Tempest
IT makes sense

Čo robiť, aby bol ÚOOU „spokojný“?

Daniela Palkovičová
Úrad na ochranu osobných údajov SR

Nový zákon o ochrane osobných údajov

- Pôsobnosť aj „popri“ *Nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)*
  - Osobitné situácie spracúvania osobných údajov *(účely akademické, umelecké alebo literárne; pre potreby informovania verejnosti masovokomunikačnými prostriedkami; prevádzkovateľ v postavení zamestnávateľa; podmienky spracúvania pre rodné číslo, osobitná kategória osobných údajov; získanie osobných údajov od inej fyzickej osoby ako dotknutej osoby; zosnulá dotknutá osoba; vedecké, historické a štatistické účely)*
- Postavenie a pôsobnosť úradu, dozorná činnosť *(kontrola, sťažnosť a one-stop-shop)*
- Kódex správania, certifikát a akreditácie *(možnosť preukázať splnenie bezpečnostných požiadaviek ochrany osobných údajov)*

Legislatívny proces - materiál preložený do NR SR, predpokladaný termín zverejnenia v zbierke zákonov január 2018 s účinnosťou máj 2018

Vykonávacie predpisy

- Informácie, ktoré majú byť obsiahnuté v štandardizovaných ikonách a postupy určovania štandardizovaných ikon
- Certifikačné kritériá, podmienky certifikačného postupu *(máj 2018)*
- Kritériá na udelenie akreditácie, podmienky akreditačného postupu *(máj 2018)*
- Podmienky výkonu auditu ochrany osobných údajov vrátane podmienok odborných znalostí audítora *(máj 2018)*
- Black list spracovateľských operácií, postup pri posudzovaní vplyvu a obsahové náležitosti technickej a bezpečnostnej dokumentácie *(január 2018)*

Stav harmonizácie právnej základne členských štátov:

ČR: nový zákon zastrešujúci tak harmonizáciu s nariadením ako aj smernicou pre príslušné orgány, znížili vek dieťaťa na 13 rokov, nižšie pokuty pre orgány verejnej moci, akreditácia zverená akreditačnému orgánu, nebudú udeľovať certifikáty

DE: akreditáciu vykonáva úrad, ale preskúmanie akreditačných podmienok je zverené akreditačnému orgánu

TRANSPOSITION OF DIRECTIVE (EU) 2016/680				
Member State	separate chapter incorporated in the general privacy act	separate legal act	separate chapter incorporated in the general privacy act + sectorial law	not yet decided
AT	X			
BE			X	
BG	X			
CY		X		
CZ			X	
DE			X	
ES		X		
FI			X	
FR	X			
HR		X		
IE	X			
LV		X		
NL		X		
PL				X
RO		X		
SE		X		
SI				X
SK	X			

Aké sú „nové povinnosti“ prevádzkovateľov voči úradu

Z vlastnej iniciatívy

- povinnosť požiadať o predchádzajúcu konzultáciu
- zverejniť a oznámiť kontaktné údaje zodpovednej osoby
- požiadať o osobitné povolenie pri prenose osobných údajov mimo EU vyžadujúcom primerané záruky (povoľovací mechanizmus): záväzné vnútropodnikové pravidlá, povolenie pre neštandardné zmluvné doložky a administratívne dojednania orgánov verejnej moci
- oznámenie porušenia ochrany osobných údajov tak úradu ako aj dotknutej osobe

Aké sú „nové povinnosti“ prevádzkovateľov voči úradu

Na požiadanie zo strany úradu

- súčinnosť pri dozornej činnosti (kontrolná činnosť úradu a konanie o ochrane osobných údajov *(v rámci jedného konania aj opatrenia, prípadne aj pokuta)*
- v procese schvaľovania kódexu správania, udeľovania certifikátu a akreditácie monitorujúceho a certifikačného subjektu
- povolenie pre certifikačný subjekt v rámci procesu udeľovania certifikátu

Predchádzajúca konzultácia

- pred začiatkom spracovateľskej operácie
- z posúdenia vplyvu vyplýva, že spracúvanie predstavuje vysoké „zvyškové“ riziko (vysoké riziko: typ spracúvania, rozsah a frekvencia spracúvania, stupeň ochrany osobných údajov)
- zvyškové riziko sa nedá zmierniť primeranými prostriedkami, pokiaľ ide o dostupné technológie a náklady na vykonanie opatrení
- v rámci žiadosti sa predkladá posúdenie vplyvu
- nie je povinnosťou sprostredkovateľa, ale má byť nápomocný prevádzkovateľovi (zásada zodpovednosti)

Predchádzajúca konzultácia

Úrad

- skúma či plánované spracúvanie osobných údajov je v súlade so zákonom, najmä či prevádzkovateľ správne identifikoval možné riziká, prípadne opatrenia na zmiernenie tohto rizika
- môže požadovať ďalšie informácie
- môže vykonať audit ochrany osobných údajov
- môže získať prístup k informačným systémom alebo do priestorov prevádzkovateľa
- môže uložiť opatrenia v prípade zistenia nesúladu so zákonom/nariadením obmedziť alebo zakázať spracovateľskú činnosť

Ak úrad zmešká lehotu, prevádzkovateľ môže začať so spracúvaním (nejde o súhlas so spracúvaním osobných údajov úradom, len o splnenie povinnosti zo strany prevádzkovateľa).

Zodpovedná osoba

- povinnosť ako aj dobrovoľnosť prevádzkovateľa alebo sprostredkovateľa poveriť
- povinnosť, ak:
  - spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt, najmä verejná doprava, energetika; hl. činnosťou, t.j. primárne činnosti – kľúčové operácie na dosiahnutie cieľov, nie doplnkové činnosti
  - dochádza k pravidelnému systematickému monitorovaniu dotknutých osôb vo veľkom rozsahu, napr. SBS pre veľké obchodné centrá
  - dochádza v rámci hl. činnosti k spracúvaniu citlivých údajov alebo údajov o uznaní viny za trestné činy alebo priestupky vo veľkom rozsahu, napr. nemocnice, nie súkromný lekár, advokát, účtovník
- spoločná zodpovedná osoba (účelnosť a dostupnosť pre úrad, v rámci organizácie a pre dotknuté osoby)

Zodpovedná osoba

Postavenie

- môže byť tak FO ako aj PO (nie priamo štatutárny zástupca ale priamo zodpovedný štatutárnemu orgánu)
- centralizácia alebo decentralizácia výkonu úloh zodpovednej osoby
- vyžadovanie a preukázanie odborných kvalít ako odborné znalosti a zručnosti
- zvládnutie konfliktu záujmu
- nezávislé postavenie a princíp dôvernosti výkonu funkcie (mlčanlivosť)
- nepodlieha pokute – poriadkovej pokute áno

Oznámenie o porušenia ochrany osobných údajov

- Oznámenie o porušenia ochrany osobných údajov (jeden informačný systém pri kybernetickom incidente; ostáva povinnosť hlásiť porušenie ochrany osobných údajov na Telekomunikačný úrad vs. EPrivacy; nie je sankcia za oznámenie o porušení, ostáva právo odvolať oznámenie napr. k porušeniu nedošlo - strata CD v prostredí prevádzkovateľa; strata šifrovacieho mechanizmu nie kľúča)
- Porušenie
  - porušenie dôvernosti – nezákonné zverejnenie ou a nezákonný prístup k ou
  - porušenie dostupnosti – strata ou (trvalá alebo závažná; ou existujú) a zničenie ou (ou neexistujú)
  - narušenie integrity – zmena ou
- Dopad na práva DO (postačí riziko; ak existuje vysoké riziko aj dotknutej osobe BZO, čo môže byť aj skôr ako úradu; info, ako sa má DO následne správať) strata kontroly, obmedzenie práv, diskriminácia, krádež identity, podvod, finančné straty, neoprávnené zvrátenie pseudonymizácie, poškodenie dobrej povesti, strata dôvernosti alebo integrity

Oznámenie o porušenia ochrany osobných údajov

- Povinnosť prevádzkovateľa oznámiť a zdokumentovať
- Povinnosť sprostredkovateľa hlásiť prevádzkovateľovi – považuje sa za „vedomé porušenie“
- Oznámiť do 72 hodín (úrad poskytuje pomoc a súčasne preveruje správnosť postupu)
  - v rámci bezpečnostnej politiky prevádzkovateľa a sprostredkovateľa potrebné prijať postupy na odhaľovanie a zvládnutie incidentov
  - bez zbytočného odkladu prijať opatrenia na preverenie incidentu, odstránenie následkov incidentu a obnovenie sprac. Ou
  - od zistenia – vedomé porušenie nastáva až po prešetrení incidentu a nadobudnutí istoty, že k nemu došlo (dôkaz) a po posúdení rizika (môže viesť k opätovnému posúdeniu vplyvu)

Otázky ?

statny.dozor@pdp.gov.sk

www.dataprotection.gov.sk

Ďakujem za pozornosť a prajem pohodový deň.