# DORA

# Zmluvné dojednania s TPP

# Kapitola V, oddiel 1

## Všeobecné požiadavky (čl. 28 – 30 DORA)

## Špecificky k zmluvám podporujúcim CIF (RTS/deleg nariadenie)

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Dana Kravecová, OFI

19. jún 2024

# Požiadavky na zmluvy s TPP

- požiadavky na všetky zmluvy (bez ohľadu na CIF): čl. 28 – 30 DORA
  - všeobecné zásady
  - predbežné posúdenie rizika koncentrácie IKT na úrovni subjektu
  - kľúčové zmluvné ustanovenia

- dodatočné požiadavky na zmluvy podporujúce CIF
  - čl. 30 ods. 3 DORA
  - politika o zmluvách s TPP podporujúcimi CIF (delegované nariadenie/RTS)

# DORA

# kapitola V, oddiel 1

# Riadenie externého IKT rizika

- súčasť IKT RMF

- zásady:
  - FE je vždy plne zodpovedná za dodržiavanie všetkých povinností z DORA a ďalších predpisov v oblasti finančných služieb
  - proporcionalita
    - dôležitosť závislostí súvisiacich s IKT
    - riziká vyplývajúce zo zmlúv
- stratégia externého IKT rizika – súčasť IKT RMF
  - politika pre využívanie IKT služieb podporujúcich CIF
- riadiaci orgán FE má pravidelne preskúmavať riziká

- register informácií

# Informačné povinnosti

- register informácií (na vyžiadanie CA úplný register)

- aspoň raz ročne:
  - počet nových dojednaní o využívaní IKT služieb
  - kategórie TPP
  - druh dojednaní
  - poskytované IKT služby a funkcie

- včas: info o každom plánovanom dojednaní o IKT službách na podporu CIF

# Kroky FE vo vzťahu k zmluvám

- pred uzavretím zmluvy (čl. 28 ods. 4 a 5 DORA)
  - či sa zmluvy vzťahujú na CIF, identifikácia a posudzovanie rizík, ...
- počas trvania zmluvy (čl. 28 ods. 6 DORA)
  - právo na prístup, inšpekcie, audity
- ukončovanie zmluvy (čl. 28 ods. 7 a 8 DORA)
  - kedy je povinnosť zmluvu ukončiť
  - čo treba zabezpečiť pri ukončovaní zmluvy
  - stratégie ukončenia angažovanosti (pre CIF), plány transformácie
  - opatrenia na business continuity
- riziko koncentrácie
- subcontracting

# Kľúčové zmluvné ustanovenia – všeob.

- písomne, jeden zmluvný dokument (vrátane SLA) – papier/stiahnuteľný trvanlivý a prístupný formát

- **povinné náležitosti pre všetky zmluvy o IKT (čl. 30 ods. 2 DORA):**
  - čo má TPP poskytovať (aj či sa povoľujú subdodávatelia + podmienky)
  - kde (poskytovanie služby, spracovávanie a uchovávanie údajov)
  - ochrana údajov a osobných údajov
  - prístup k údajom (aj v prípade ukončenia zmluvy)
  - opis úrovne poskytovaných služieb (aj aktualizácie a revízie)
  - podpora od TPP pre FE bez dodatočných nákladov (alebo stanovených ex-ante) v prípade IKT incidentu
  - povinnosť TPP spolupracovať s CA a NRA/SRB (vrátane nimi určených osôb)
  - právo ukončiť zmluvný vzťah (+ podmienky, výpovedná lehota)
  - účasť TPP na zvyšovaní informovanosti FE o IT bezpečnosti a DOR

# Kľúčové zmluvné ustanovenia – CIF

- **povinné náležitosti pre zmluvy o IKT podporujúce CIF (čl. 30 ods. 3 DORA):**
  - úplny opis úrovne služieb + aktualizácie a revízie (+ presné kvantitatívne a kvalitatívne výkonnostné ciele) – aby FE mohla monitorovať IKT služby
  - výpovedné lehoty a nahlasovacie povinnosti TPP voči FE
  - požiadavky na TPP na vykonávanie a testovanie obchodných krízových plánov, zavedenie bezpečnostných opatrení, nástrojov a politík
  - povinnosť účasti TPP na TLPT testovaní FE
  - právo priebežne monitorovať výkonnosť TPP
    - neobmedzené právo na prístup, inšpekciu, audit (FE, iná strana, CA)
    - povinnosť spolupráce TPP na inšpekcii, audite – NCA, LO, FE, iná strana
  - stratégie ukončovania angažovanosti – primerané prechodné obdobie
    - počas ktorého ešte TPP bude poskytovať služby
    - ktoré umožní FE prejsť k inému TPP

# RTS / delegované nariadenie EK k politike pre zmluvy s TPP o CIF

# Účel politiky

- úprava zmluvného vzťahu medzi FE a TPP
  - aby TPP dostatočne spolupracovali s FE a bolo možné nad nimi vykonávať účinnú kontrolu (zo strany FE, CA, nezávislého auditu)

- aké všetky kroky má FE vykonať vo vzťahu k TPP
  - pred vstupom do zmluvy
  - počas trvania zmluvy
  - pri ukončovaní zmluvy

- súčasť stratégie pre externé IKT riziko – ako súčasť IKT RMF

# Celkový rizikový profil a zložitosť FE

- veľkosť, rizikový profil FE
- prvky zvyšujúce alebo znižujúce zložitosť služieb, činností, prevádzky FE, najmä:
  - typ IKT služieb odoberaný od TPP
  - umiestnenie TPP alebo jeho matky
  - kde poskytuje služby – EÚ/tretia krajina
  - povaha dát zdieľaných s TPP
  - či FE a TPP sú z rovnakej skupiny
  - či nad TPP je vykonávaný dohľad nejakej autority (EÚ/tretia krajina)
  - koľko TPP poskytuje danú službu na trhu
  - substituovateľnosť služieb TPP
  - dopad prerušení dodávky služby TPP na FE
- uplatnenie na skupinu

# Organizačné aspekty politiky

- pravidelné revidovanie
- metodika na určenie IKT služieb, ktoré podporujú CIF
- priradenie internej zodpovednosti za schvaľovanie, riadenie, kontrolu a dokumentáciu zmlúv
- či TPP má dostatočné zdroje – hoci finálna zodpovednosť FE
- jasné určenie člena senior managementu zodpovedného za monitorovanie zmlúv + jeho kooperáciu s kontrolnými funkciami FE + reporting na ŠO
- konzistentnosť zmlúv s:
  - ICT RMF
  - information security policy
  - ICT business continuity policy
  - požiadavkami na incident reporting
- explicitné požiadavky na zmluvy

# Životný cyklus zmlúv

- politika má špecifikovať požiadavky, pravidlá, zodpovednosti a procesy pre každú fázu životného cyklu zmluvy, najmä:
  - zodpovednosti riadiaceho orgánu
  - plánovanie zmlúv (posúdenie rizík, odb. starostlivosť, schvaľovací proces zmlúv alebo ich podstatných zmien)
  - zahrnutie business units, internal control units a iných útvarov do príslušných zmluvných ustanovení
  - implementácia, monitoring a management zmlúv (vrátane na subkonsol. a konsolidovanej úrovni)
  - dokumentácia a zaznamenávanie (register informácií)
  - exit stratégie a ukončovanie procesov

# Posúdenie pred vstupom do zmluvy

- definovanie business potrieb FE

- posúdenie rizík na úrovni FE, sub-konsol a konsolidovanej
- dopad poskytovania služby od TPP pre CIF na všetky riziká FE

- aspekty posudzovania TPP:
  - dostatočnosť zdrojov, business reputácia, štandardy pre informačnú bezpečnosť, riadenie rizík, interná kontrola, potrebné oprávnenia
  - schopnosť monitorovať relevantný technologický vývoj
  - zámer používať subdodávateľov
  - lokalizácia – vplyv na operačné riziko, reputačné riziko, možné reštrikčné opatrenia (embargá, sankcie)
  - súhlas s výkonom efektívnej kontroly nad TPP zo strany FE, CA, tretích strán
  - etické jednanie, dodržiavanie ľudských práv, ochrana životného prostredia

# Proces výberu budúcich TPP

- zdroje informácií pre posúdenie TPP
  - audity, nezávislé posúdenia zo strany FE (al. na jej žiadosť)
  - nezávislé audit správy vykonané na žiadosť TPP
  - správy interného auditu TPP
  - certifikácie od tretích strán
  - iné relevantné informácie dostupné pre FE alebo od TPP

- konflikt záujmov
  - identifikácia, prevencia, riadenie
  - vnútroskupinové poskytovanie služieb – zaručiť objektívne rozhodovanie

# Požiadavky na zmluvy

- FE má mať prístup k informáciám, kontrolám, auditom a vykonávať testy IKT
- na tento účel FE použije najmä:
  - svoj vlastný interný audit alebo poverenú tretiu stranu
  - certifikácie od tretích strán
  - interný audit alebo audit tretej strany vykonaný na žiadosť TPP
- FE má mať *možnosť posúdiť* relevanciu audit plánov, spôsobilosť certifikujúcej tretej strany alebo audítora

- monitorovanie TPP zo strany FE:
  - pravidelné reporty, incident reporty, service delivery reporty, reporty o business continuity measures a testovaní,
  - posudzovanie výkonnosti: KPI, key control indicators, interné a nezávislé revízie
- opatrenia v prípade nedostatkov TPP

# Povinnosti pri ukončovaní zmluvy

- zdokumentované exit plány pre každé zmluvné dojednanie + ich pravidelná revízia a testovanie
- pri zostavovaní exit plánov treba brať do úvahy:
  - nepredvídané a pretrvávajúce prerušenia služby
  - nedostatočné alebo úplne neposkytnutie služby
  - neočakávané ukončenie zmluvy

- exit plán:
  - má byť realistický, uskutočniteľný, založený na pravdepodobných scenároch a primeraných predpokladoch a
  - má mať plánovaný harmonogram kompatibilný s podmienkami ukončenia stanovenými v príslušných zmluvách

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

# Ďakujem za pozornosť.