicach:
ul. Warszawska 10
40-006 Katowice
tel.: +48 32 352 19 60
faks: +48 32 621 90 01
e-mail: katowice@spcg.pl

Oddział we Wrocławiu:
ul. św. Mikołaja 7
50-125 Wrocław
tel.: +48 71 739 55 00
faks: +48 71 739 55 01
e-mail: wroclaw@spcg.pl

SPCG
KANCELARIA ADWOKATÓW I RADCÓW PRAWNYCH