Dopad nariadenia GDPR na nastavenie procesov v organizácii

Juraj Richter, Michal Hüber

20. september 2017

EY
Building a better working world

Agenda

1 Úvod

2 Prehľad procesných vzťahov

3 Vplyv GDPR na procesy v organizácii

4 Ako ďalej?

EY v Slovenskej republike

O nás

Služby

Komplexné poradenstvo zahrňujúce audit, podnikové, daňové a transakčné poradenské služby

Globálna sieť EY

Súčasťou globálnej siete EY, regiónu Central and South-East Europe (CSE) a širšieho regiónu Europe, Middle East, India and Africa (EMEIA)

Kancelárie

Bratislava (sídlo), Žilina a Košice

Počet odborníkov

300+

Spoločnosť EY pôsobí na Slovensku v oblasti odborného poradenstva už viac ako dvadsaťpäť rokov. Boli sme jednou z prvých poradenských firiem, ktoré sa etablovali v regióne strednej a juhovýchodnej Európy. V súčasnosti má naša spoločnosť vyše tristo zamestnancov so sídlom v Bratislave, Žiline a Košiciach.

V Slovenskej republike poskytujeme poradenské služby mnohým slovenským i medzinárodným spoločnostiam. Pracujeme pre najvýznamnejšie spoločnosti na slovenskom trhu.

V roku 2008 vznikla integrácia 87 zastúpení v krajinách západnej a východnej Európy, Stredného východu, Indie a Afriky, nová oblasť EMEIA. Slovenské zastúpenie patrí do jedného z 13 organizačných celkov EMEIA, Central and Southeast Europe, ktorý tvorí 22 krajín strednej a juhovýchodnej Európy. Vďaka spolupráci našich odborníkov s expertmi z celosvetovej siete EY sme schopní vytvárať medzinárodné tímy zložené z tých najskúsenejších špecialistov, ktorí poskytujú služby prvotriednej kvality.

Výsledky prieskumov

Zistenia spoločného prieskumu IAPP a EY – Annnual Privacy Governance Report 2016 ako aj výsledky Global Information Security Survey 2016 ukazujú, že organizácie stále potrebujú zlepšiť ochranu údajov.

Obidva reporty

potvrdzujú, že ochrana údajov nie je pre organizácie prioritou

63%

respondentov uviedlo, že ochrana údajov je u nich iba na základnej, prípadne mierne pokročilej úrovni

Organizácie budú musieť venovať zvýšenú pozornosť ochrane dát v súvislosti so sprísnením požiadaviek ako aj s hroziacimi pokutami.

69%

organizácií uviedlo, že legislatívne požiadavky sú jedným z hlavných dôvodov investovania do ochrany údajov

37%

organizácií očakáva, že v nasledovných rokoch sa množstvo zamestnancov venujúcich sa ochrane osobných údajov zvýši

Zdroj: https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2016/
http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

Agenda

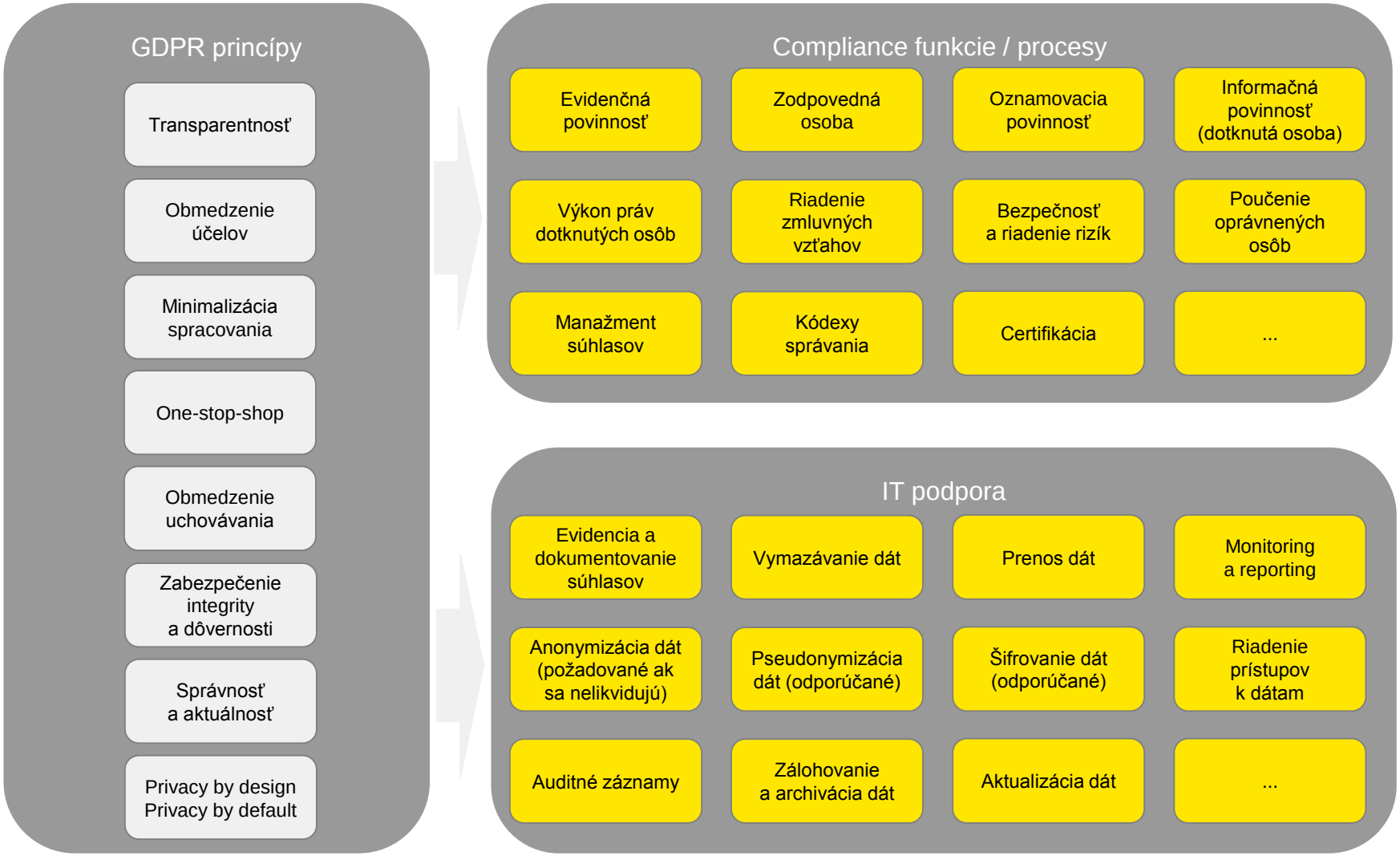
1 Úvod

2 Prehľad procesných vzťahov

3 Vplyv GDPR na procesy v organizácii

4 Ako ďalej?

Prehľad procesných vzťahov



Agenda

1 Úvod

2 Prehľad procesných vzťahov

3 Vplyv GDPR na procesy v organizácii

4 Ako ďalej?

Vplyv GDPR na procesy v organizácii – 1/11
Evidenčná povinnosť

Súčasný stav

- V zákone č. 122/2013 Z. z. sú podmienky evidencie stanovené v § 43
- Povinnosť mať vypracované evidenčné listy sa vzťahuje na systémy, ktoré nepodliehajú oznamovacej povinnosti alebo osobitnej registrácii

Zmeny vyplývajúce z GDPR

- **Článok 30 nariadenia**
- Zmena formy – záznamy o spracovateľských činnostiach
- Nariadenie explicitne nehovorí o formulároch, ale čo je potrebné evidovať (názov a kontaktné údaje prevádzkovateľa, údaje o zodpovednej osobe, účely spracúvania, kategórie dotknutých osôb, kategórie osobných údajov, všeobecný opis bezpečnostných opatrení)
- Po novom je potrebné v rámci procesu evidencie počítať s povinnosťou evidovať aj predpokladanú retenčnú dobu
  - lehota
  - kritériá

Vplyv GDPR na procesy v organizácii – 2/11
Zodpovedná osoba

Súčasný stav

- Organizácia môže ustanoviť zodpovednú osobu v súlade s § 23 zákona č. 122/2013 Z. z.
- Zodpovedná osoba musí absolvovať skúšku na výkon funkcie zodpovednej osoby na ÚOOÚ podľa § 24 zákona č. 122/2013 Z. z.

Zmeny vyplývajúce z GDPR

- **Články 37, 38 a 39 nariadenia**
- Ak je prevádzkovateľom orgán verejnej moci alebo verejnoprávny subjekt je určenie zodpovednej osoby (Data Protection Officer) povinné
- Nariadenie nestanovuje povinnosť absolvovať skúšku zodpovednej osoby
- Skupina podnikov môže určiť jednu zodpovednú osobu
- Dobrou praxou je, aby zodpovedná osoba absolvovala certifikáciu IAPP (CIPP/E, CIPM)

Vplyv GDPR na procesy v organizácii – 3/11
Oznamovacia povinnosť

Súčasný stav

- Oznamovacia povinnosť je ustanovená v § 34 až 36 zákona č. 122/2013 Z. z.:
  - Nahlasovanie zodpovednej osoby
  - Ak nie je ustanovená zodpovedná osoba, oznamujú sa systémy
  - Osobitná registrácia podľa § 37 zákona č. 122/2013 Z. z.

Zmeny vyplývajúce z GDPR

- Oznamovacia povinnosť voči dozorným orgánom spôsobovala administratívnu a finančnú záťaž
- Typy oznamovacích povinností, ktoré je potrebné zaviesť do procesného riadenia:
  - Oznámenie porušenia ochrany osobných údajov dozornému orgánu (do 72 hodín)
  - Oznámenie porušenia ochrany osobných údajov dotknutej osobe (bez zbytočného odkladu)
  - Oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania (smerovaná k príjemcom osobných údajov)

Vplyv GDPR na procesy v organizácii – 4/11
Informačná povinnosť voči dotknutým osobám

Súčasný stav

- Poskytovanie informácií dotknutej osobe je ustanovené v § 29 zákona č. 122/2013 Z. z.

Zmeny vyplývajúce z GDPR

- **Články 13 a 14 nariadenia**
- Nariadenie prináša zmenu v rozsahu informačnej povinnosti:

  totožnosť a kontaktné údaje prevádzkovateľa, kontaktné údaje prípadnej zodpovednej osoby, účely spracúvania, oprávnené záujmy, príjemci osobných údajov, úmysel preniesť osobné údaje do tretej krajiny, doby uchovávania atď.
- Výhodné je zaviesť proces poskytovania informácií vo forme Privacy notice v dvoch úrovniach:
  - Zverejnenie základných informácií v zrozumiteľnej forme na webovom sídle
  - Možnosť zobraziť úplnú Privacy notice

Vplyv GDPR na procesy v organizácii – 5/11
Výkon práv dotknutých osôb

Súčasný stav

- Práva dotknutých osôb zákon č. 122/2013 Z. z. upravuje v § 28

Zmeny vyplývajúce z GDPR

- **Články 15 až 22 nariadenia**
- Nariadenie výrazne posilňuje práva dotknutých osôb
- Najdôležitejšie práva, ktoré je nutné procesne ošetriť:
  - Právo na prenositeľnosť
  - Právo na výmaz (napr. odvolaním súhlasu)
  - Automatizované individuálne rozhodovanie:
    - Žiadosti o úver (automatizované overovanie a schvaľovanie)
    - Výber zamestnancov (pre-screening životopisov uchádzačov o zamestnanie)

Vplyv GDPR na procesy v organizácii – 6/11
Riadenie zmluvných vzťahov

Súčasný stav

- Spoloční prevádzkovatelia sú v zákone č. 122/2013 Z. z. uvedení len nepriamo (§ 4 ods. 2 b))
- Obsah zmluvy medzi prevádzkovateľom a sprostredkovateľom je stanovený v § 8 zákona č. 122/2013 Z. z.

Zmeny vyplývajúce z GDPR

- **Články 26 až 29 nariadenia**
- Nariadenie explicitne definuje pojem spoloční prevádzkovatelia
- Nové požiadavky na zmluvy so sprostredkovateľmi:
  - spracúvanie osobných údajov len na základe zdokumentovaných pokynov prevádzkovateľa
  - osoby sprostredkovateľa oprávnené spracúvať osobné údaje sú zaviazané, že zachovajú dôvernosť informácií
  - sprostredkovateľ zabezpečí vykonanie všetkých požadovaných bezpečnostných opatrení podľa článku 32 nariadenia

Vplyv GDPR na procesy v organizácii – 7/11
Bezpečnosť a riadenie rizík

Súčasný stav

- Zákon č. 122/2013 Z. z. rieši bezpečnosť osobných údajov v druhej hlave (zodpovednosť za bezpečnosť osobných údajov, bezpečnostný projekt, poučenie oprávnenej osoby, povinnosť mlčanlivosti)

Zmeny vyplývajúce z GDPR

- **Článok 32 nariadenia**
- Bezpečnostné projekty nie je potrebné zahadzovať
- Nariadenie požaduje riadenie rizík ako všeobecný prístup
- Zabezpečenie trvalej dôvernosti, integrity a dostupnosti (CIA) systémov – informačná bezpečnosť podľa 27001
- Integrácia PIA (posúdenie vplyvu na ochranu osobných údajov) do riadenia rizík
- K posudzovaniu rizík sa pristupuje z pohľadu rizík vyplývajúcich pre dotknutú osobu
- Identifikácia rôznych typov rizík (procesné, organizačné, IT, právne)
- Nariadenie priamo nešpecifikuje bezpečnostné opatrenia, ale odporúča napr. šifrovanie a architektonický princíp pseudonymizácie (oddelenie jednoznačných identifikátorov od ostatných osobných údajov)

Vplyv GDPR na procesy v organizácii – 8/11
Poučenie oprávnených osôb

Súčasný stav

- Zákon č. 122/2013 Z. z. vyžaduje poučenia oprávnených osôb a prevádzkovateľ je povinný o poučení vyhotoviť hodnoverne preukázateľný záznam (§ 21)

Zmeny vyplývajúce z GDPR

- Snaha nariadenia o menej formalizmu
- Nariadenie samo o sebe explicitne nehovorí povinnosti preukázateľného poučenia oprávnených osôb, avšak je to jedno z odporúčaných bezpečnostných opatrení prevádzkovateľa
- Vykonávanie kontinuálneho vzdelávania pre oblasť ochrany osobných údajov je nevyhnutné a je potrebné ho integrovať do vnútorných procesov organizácie

Vplyv GDPR na procesy v organizácii – 9/11
Manažment súhlasov

Súčasný stav

- Súhlasy dotknutých osôb sú rámcovo upravené v § 11 a 12 zákona č. 122/2013 Z. z.

Zmeny vyplývajúce z GDPR

- **Články 7 až 9 nariadenia**
- Procesy v organizácii je potrebné upraviť tak, že:
  - prevádzkovateľ musí vedieť preukázať súhlas dotknutej osoby so spracúvaním svojich osobných údajov
  - žiadosť o vyjadrenie súhlasu musí byť sformulovaná v zrozumiteľnej a ľahko dostupnej forme a oddelená od iných dokumentov (napr. Zmluva)
  - dotknutá osoba má právo kedykoľvek odvolať súhlas
  - odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie
- Úprava súhlasu dieťaťa – do 16 rokov (súhlas musí vyjadriť rodič)

Vplyv GDPR na procesy v organizácii – 10/11
Kódexy správania

Súčasný stav

- Súčasný zákon č. 122/2013 pojem kódex správania nepozná

Zmeny vyplývajúce z GDPR

- **Články 40 a 41 nariadenia**
- Úlohou dozorného orgánu je povzbudzovať združenia a iné subjekty zastupujúce kategórie prevádzkovateľov na prijatie kódexov správania
- Kódexy správania sa vytvárajú za účelom spresnenia uplatňovania nariadenia
- Slovenská banková asociácia pripravuje kódex v zmysle nariadenia
- Zatiaľ nemáme vedomosť, že by sa pripravoval kódex správania pre verejný sektor
- Monitorovanie súladu s kódexom správania môže vykonávať akreditovaný subjekt (akreditáciu udeľuje dozorný orgán)

Vplyv GDPR na procesy v organizácii – 11/11
Certifikácia

Súčasný stav

- Zákon č. 122/2013 pojem certifikácia nepozná

Zmeny vyplývajúce z GDPR

- **Články 42 a 43 nariadenia**
- Certifikácia je dobrovoľná
- Certifikácia sa vydáva na maximálne obdobie troch rokov
- ÚOOÚ (dozorný orgán) má ambíciu vykonávať akreditáciu aj certifikáciu, čo je v súlade s nariadením
- Zvážiť rozdelenie akreditačnej a certifikačnej funkcie obdobne ako napríklad pri európskom nariadení eIDAS
- V súčasnosti zatiaľ nie sú známe konkrétnejšie detaily (pripravuje sa nový zákon na ochranu OÚ, ktorý upraví aj pôsobnosť ÚOOÚ)

Agenda

1 Úvod

2 Prehľad procescných vzťahov

3 Vplyv GDPR na procesy v organizácii

4 Ako ďalej?

Čo môžete urobiť sami?

Základom pre úspech je poznanie Vašej súčasnej situácie.

Prvým najdôležitejším krokom je analýza spracovania osobných dát

Kto	Aké	Kde	Kam	Ako
je zodpovedný za prácu s osobnými údajmi?	osobné údaje sa spracovávajú?	sa tieto údaje spracovávajú?	sa prenášajú?	sú zabezpečené?

Po dôkladnom pochopení aktuálneho stavu je jednoduchšie pristúpiť k opatreniam na zabezpečenie súladu s GDPR

Ako Vám môže EY pomôcť?

Poradenstvo a podpora EY

Poznajte svoje osobné údaje

Identifikujeme, aký je stav ochrany osobných údajov v rámci vašej organizácie a vytvoríme „inventár osobných údajov“

Základné posúdenie pripravenosti na GDPR

Spoločne zrealizujeme workshopy a stretnutia na zistenie kľúčových nedostatkov.

Hĺbkové GDPR 360-stupňové posúdenie

Vykonáme detailné posúdenie vyspelosti (maturity) a súladu s GDPR.

Posúdenie vplyvu na ochranu údajov (DPIA)

Posúdime riziká pôsobiace na osobné údaje v systémoch alebo pri projektoch.

Program na zdokonalenie ochrany osobných údajov

Fáza návrhu riešení. Holistický program na dosiahnutie úplného súladu s GDPR.

Otázky

Ďakujeme za pozornosť

Kontaktné údaje

Michal Hüber
senior konzultant
Tel.: +421 918 447 843
E-mail: michal.huber@sk.ey.com

Juraj Richter
senior konzultant
Tel.: +421 910 820 827
E-mail: juraj.richter@sk.ey.com

Upozornenie

Informácie uvedené v tejto prezentácii majú všeobecný charakter a ich výhradným cieľom je poskytovať len rámcový prehľad príslušných tém. Tieto informácie nie je možné považovať za úplné alebo dostatočné pre rozhodovanie, ani sa nedajú použiť namiesto poradenstva poskytovaného odborným poradcom.

Ernst & Young, s. r. o., nepreberá žiadnu zodpovednosť za straty spôsobené konaním či opomenutím zo strany osôb využívajúcich informácie obsiahnuté v tejto prezentácii.

EY | Audit | Dane | Transakcie | Poradenstvo

Informácie o EY

EY patrí medzi najvýznamnejšie celosvetové firmy poskytujúce odborné poradenské služby v oblasti auditu a daňového, transakčného a podnikového poradenstva. Našimi názormi a kvalitou služieb prispievame k budovaniu dôvery v kapitálové trhy a ekonomiky celého sveta. Podporujeme rozvoj popredných lídrov, ktorých spája dôraz na kvalitu poskytovaných služieb vo vzťahu k všetkým zainteresovaným skupinám. V tom je náš hlavný prínos k lepšie fungujúcemu svetu pre našich ľudí, klientov a širšiu komunitu.

Označenie EY sa vzťahuje na celosvetovú organizáciu spoločností, ktorej riadiacou spoločnosťou je britská Ernst & Young Global Limited. Každá členská spoločnosť je nezávislým právnym subjektom. Ernst & Young Global Limited neposkytuje služby priamo klientom. Ďalšie informácie nájdete na našich webových stránkach ey.com.

ey.com/sk