

Špecifiká implementácie nariadenia GDPR vo veľkých organizáciách štátnej správy

Špecifiká štátnej správy z pohľadu GDPR

Mandát konať

Podľa Ústavy Slovenskej republiky

➤ Čl. 2 ...

(2) Štátne orgány môžu **konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.**

➤ Čl. 7 ...

(2) Slovenská republika môže medzinárodnou zmluvou, ktorá bola ratifikovaná a vyhlásená spôsobom ustanoveným zákonom, alebo na základe takej zmluvy preniesť výkon časti svojich práv na Európske spoločenstvá a Európsku úniu. **Právne záväzné akty Európskych spoločenstiev a Európskej únie majú prednosť pred zákonmi Slovenskej republiky.**

➤ Vznikol mandát konať platnosťou nariadenia publikáciou Nariadenia vo Vestníku EÚ + 20 – od 24.5.2016?

➤ Čo sa deje s kontinuitou mandátu po voľbách?

Aký mandát konať ale vznikol?

➤ Je účinný zákon č. 122/2013 Z. z. o ochrane osobných údajov, ktorý niečo požaduje vs. je platné nariadenie EÚ s inými požiadavkami.

➤ Ako teda má orgán štátnej správy konať?

Nejasný zdroj proaktivity

➤ Proaktívnosť sa očakáva zhora, plnia sa zadané úlohy.

➤ Otázka: kto a ako má byť proaktívny v zabezpečovaní súladu s GDPR?

➤ Kto prenesie informáciu o existencii nového nariadenia a vyplývajúcich povinností na úroveň výkonných zamestnancov (odbor informatiky, bezpečnosti)?

Komplikovanejšie rozhodovacie procesy

Potreba formálneho schvaľovania a úradných postupov, často aj na viacerých úrovniach.

Časovo náročné obstarávanie

➤ Obstarávanie pre posúdenie aktuálneho stavu a rozdielovú analýzu. Výsledky určia rámec pre analýzu rizík, prípadne posúdenie vplyvov.

➤ Obstarávanie pre analýzu rizík. Výsledky určia potrebu primeraných organizačných a technických opatrení.

➤ Obstarávanie pre jednotlivé bezpečnostné opatrenia. Na bezpečnostný HW, SW. Obstarávanie pre riešenie na plnenie informačných povinností.

➤ Zmenové konania pre existujúce IS – doplnkové bezpečnostné opatrenia.

Špecifiká veľkej organizácie štátnej správy

Veľa rôznorodých IS - desiatky

- Centrálne IS verejnej správy.
- Veľké aj menšie interné aplikácie.
- Súbory v Exceli.
- Wordovské súbory kombinované s papierom.
- Bezpečnostné aplikácie (antimalware, DRM, FW, IDS, IPS, SIEM, ...).
- Monitorovacie a prevádzkové nástroje (sieť, doména, aplikácie).

Rôznorodosť rolí

- Prevádzkovateľ so sprostredkovateľmi.
- Prevádzkovateľ s dodávateľmi, ktorí môžu byť aj sprostredkovatelia
- Spoločný prevádzkovateľ - voči niektorým centrálnym IS štátnej správy alebo podriadeným organizáciám.
- Sprostredkovateľ - voči niektorým centrálnym IS štátnej správy alebo podriadeným organizáciám.

Zložité organizačné členenie

- Viacero úrovní - sekcie, samostatné odbory, odbory, samostatné oddelenia, oddelenia.
- Desiatky organizačných jednotiek, každá so svojimi OÚ.
- Sídli vo viacerých objektoch.
- Samostatné odbory IT a bezpečnosti.
- Zložité zabezpečovanie súčinnosti.
- Podriadené organizácie (niekedy až desiatky).
 - Rozpočtové, príspevkové, š.p., a.s. s účasťou štátu, ...
- Zodpovednosť za rezort alebo jeho časť

Zastaralé IS uchovávajúce OÚ

- Potreba archivácie údajov aj desiatky rokov.
- Časť údajov je v IS pred dvadsiatich rokov na odstavenom serveri.
- Časť údajov na médiách, ktoré roky nikto nečítal.
- Ako plniť právo na informovanosť a zabudnutie u týchto IS?

Smernice a Nariadenia

Nariadenia

- Nariadenia sú právne akty, ktoré sa uplatňujú automaticky a jednotne vo všetkých krajinách EÚ hneď po nadobudnutí ich účinnosti bez toho, aby museli byť transponované do vnútroštátnych právnych predpisov.
- Sú záväzné v celom svojom rozsahu pre všetky krajiny EÚ.
- Príklad: GDPR
- Mandát konať vzniká platnosťou Nariadenia, nie až platnosťou zákona.
- V prípade GDPR od 24.5.2016
- Postačujúca legisakvačná lehota
- Poučenie: pravidelne sledovať všetky nové nariadenia
- Poznámka: Nariadenie s tak masívnymi dopadmi ešte nebolo

Smernice

- Smernice zaväzujú krajiny EÚ, aby dosiahli určitý pokrok, avšak spôsob, ako ho dosiahnuť, záväzný nie je.
- Krajiny EÚ musia prijať opatrenia a začleniť ich do svojho práva (transponovať), aby dosiahli ciele stanovené v smernici. Vnútroštátne orgány musia oznámiť tieto opatrenia Európskej komisii.
- Príklad: Smernica o bezpečnosti NIS transponovaná do Zákona o kybernetickej bezpečnosti.
- Mandát konať vzniká platnosťou zákona, ktorý je transpozíciou smernice.
- Ale:
 - Ak nie je smernica včas transponovaná, niektoré jej ustanovenia môžu mať účinnosť ako Nariadenie
 - Príklad - Zákon o kybernetickej bezpečnosti:
 - Dátum vyhlásenia: 9.3.2018
 - Účinnosť: od 1.4.2018
- Poučenie: pravidelne sledovať aj nové smernice



Spresniť vyhľadávanie

🔍 📄 ⭐ Zdieľať

Vybrali ste:

Nariadenie ✕

▼ Podľa domény

Úradný vestník (22)

Právo EÚ a súvisiace dokumenty (22)

▼ Podľa poddomény

Všetky dokumenty (22)

Všetky právne predpisy EÚ (22)

Právne predpisy (22)

▼ Podľa autora

Európska komisia (10)

Európska centrálna banka (7)

Rada Európskej únie (5)

Európsky parlament (4)

Generálne riaditeľstvo pre preklad (4)

Viac... ▼

Kritériá vyhľadávania

Najnovšie dokumenty – Právne predpisy

Požiadavka: FM_CODED = REG AND ((DTS = 3 OR 4) AND (XC >= TODAY - 14 DAYS)) ORDER BY XC DESC, Jazyk vyhľadávania: slovenčina

📄 Uložiť do Moje vyhľadávania

📡 Vytvoriť kanál v Moje kanály RSS

📄 Uložiť do Moje položky

Poradie bolo stanovené pri vyhľadávaní

☐ Výsledky 1 – 10 z 22 [Export výsledkov/Exportovať všetky](#) | [Zmeniť zobrazovanie metaúdajov](#) | [Zrušiť výber](#) 1 2 3

☐ Nariadenie Komisie (EÚ) 2018/401 zo 14. marca 2018, ktorým sa mení nariadenie (EÚ) č. 139/2014, pokiaľ ide o klasifikáciu vzletových a pristávacích dráh

C/2018/1487

Ú. v. EÚ L 72, 15.3.2018, s. 17 – 19 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Priamy prístup k textu: 📄 📡

Celexové číslo: 32018R0401

Forma: Nariadenie

Autor: Európska komisia, Generálne riaditeľstvo pre mobilitu a dopravu

Dátum dokumentu: 14/03/2018

☐ Nariadenie Komisie (EÚ) 2018/400 zo 14. marca 2018, ktorým sa mení nariadenie (ES) č. 1126/2008, ktorým sa v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 1606/2002 prijímajú určité medzinárodné účtovné štandardy, pokiaľ ide o medzinárodný účtovný štandard (IAS) 40 (Text s významom pre EHP)

C/2018/1405

Ú. v. EÚ L 72, 15.3.2018, s. 13 – 16 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Priamy prístup k textu: 📄 📡

Celexové číslo: 32018R0400

Forma: Nariadenie

Autor: Európska komisia, Generálne riaditeľstvo pre finančnú stabilitu, finančné služby a úniu kapitálových trhov

Dátum dokumentu: 14/03/2018

Môj EUR-Lex

🔒 Prihlásiť sa

alebo [Registrácia](#)

• Moje nedávne vyhľadávania (0)

📡 Preddefinované RSS kanály

🔒 Webová služba – registrácia

📺 Inštruktážne videá online

📊 Štatistiky

✉ Napíšte nám

Vzťah GDPR a zákona

Citácia z dôvodovej správy k zákonu:

„Účelom návrhu zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“) je dosiahnuť súlad vnútroštátneho právneho poriadku pre oblasť ochrany osobných údajov s **Nariadením** Európskeho parlamentu a rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov ...

Návrhom zákona sa zároveň transponuje **Smernica** Európskeho parlamentu a rady (EÚ) č. 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií ...

V rámci všeobecnej ochrany osobných údajov predpisovej základne Slovenskej republiky sa bude uplatňovať:

1. pre spracúvanie osobných údajov v rámci činností, ktoré podliehajú právu Európskej únie tak nariadenie, ako aj zákon, s výnimkou 1. časti až 3. časti zákona.
2. pre spracúvanie osobných údajov v rámci činností, ktoré nepodliehajú právu Európskej únie zákon ako celok,
3. pre spracúvanie osobných údajov na účely plnenia trestného konania príslušným orgánom zákon, s výnimkou vybraných ustanovení 3. časti návrhu zákona.“

Regulácie a povinnosti

Identifikácia regulácií (GDPR / zákon)

- Vyplývajúce zo zásad spracúvania osobných údajov
- Vyplývajúce z podmienok spracúvania osobných údajov
- Vyplývajúce z práv fyzických osôb
- Priamo uložené povinnosti prevádzkovateľovi v Tretej hlave Druhej časti zákona
- Povinnosti prevádzkovateľa pri prenose osobných údajov do tretej krajiny
- Možné povinnosti prevádzkovateľa vyplývajúce zo Štvrtej časti zákona
- Možné povinnosti prevádzkovateľa vyplývajúce zo Piatej časti zákona

Identifikovali sme 136 možných povinností prevádzkovateľa, niektoré z nich sa týkajú len istej skupiny prevádzkovateľov.

Transformácia regulácií do povinností a následných aktivít

- Klasifikácia regulácií ako sú
 - povinnosti,
 - práva fyzických osôb vyvolávajúce povinnosti,
 - práva / oprávnenia,
 - príkazy, zákazy, ...)
- Identifikácia regulácií vo forme povinností
- Priradenie konkrétnych aktivít danej povinnosti
- Priradenie zodpovednosti za dané aktivity
- Odhad vecného a časového rámca pre jednotlivé aktivity
- Závislosti aktivít, napr.
 - identifikácia IS / spracovateľské operácie
 - spracovateľské operácie / riziká
 - riziká / návrhy primeraných opatrení
 - opatrenia / obstarávaní
 - opatrenia / plánovanie ďalších zdrojov

1. Komplexné povinnosti prevádzkovateľa vyplývajúce zo zásad spracúvania osobných údajov

Tieto povinnosti sú bezpodmienečné - týkajú sa všetkých prevádzkovateľov. Sú komplexné, na ich splnenie je potrebné realizovať množstvo čiastkových aktivít. U týchto povinností sa predpokladá, že sú identifikované všetky IS s osobnými údajmi, spracovateľské operácie a sú posúdené riziká.



ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
1.1	Zásada zákonnosti - Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.	P 1.1.1 Zabezpečiť zákonnosť spracúvania osobných údajov (u existujúceho aj pripravovaného spracúvania) – vid' § 13. P 1.1.2 Preveriť, či pri spracúvaní nedochádza k porušeniu základných práv dotknutej osoby. Ak áno, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 6
1.2	Zásada obmedzenia účelu - Osobné údaje sa môžu ziskávať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.	P 1.2.1 Posúdiť, či sú osobné údaje získavané len na konkrétne určený, výslovne uvedený a oprávnený účel. Ak nie, zastaviť ich spracúvanie. P 1.2.2 V prípade spracúvania osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel preveriť, či je to v súlade s osobitným predpisom a či sú dodržané primerané záruky ochrany práv dotknutej osoby. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 7
1.3	Zásada minimalizácie osobných údajov - Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.	P 1.3.1 Preveriť, či spracúvané osobné údaje sú primerané, relevantné a obmedzené na nevyhnutný rozsah. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 8
1.4	Zásada správnosti - Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.	P 1.4.1 Mať nástroje na overenie správnosti osobných údajov a overovať, či sú osobné údaje správne a aktualizované. P 1.4.2 Mať nástroje na opravu alebo výmaz nesprávnych osobných údajov z hľadiska účelu spracúvania.	§ 9
1.5	Zásada minimalizácie uchovávania - Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8.	P 1.5.1 Mať určenú dobu pre uchovávanie osobných údajov so zohľadnením účelu ich spracúvania. P 1.5.2 Uchovávať osobné údaje tak, aby bola možná identifikácia dotknutej osoby. P 1.5.3 Ak je potreba uchovávať osobné údaje dlhšie, preveriť, či je to na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel a v súlade s osobitným predpisom a či sú dodržané primerané záruky ochrany práv dotknutej osoby. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 10

Zmena paradigmy – riadenie operačného rizika

GDPR a risk-driven prístup

- Nový prístup vo verejnej správe.
- Aktivity prispôsobujeme miere rizika (napr. spracovateľské operácie).
- Je potrebné poznať riziko a jeho mieru.
- Neriešime len riziká pre našu organizáciu
- Zaoberáme sa aj rizikami pre externé aktívum,

Nové aktívum pre analýzy rizík

- Práva a slobody fyzických osôb vo variantoch GDPR/zákon:
 - základné práva a slobody,
 - práva a slobody,
 - práva
- Je to aktívum našich klientov, ktoré je ohrozené našimi aktivitami.
- Toto aktívum je z pohľadu GDPR prioritné.
- Analýza rizík tohto aktíva má svoje špecifiká.
- IT firmy s tým doteraz skúsenosti nemali.
- Bez správneho posúdenia rizík pre toto aktívum nemôže byť organizácia v súlade.

Zvýšené operačné riziko vyplývajúce s GDPR

➤ **Sankcie**

- 100 krát vyššia úroveň priamej sankcie.
- Sankcie až do 4 % celosvetového obratu.

➤ **Súdne spory**

- Právo na náhradu škody a zodpovednosť (Článok 82, GDPR)
 - Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.

➤ **Neexistuje istota, že prijaté technické a organizačné opatrenia sú primerané.**

- Článok 32 GDPR: „Prevádzkovateľ a sprostredkovateľ prijímú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, **primerané technické a organizačné opatrenia...**“

Posúdenie rizika – 2 príbehy

Článok 24, GDPR

Aktívum: práva slobody fyzických osôb, podobne aj článok 35 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.
- Pre aké práva a slobody fyzických osôb?
- Aké sú riziká pre práva a slobody?
- Ako posúdiť ich pravdepodobnosť a závažnosť?
- Podľa akého štandardu postupovať?
 - Rodina noriem ISO 2700x?
 - Rodina noriem ISO 3100x?

Článok 32, GDPR

Aktívum: spracúvané osobné údaje

- Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na **riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku**
 - náhodného alebo nezákonného zničenia,
 - straty,
 - zmeny,
 - neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.
- Štandardná ISO 2700x analýza rizík
 - dôvernoscť,
 - dostupnosť,
 - integrita

Logy / záznamy o činnostiach

Zdroje logov

- Aplikácie
 - Transakčné systémy
- Správa domény
- Monitorovacie systémy (od aplikácií, cez e-mail až po sieťové vrstvy)
 - HW / appliance
 - SW riešenia
- Bezpečnostné systémy (antimalware, FW, IDS, IPS, DRM, SIEM, ...)

Obsah logov z pohľadu OÚ

- Záznamy o činnosti entít
 - Používatelia
 - Pracovné stanice
 - Sieťové prvky
 - Sieťová prevádzka
- prístup k časti aplikácie s logmi
 - správca
 - operátori

- Veľa aplikácií a zariadení s logmi
- Aké logy sú napr. v sieťových zariadeniach (switche, routre a ďalšie)?
 - Potrebná súčinnosť dodávateľa
 - Pôvodný dodávateľ už často nie je dostupný
- Sú to osobné údaje?
- Právne základy pre monitoring.
 - Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
 - Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy
 - Už aj zákon o kybernetickej bezpečnosti
 - Oprávnené záujmy.
- Aké činnosti s logmi sú spracovateľské činnosti v zmysle GDPR?
- Monitoring a právo osoby na súkromie a poštové tajomstvo (využívanie elektronickej pošty na súkromné účely)?

Pripravenosť na preukázanie súladu

Primeranosť opatrení - článok 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.
- Potrebné sú teda **nasledujúce kroky**:
 - Posúdenie povahy, rozsahu, kontextu a účelov spracúvania
 - Posúdenie rizík (pravdepodobnosti, závažnosti)
 - Výber vhodných technických a organizačných opatrení
 - Implementácia opatrení
 - Pravidelné preskúmanie, vrátane rizík
 - Aktualizácia opatrení
- Platí princíp prezumpcie viny – dôkazné bremeno je na prevádzkovateľovi.
- Úrovne posudzovania:
 - Interná
 - Externý audit
 - Úrad
 - Pri súdnom spore
- Či sme skutočne v súlade sa dozvieme až po kontrole alebo súdnom spore
- Realistické ciele:
 - Znižovanie rizík pre aktíva
 - Znižovanie pravdepodobnosti nesúladu
 - Znižovanie miery možných sankcií
- Nemôžeme byť v súlade, ak:
 - Nemám identifikované všetky IS / spracovateľské operácie
 - Nemáme identifikované všetky riziká
 - Nemáme určené primerané opatrenia
 - Nemáme implementované všetky primerané opatrenia

Otvorené otázky - príklady

Posúdenie vplyvov (DPIA)

Článok 35:

„Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.“

- Týka sa DPIA aj IS resp., spracovateľských operácií, ktoré sú už dnes v prevádzke? Alebo len tých nových?
- Ako správne rozhodnúť, či je DPIA potrebná?
 - Sankcia za chybné rozhodnutie – do 10. mil. euro.
- Ak máme posúdiť, či nejde pravdepodobne vysoké riziko, potrebujeme analýzu rizík už pred DPIA. Tá kvôli riziku sankcie musí byť na detailnej úrovni.
- Vysoké riziko môže nastať aj po zero-day hrozbe alebo exploite.
- Kedy Úrad vydá zoznam pre DPIA spracovateľské operácie?
- Doterajšia pomôcka: Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov (DPIA)

Práva fyzických osôb

Recitál 62 preambuly:

Nie je však potrebné uložiť povinnosť poskytovať informácie, ak dotknutá osoba už informácie má, ak zaznamenanie alebo poskytnutie osobných údajov je výslovne stanovené zákonom, alebo **ak sa poskytnutie informácií dotknutej osobe ukáže ako nemožné alebo by si vyžiadalo vynaloženie neprimeraného úsilia**. Posledná situácia by mohla byť najmä spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely. V tejto súvislosti by sa mal zohľadniť počet dotknutých osôb, vek údajov a všetky prijaté primerané záruky.

- Nakoľko je možné riadiť sa daným recitálom?
- Ako zabezpečiť právo na zabudnutie pri používaní masívneho zálohovania na neprepisovateľné médiá?
- Ako zabezpečiť právo na informovanosť – poskytnutie osobných údajov zo starých, archívnych systémov?
- Nástroje na sniffing všetkých osobných údajov zo všetkých IS predstavujú vážne bezpečnostné riziko, pritom sú ale účinným nástrojom na plnenie informačných povinností.

Zhrnutie

Zabezpečovanie súladu (compliance) predstavuje vážnu výzvu v manažmente operačného rizika, celkovej činnosti štátnej správy aj podnikateľských subjektov, informačnej spoločnosti. Problémom je veľký počet nových regulácií s náročnými požiadavkami a dopadmi z úrovne EÚ aj národnej legislatívy.

Nariadenie GDPR prináša množstvo regulácií, ktorých zabezpečenie je časovo aj finančne náročné, ak daný subjekt chce významne minimalizovať riziko sankcií a súdnych sporov pri náhrade škody od fyzických osôb.

25.5.2018 sa napĺňanie požiadaviek GDPR a zákona č. 18/2018 Z.z. nekončí, ale len prechádza do ďalšej fázy. GDPR isto bude tu s nami najbližších 10 rokov a s každou novou významnou hrozbou a zraniteľnosťou nám prinesie ešte veľa výziev, otvorených otázok, problémov a starostí – ale ako fyzickým osobám aj veľa významných benefitov.



Ďakujem za pozornosť

Michal Danilák, Lewik s.r.o.

www.lewik.org

<https://knowwww.eu/>

