ROZPORZĄDZENIE DORA

GŁÓWNE ZAŁOŻENIA I WPŁYW NA DZIAŁALNOŚĆ PODMIOTÓW FINANSOWYCH

Lipiec 2022 r.

SPCG

KANCELARIA
ADWOKATÓW
I RADCÓW
PRAWNYCH

CEL	Celem rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (ang. *The Digital Operational Resilience Act,* „DORA") jest ustanowienie jednolitych wymogów dotyczących bezpieczeństwa informatycznego sektora finansowego na rynku UE oraz kluczowych dostawców usług ICT. Rozporządzenie DORA jest częścią pakietu unijnych aktów prawnych dla sektora finansowego, na który składają się: 1) rozporządzenie o rynkach kryptoaktywów (MiCA); 2) rozporządzenia w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych w oparciu o technologię rozproszonego rejestru; 3) rozporządzenie DORA. O ww. rozporządzeniach piszemy na naszym blogu: https://spcgblog.pl/spcg-for-fintech/spcg-for-fintech-cz-7-nowe-unijne-regulacje-dla-sektora-finansowego
KOGO DOTYCZY?	Rozporządzenie będzie miało zastosowanie do podmiotów finansowych wymienionych w art. 2 DORA, w szczególności do banków, firm inwestycyjnych, instytucji płatniczych, towarzystw funduszy inwestycyjnych, dostawców usług w zakresie kryptoaktywów, zakładów ubezpieczeń i reasekuracji, dostawców usług finansowania społecznościowego.
OD KIEDY?	Podmioty finansowe będą zobowiązane do stosowania DORA najpewniej już w 2023 roku. Zgodnie z art. 56 ust. 2 p termin rozpoczęcia stosowania DORA to 12 miesięcy od dnia wejścia DORA w życie. Prezydencja Rady UE i Parlament Europejski osiągnęły już wstępne porozumienie dotyczące treści DORA, co oznacza, że do formalnego wejścia w życie potrzebne jest jeszcze zatwierdzenie projektu przez Radę UE oraz Parlament.
ROLA ZARZĄDU	Głównym założeniem DORA jest **pełna odpowiedzialność organu zarządzającego** (tj. zarządów spółek) za określenie, zatwierdzenie, nadzorowanie wdrożenia ram zarządzania ryzykiem związanym z ICT (art. 4 ust. 2 DORA).

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 finansowy jest **pochodną zasady proporcjonalności**, tzn. obowiązki różnią się one w zależności od rozmiaru, profilu działalności oraz profilu ryzyka podmiotu finansowego.

Na wspomniane pięć filarów składają się:

1) **Zarządzanie ryzykiem związanym ICT (art. 5-14 DORA).** Podmioty finansowe mają m.in. obowiązek utworzenia i utrzymania odpornych systemów i narzędzi ICT, środków ochrony i zapobiegania ryzykom, monitorowania incydentów ICT, wprowadzenia strategii ciągłości działania oraz planów przywrócenia gotowości do pracy.

2) **Zgłaszanie incydentów związanych z ICT (art. 15-20 DORA).** Podmioty finansowe są zobowiązane do ustanowienia oraz wdrożenia procesu zarządzania incydentami związanymi z ICT, klasyfikowania ich i zgłaszania do odpowiednich organów nadzorów (co ważne, ujednolicono procedury zgłaszania incydentów ICT w związku z różnymi procedurami określonymi w dyrektywie NIS czy PSD2).

3) **Testowanie operacyjnej odporności cyfrowej (art. 21-24 DORA).** DORA zobowiązuje podmioty finansowe m.in. do przeprowadzania okresowych testów odporności cyfrowej, przygotowania i dokonywania przeglądów programu testowania odporności cyfrowej. DORA określa również wymogi dla testerów oraz zasady uznawania wyników testów penetracyjnych w przypadku podmiotów finansowych działających w kilku państwach UE.

4) **Ryzyko ze strony zewnętrznych dostawców ICT (art. 25-39 DORA).** DORA wprowadza obowiązek monitorowania ryzyka ze strony zewnętrznych dostawców ICT, w tym na etapie wykonywania umowy i zakończenia współpracy oraz ustanawia minimalne wymogi dla umów z zewnętrznymi dostawcami ICT (szerzej poniżej). Ponadto DORA obejmuje nadzorem właściwych organów także kluczowych zewnętrznych dostawców ICT (wybranych zgodnie z art. 28 DORA).

5) **Wymiana informacji (art. 40 DORA).** DORA umożliwia podmiotom finansowym zawieranie umów współpracy dotyczących wymiany informacji oraz danych związanych z cyberzagrożeniami.

UMOWY Z DOSTAWCAMI ICT

DORA określa **minimalne postanowienia umowne**, które powinny zostać uwzględnione w umowie z dostawcą ICT (art. 27 DORA):

a) pełny opis usług ICT;

b) postanowienia dotyczące podwykonawstwa tzw. kluczowej lub ważnej funkcji lub jej istotnych części, w tym – jeżeli podwykonawstwo jest dozwolone – warunki jakie mają zastosowanie do podwykonawstwa;

c) wskazanie lokalizacji, w których będą świadczone usługi i w których będą przetwarzane dane;

d) zapewnienie dostępu, dostępności, integralności, bezpieczeństwa i ochrony danych osobowych przez dostawcę ICT oraz zwrotu danych osobowych i nieosobowych na wypadek zakończenia współpracy;

e) pełny opis poziomu świadczenia usług;

f) prawo wypowiedzenia umowy z dostawcą ICT, w tym odpowiednio długie okresy wypowiedzenia umowy przez dostawcę ICT;

g) obowiązki sprawozdawcze dostawcy ICT wobec podmiotu finansowego;

h) zapewnienie podmiotowi finansowego przez dostawcę ICT pomocy w przypadku wystąpienia incydentu związanego z ICT (bez dodatkowych opłat lub w ramach opłaty uiszczonej z góry);

i) prawo dostępu, kontroli i audytu dostawcy ICT przez podmiot finansowy lub wyznaczoną osobę trzecią;

j) strategie wyjścia (tj. *exit plan*).

USŁUGI SPCG

W związku z nadchodzącym rozpoczęciem stosowania DORA oferujemy:

- audyt prawny umów IT (np. umów wdrożeniowych, utrzymaniowych, rozwojowych, licencyjnych, body leasingowych) oraz polityk wewnętrznych pod kątem zgodności z DORA;
- dostosowanie – w ramach zaleceń poaudytowych – zawartych umów IT oraz polityk wewnętrznych do wymogów DORA;
- przygotowanie wzorów umów IT zgodnych wymogami DORA;
- szkolenia przygotowujące do wdrożenia DORA w działalności podmiotów finansowych.

Artur Zapała
radca prawny
Partner

Kieruje pracami warszawskiego oddziału SPCG. Doświadczenie zdobywał w pracy zarówno w administracji państwowej (Komisja Papierów Wartościowych i Giełd, poprzednik KNF) jak i w międzynarodowej kancelarii prawnej.

Specjalizuje się w prawie papierów wartościowych, obsłudze firm inwestycyjnych, towarzystw funduszy inwestycyjnych, banków, zakładów ubezpieczeń i innych instytucji finansowych. Posiada doświadczenie w transakcjach typu M&A, sekurytyzacji i nabywaniu portfeli wierzytelności.

Wielokrotnie reprezentował klientów w procesach dotyczących nabywania akcji instytucji finansowych, postępowaniach administracyjnych przed KNF, przygotowywaniu i przeprowadzaniu publicznych ofert papierów wartościowych i innych transakcji na rynku kapitałowym, w tym wezwań do zapisywania się na sprzedaż lub zamianę akcji spółki publicznej.

dr Marcin Balicki
adwokat
Senior Associate

Adwokat, zawodowy pełnomocnik przed Europejskim Urzędem ds. Własności Intelektualnej, doktor nauk prawnych ze specjalnością prawo własności intelektualnej (obrona na Wydziale Prawa i Administracji UJ), przewodniczący Sekcji Własności Intelektualnej w Instytucie Allerhanda, arbiter Sądu Polubownego ds. Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji, członek Stowarzyszenia Prawa Nowych Technologii, wykładowca na prowadzonych przez SGH studiach podyplomowych „FinTech - nowe zjawiska i technologie na rynku finansowym" oraz w Szkołach IP oraz IT organizowanych przez Centrum Praw Własności Intelektualnej im. H. Grocjusza.

Autor publikacji naukowych i popularnonaukowych z zakresu prawa autorskiego oraz prawa własności przemysłowej, w tym komentarza do Ustawy o prawie autorskim i prawach pokrewnych w zakresie dotyczących ochrony programów komputerowych (A. Michalak [red.] Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, C.H. Beck, Warszawa 2019). W 2020 roku, nakładem wydawnictwa Wolters Kluwer Polska ukazała się monografia jego autorstwa pt. „Ochrona wzorów użytkowych" – pierwsza na rynku polskim publikacja poświęcona tej tematyce.

Specjalizuje się w doradztwie z zakresu prawa własności intelektualnej oraz prawa nowych technologii, w tym negocjowaniu umów dotyczących realizacji projektów technologicznych (m.in. systemy IT, IoT, automatyzacja przemysłu), umów licencyjnych oraz prowadzeniu sporów sądowych w tym obszarze (m.in. nieprawidłowe wdrożenia oprogramowania, naruszenia praw własności intelektualnej).

Aleksandra Modzelewska

adwokat
Associate

Specjalizuje się w kompleksowej obsłudze prawnej projektów informatycznych. W swej dotychczasowej karierze wspierała zaawansowane i skomplikowane projekty IT dla największych przedsiębiorstw w Polsce działających w branży paliwowej, ubezpieczeniowej, spożywczej, handlowej, farmaceutycznej, motoryzacyjnej, biomedycznej, etc. Wspierała klientów w opracowywaniu oraz negocjowaniu umów wdrożeniowych, utrzymaniowych, rozwojowych, w tym również bazujących na technologiach Microsoft, SAP oraz innych. Obsługuje dostawców IT, w tym dostawców technologii finansowych, międzynarodowe korporacje, software house'y, integratorów i start-upy.

Posiada doświadczenie w prowadzeniu spraw spornych oraz rejestracyjnych w zakresie ochrony własności intelektualnej (znaki towarowe, wzory przemysłowe) i sporów dotyczących naruszenia tajemnicy przedsiębiorstwa.

Doświadczenie zdobywała w renomowanych warszawskich kancelariach prawnych obsługujących największe podmioty z rynku IT i nowych technologii. Absolwentka Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie (2017). Stypendystka Uniwersytetu w Antwerpii (2017). Ukończyła studia podyplomowe na kierunku „Prawo Nowoczesnych Technologii" organizowane przez Akademię Leona Koźmińskiego (2019).

Malwina Przyborowska

radca prawny
Senior Associate

Specjalizuje się w zagadnieniach związanych z prawem rynku kapitałowego, w szczególności w zakresie działalności firm inwestycyjnych oraz funduszy inwestycyjnych. Doradza prawnie w projektach dot. outsourcingu regulowanego dla instytucji finansowych.

Doświadczenie zdobywała w UKNF w obszarze nadzoru bieżącego nad firmami inwestycyjnymi, bankami prowadzącymi działalność maklerską i bankami powierniczymi, a następnie w obszarze regulacji rynku kapitałowego oraz FinTech. Brała udział w pracach grupy roboczej ds. crowdfundingu przy ESMA.

W ramach praktyki w jednej z warszawskich kancelarii prawnych reprezentowała klientów w postępowaniach administracyjnych przed KNF oraz doradzała podmiotom rynku finansowego w obszarze prawnym i regulacyjnym, m.in. w projektach dostosowania prowadzonej działalności do wymogów pakietu MiFID II. Doradzała również w obszarze regulacyjnym w zagadnieniach związanych z crowdfundingiem i tokenizacją aktywów.

Absolwentka Wydziału Prawa i Administracji Uniwersytetu Warszawskiego (2008).

Artur Zapała
radca prawny
Partner

a.zapala@spcg.pl

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

tel.: +48 22 244 83 00
m.: +48 604 949 923

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

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

Cykl artykułów analizujących przepisy oraz regulacje podmiotów sektora FinTech: https://spcgblog.pl/spcg-for-fintech/

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