

Riziká zabezpečenia súladu s legislatívou (Compliance risk management)



RNDr. Michal Danilák, Lewik

Vymedzenie pojmu – compliance risk

Compliance risk is exposure to legal penalties, financial forfeiture and material loss an organization faces

when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

Compliance risk management is part of the collective governance, risk management and compliance (GRC) discipline.

The three fields frequently overlap in the areas of incident management, internal auditing, operational risk assessment.

Rozsah legislatívy, s ktorou máme byť v súlade

700+ zákonov

2300+ podzákonných predpisov

6000+ nariadení vlády
slovenskej republiky

EÚ: 21000+ predpisov

- [01 Všeobecné, finančné a inštitucionálne záležitosti 1602](#)
- [02 Colná únia a voľný pohyb tovaru 1173](#)
- [03 Poľnohospodárstvo 3178](#)
- [04 Rybárstvo 625](#)
- [05 Voľný pohyb pracovníkov a sociálna politika 699](#)
- [06 Právo usadiť sa a sloboda poskytovať služby 543](#)
- [07 Dopravná politika 766](#)
- [08 Politika hospodárskej súťaže 574](#)
- [09 Zdaňovanie 202](#)

- [10 Hospodárska a menová politika a voľný pohyb kapitálu 578](#)
- [11 Vonkajšie vzťahy 4429](#)
- [12 Energetika 388](#)
- [13 Priemyselná politika a vnútorný trh 1537](#)
- [14 Regionálna politika a koordinácia štrukturálnych nástrojov 362](#)
- [15 Životné prostredie, ochrana spotrebiteľov a zdravia 2439](#)
- [16 Veda, informácie, vzdelávanie a kultúra 470](#)
- [17 Predpisy týkajúce sa podnikov 112](#)
- [18 Spoločná zahraničná a bezpečnostná politika 657](#)
- [19 Priestor slobody, bezpečnosti a spravodlivosti 812](#)
- [20 Európa občanov 34](#)

IT legislatíva s významnými dopadmi

- ❖ Nariadenie GDPR resp. zákon č. 18/2018 Z.z. o ochrane osobných údajov
- ❖ Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- ❖ Zákon č. 305/2013 Z. z. o e-Governmente
- ❖ Zákon č. 351/2011 Z. z. o elektronických komunikáciách
- ❖ Zákon č. 272/2016 Z. z. o dôveryhodných službách
- ❖ Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
- ❖ Zákon č. 177/2018 Z. z. zákon proti byrokracii
- ❖ Pripravovaný zákon o IT VS

Dopady pri nesúlade s legislatívou

- **Sankcie** (napr. 4 % celosvetového obratu alebo 20 mil. € v prípade GDPR, 300.000 € podľa zákona o kybernetickej bezpečnosti)
- **Súdne spory** s subjektami dotknutými nesúladosom (napr. pri úniku osobných údajov, kybernetickom útoku)
- **Trestnoprávna zodpovednosť** (v prípade vážneho porušenia zákona)
- **Narušenie chodu organizácie** (až po zastavenie jej činnosti)
- **Finančné straty** (napr. pri strate zákazníkov)
- **Náklady** na dodatočné opatrenia
- **Narušenie dobrého mena** (napr. medializáciou nesúladu)

Príklad vymedzenia sankcií

Úrad uloží pokutu od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 eur, prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť

- a) podľa § 17 ods. 1,
- b) podľa § 19 ods. 1 alebo ods. 6,
- c) prijať bezpečnostnú dokumentáciu podľa § 20 ods. 5,
- d) nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo odoslať neúplné hlásenie podľa § 24 ods. 5,
- e) riešiť kybernetický bezpečnostný incident na základe rozhodnutia úradu podľa § 27 ods. 3, vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5 alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6,
- f) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8,
- g) podľa § 29 ods. 1, 2 alebo ods. 4, alebo
- h) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29.

Príklad dodatočných nákladov

V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad ...

- b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,
- c) uložiť povinnosť vykonať reaktívne opatrenie,
- d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).

Možnosť súdnych sporov

Právo na náhradu škody a zodpovednosť (Článok 82, GDPR)

1. Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.
2. Každý prevádzkovateľ, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním, ktoré bolo v rozpore s týmto nariadením. Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním, len ak neboli splnené povinnosti, ktoré sa týmto nariadením ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom.
- ...
6. Návrhy na začatie súdnych konaní na účely uplatnenia práva na náhradu škody sa podávajú na súdy príslušné podľa práva členského štátu uvedeného v článku 79 ods. 2.

Možné narušenie chodu organizácie

Právomoci (Článok 58, GDPR)

2. Každý dozorný orgán má všetky tieto nápravné právomoci: ...

d) nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby svoje spracovateľské operácie zosúladil podľa potreby určeným spôsobom a v rámci určenej lehoty s ustanoveniami tohto nariadenia; ...

f) nariadiť dočasné alebo trvalé obmedzenie vrátane zákazu spracúvania;

g) nariadiť opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania podľa článkov 16, 17 a 18 a informovanie príjemcov, ktorým boli osobné údaje poskytnuté, o takýchto opatreniach v súlade s článkom 17 ods. 2 a článkom 19;

Základné otázky pri zabezpečovaní súladu

1. Aká nová legislatíva sa nás týka?
2. Odkedy je platná a účinná?
3. Aké konkrétne regulácie sa nás v danom právnom akte týkajú?
4. Čo presne sa po nás chce?
5. Aká je primeraná úroveň zabezpečenia súladu?
6. Ako zabezpečíme dané požiadavky?
7. Aké sú potrebné ľudské a finančné zdroje?
8. Kto bude za zabezpečenie súladu zodpovedný?
9. Ako si overíme, či sme skutočne v súlade?
10. Ako využijeme situáciu, že sme v súlade?

Nová legislatíva – Slov-lex

71/2018 Z. z.	Nariadenie vlády Slovenskej republiky, ktorým sa dopĺňa nariadenie vlády Slovenskej republiky č. 247/2016 Z. z., ktorým sa ustanovuje systém uplatňovania niektorých právomocí Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu.
70/2018 Z. z.	Zákon, ktorým sa mení a dopĺňa zákon Slovenskej národnej rady č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov
69/2018 Z. z.	Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
68/2018 Z. z.	Zákon, ktorým sa mení a dopĺňa zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov a ktorým sa mení zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
67/2018 Z. z.	Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovujú podrobnosti o mesačnom prerozdeľovaní preddavkov na poistné na verejné zdravotné poistenie a o ročnom prerozdeľovaní poistného na verejné zdravotné poistenie
66/2018 Z. z.	Zákon, ktorým sa mení a dopĺňa zákon č. 201/2008 Z. z. o náhradnom výživnom a o zmene a doplnení zákona č. 36/2005 Z. z. o rodine a o zmene a doplnení niektorých zákonov v znení nálezů Ústavného súdu Slovenskej republiky č. 615/2006 Z. z. v znení neskorších predpisov
65/2018 Z. z.	Zákon, ktorým sa mení a dopĺňa zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
64/2018 Z. z.	Zákon, ktorým sa mení a dopĺňa zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Nová legislatíva – Eur-lex

- **Smernica Rady (EÚ) 2018/912 z 22. júna 2018, ktorou sa mení smernica 2006/112/ES o spoločnom systéme dane z pridanej hodnoty, pokiaľ ide o povinnosť uplatňovať minimálnu štandardnú sadzbu**
ST/7166/2018/INIT

Ú. v. EÚ L 162, 27.6.2018, s. 1 – 2 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● Účinné

Celexové číslo: 32018L0912

Forma: Smernica

Autor: Rada Európskej únie

Dátum dokumentu: 22/06/2018; Dátum prijatia



- **Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ (Text s významom pre EHP)**
PE/72/2017/REV/1

Ú. v. EÚ L 156, 19.6.2018, s. 43 – 74 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● Účinné

Celexové číslo: 32018L0843

Forma: Smernica

Autor: Európsky parlament, Rada Európskej únie

Dátum dokumentu: 30/05/2018; Dátum podpisu



- **Smernica Európskeho parlamentu a Rady (EÚ) 2018/844 z 30. mája 2018, ktorou sa mení smernica 2010/31/EÚ o energetickej hospodárnosti budov a smernica 2012/27/EÚ o energetickej efektívnosti (Text s významom pre EHP)**
PE/4/2018/REV/1

Ú. v. EÚ L 156, 19.6.2018, s. 75 – 91 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● Účinné

Celexové číslo: 32018L0844

Forma: Smernica

Autor: Európsky parlament, Rada Európskej únie

Dátum dokumentu: 30/05/2018; Dátum podpisu



Zabezpečovanie súladu I. – čo je nové?

- Je určená organizačná jednotka alebo osoba zodpovedná za sledovanie legislatívy (napr. právny odbor).
- Osoba identifikuje novo pripravované, platné a účinné právne akty.
- Organizačná jednotka posúdi, či sa týkajú jej organizácie.
- Ak sa jej týkajú - posúdi, na ktoré organizačné jednotky to má dopad.
- Daným organizačným jednotkám sa pošle informácia o novinkách v právnych predpisoch.
- Organizačné jednotky informáciu vyhodnotia a potvrdia, či sa ich právne predpisy týkajú (*napr. odbor informatiky – zákon 69/2018*).
- Príslušní zamestnanci dostanú informáciu na vedomie.

Zabezpečovanie súladu II. – čo sa po nás chce?

- Zodpovedná organizačná jednotka identifikuje regulácie, ktoré sa organizácie týkajú. Posúdenie môže byť netriviálne, napr.
 - Je organizácia prevádzkovateľom základnej služby?
 - Má organizácia realizovať test proporcionality alebo DPIA?
 - Je daný IS informačným systémom verejnej správy?
- Roztriedi regulácie na 3 skupiny – povinnosti, práva a vymedzenia.
 - Povinnosti organizácie sú skryté aj v právach fyzických a iných osôb.
- Posúdi, ktorých organizačných jednotiek sa týkajú jednotlivé práva a povinnosti.
 - Práva sú zdrojom možných benefitov (napr. právo žiadať o dotácie).
 - Povinnosti sú zvyčajne brané ako záťaž. V novej paradigme bezpečnosti aj tieto povinnosti sú oportunitou voči konkurencii, ktorá má problém s ich súladom.

Zabezpečovanie súladu III. – ako na to?

- Zodpovedná organizačná jednotka posúdi, ako naplniť požiadavky danej regulácie. Môže to byť veľmi netriviálna úloha, napr.
 - Článok 5 GDPR: Osobné údaje musia byť: ... spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).
Prevádzkovateľ je zodpovedný za súlad s odsekom 1 a musí vedieť tento súlad preukázať („zodpovednosť“).
- Posúdi potrebnú úroveň zabezpečenia súladu – na základe analýzy rizík.
- Navrhne spôsob zabezpečenia súladu.
- Identifikuje potrebné ľudské, technické a finančné zdroje.
- Navrhne implementačný postup, alebo akčný plán a nechá ho schváliť.

Zabezpečovanie súladu IIIa. – posudzujeme

Otázka: aká je primeraná miera aktivít na zabezpečenie súladu?

V oblasti bezpečnosti je možné investovať ľubovoľné množstvo zdrojov.

Je čas posúdiť riziká.

Napr. podľa článku 24 GDPR:

S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na **riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb** prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.

Posúdime hrozby –zraniteľnosti, dopady a pravdepodobnosti realizácie hrozby; určíme mieru rizika. **Miera rizika výrazne závisí aj od sankcií a non-IT dopadov!**

Zabezpečovanie súladu IV. – implementujeme

- Sú naplánované potrebné ľudské, technické a finančné zdroje.
- Sú zabezpečené potrebné ľudské, technické a finančné zdroje.
- Sú jasne vymedzené legislatívne, organizačné a technické aktivity.
- Je zabezpečená potrebná súčinnosť iných organizačných jednotiek.
- Je vytvorený projektový tím a projektový plán.
- Je určený vedúci projektu alebo tím líder.
- Otvorené otázky včas konzultujeme – s autoritou (napr. ÚOOÚ, NBÚ) alebo externými subjektami.
- Priebežne informujeme vedenie o pokroku v dosiahnutí súladu.
- Priebežne plníme administratívne povinnosti voči úradom.

Zabezpečovanie súladu V. – overujeme

- Overenie účinnosti opatrení:
 - Interné
 - Interní používatelia.
 - Zákazníci.
 - Odborníci v tíme.
 - Interný audit.
 - Externé
 - Nezávislé posúdenie.
 - Testy (napr. penetračné testy).
 - Audit (často požadovaný aj autoritou).

Zabezpečovanie súladu VI. – benefity

Ak máme úspešne zabezpečený súlad, je čas to využiť:

- V rámci PR a budovania pozitívneho obrazu organizácie.
 - Interne.
 - Externe - k zákazníkom
 - Externe – k širokej verejnosti
- V marketingu – lepšia starostlivosť o klientov, ak sa ich týkajú regulácie.
- Pri plánovaní nových produktov a služieb.
- V rámci konkurenčného boja – využiť súlad ako výhodu.

Najčastejšie problémy

- Nová legislatíva unikne našej pozornosti.
- Nie všetky dôležité regulácie v právnom predpise sú identifikované.
- Nesprávne pochopenie požiadaviek v regulácii.
- Zbytočná panika vs. podceňovanie požiadaviek.
- Nepostačujúca súčinnosť vedenia.
- Nepostačujúca súčinnosť iných organizačných jednotiek.
- Nedostatok finančných aj ľudských zdrojov.
- Nesprávne ohodnotenie rizika nesúladu.
- Chybný výber technických opatrení.
- Nepochopenie zabezpečenia súladu aj ako príležitosti, nielen nákladu.

Ďakujeme za pozornosť



www.lewik.org

<https://knowww.eu/>

eFOCUS