Všeobecné nariadenie o ochrane osobných údajov

Jesenné stretnutie SACKA 2016
10. november 2016, Vyšehrad

FIREMNÉ PORADENSTVO

Pramene práva ochrany osobných údajov

- Zákon č. 122/2013 Z.z. o ochrane osobných údajov
- Vyhláška č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení
- Vyhláška č. 165/2013 Z.z., ktorou sa ustanovujú podrobnosti o skúške fyzickej osoby na výkon funkcie zodpovednej osoby
- EÚ smernica 95/46/EC
- Platia len do 24.5.2018
- Nariadenie EP a Rady č. 2016/679 z 27.4.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov („Nariadenie“)
- **Účinné od 25. mája 2018**

Predmet úpravy

- V súčasnosti v každom štáte EÚ rôzna úroveň a rôzne pravidlá ochrany osobných údajov
- Nariadenie harmonizuje ochranu osobných údajov v celej EÚ, bude takmer totožná v celej EÚ
- Nariadenie bude platiť priamo v každom členskom štáte

Predmet úpravy

- **Rozšírená teritoriálna platnosť** – EÚ organizácie aj non-EÚ organizácie (ak ponúkajú služby EÚ obyvateľom alebo monitorujú správanie EÚ obyvateľov)
- **Vysoko rizikové činnosti** – spracúvanie osobitnej kategórie OÚ vo veľkom rozsahu, automatická profilácia, systematické monitorovanie, monitorovanie verejne prístupných miest
- Spracovanie údajov detí do 13/16 rokov – **súhlas rodiča**

Pojem osobné údaje

- Pojem podobný ako v súčasnosti
- Nové OÚ
  - **Lokalizačné údaje**
  - **Online identifikátory** – IP, plávajúca IP, cookies
  - **Genetické faktory**
- Osobitná kategória osobných údajov – rovnaká definícia, precizovaná o genetické a biometrické údaje (napr. podpis na tablet)
- **Anonymné údaje** – ak sa nedá spätne určiť dotknutá osoba, nespadajú pod Nariadenie
- **Pseudonymizované údaje** – sú OÚ, pretože umožňujú identifikáciu osoby, hoci s použitím kľúča = bezpečnostné opatrenie

Súhlas

- Slobodný
- Špecifický
- Na daný účel
- Informovaný
- Jednoznačný
- Preukázateľný
- Daný ako
  - Vyhlásenie
  - Jasný potvrdzujúci úkon
- Čas uloženia
- Možnosť odvolania – rovnako jednoduché ako súhlas
- Neplatný, ak je jasný nepomer medzi dotknutou osobou a prevádzkovateľom, napr. zamestnávateľ – zamestnanec
- Neplatný je opt-out súhlas, podmienený súhlas, nekonanie
- Dieťa do 16 rokov – súhlas rodiča

Princípy

- Čestné, legálne, transparentné spracúvanie údajov, tzn. **povinnosť informovať dotknutú osobu** o rozsahu a spôsoboch spracúvania jej údajov
- Obmedzenie spracúvania len **na účel**, na ktorý boli získané, okrem:
  - Archivácia, historický a vedecký výskum, štatistické účely
  - „ak má v úmysle ďalej spracúvať OÚ na iný účel ako ten, na ktorý boli získané, poskytne dotknutej osobe PRED takýmto ďalším spracúvaním informácie o tomto účele a ďalšie relevantné informácie.“
- Princíp **nevyhnutnosti**, **správnosti** a **aktuálnosti**, **bezpečnosti**, **likvidácie**
- Prevádzkovateľ/Sprostredkovateľ musí vedieť preukázať, že splnil požiadavky Naradenia

Právny základ

- Rovnaké ako v súčasnosti
- Súhlas, zmluva a predzmluvné vzťahy, právna povinnosť (osobitný predpis), ochrana života a zdravia (dotknutej osoby alebo inej FO), verejný záujem, legitímny záujem (§10 ods. 3 písm. g))
- Členské štáty môžu upraviť aj iné právne základy
- **Osobitná kategória osobných údajov**
  - Výslovný súhlas, zamestnanecké právo, ochrana života a zdravia, OZ a cirkvi, údaje zverejnené samotnou dotknutou osobou, uplatňovanie právnych nárokov, podstatný verejný záujem, medicínska diagnostika, verejné zdravie, historické účely, výnimky podľa národného práva
- **Nový účel** – kompatibilný s pôvodným (prepojenie účelov, kontext získavania údajov, povahu údajov, možné dôsledky pre dotknuté osoby, zabezpečenie ochrany)

Práva dotknutých osôb

- **Transparentná komunikácia** – prevádzkovateľ je povinný poskytnúť dotknutej osobe minimálne informácie o spracúvaných osobných údajoch a postupoch, a to v *stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho*, najmä ak je dotknutá osoba dieťa (ikony)
- Najneskôr v čase prvej komunikácie
- **Týka sa všetkých IS**, nielen tých, kde je právny základ súhlas
- Vybavovanie sťažností dotknutých osôb – do 1 mes., max. predĺženie o 2 mes.
  - Ak nestihne lehotu, môže dotknutá osoba podať sťažnosť na Úrad

Práva dotknutých osôb

- Vybavovanie žiadostí robí prevádzkovateľ zdarma, okrem opakujúcich sa a zjavne neopodstatnených alebo neprimeraných žiadostí
- **Právo na prístup** – právo dotknutej osoby žiadať, aby jej prevádzkovateľ sprístupnil, aké osobné údaje o nej spracúva, na aký účel, aký rozsah, komu sú poskytované a dobu, po ktorú sú uchovávané, zdroj údajov
- **Právo na zabudnutie** – právo byť vymazaný
  - Ak dáta už nie sú potrebné na pôvodný účel,
  - Právny základ – súhlas - odvolanie
  - Neexistuje právo ďalšieho spracúvania
  - Nelegálne spracovanie údajov
  - Zabezpečenie súladu s osobitným predpisom

Práva dotknutých osôb

- **Obmedzenie spracúvania**
  - Napadne správnosť údajov, ide o protizákonné spracúvanie
  - Len uchovávanie a použitie na uplatňovanie právnych nárokov, ochranu práv FO, ostatné použitie len so súhlasom
- **Notifikácia tretím stranám** – prevádzkovateľ je povinný oznámiť všetkým osobám, ktorým osobné údaje poskytol, že bolo uplatnené právo na zabudnutie, obmedzenie, blokovanie.
- **Právo na prenos údajov** – právo preniesť všetky údaje v zrozumiteľnej a technicky možnej forme od prevádzkovateľ alebo priamo od jedného prevádzkovateľ k druhému

Práva dotknutých osôb

- **Právo namietať** – voči spracúvaniu osobných údajov
  - Na priamy marketing
  - Vo verejnom záujme
  - Na legitímne záujmy prevádzkovateľa
  - Na historické, štatistické a vedecké účely
  - Na účely hodnotenia len na základe automatizovaného procesu
- **Právo podať sťažnosť** Úradu alebo Výboru

Povinnosti prevádzkovateľa

- Povinnosť preukázať plnenie povinností podľa Nariadenia
- Povinnosť prijať **primerané technické a organizačné opatrenia**
- Dodržovanie Kódexu správania
- Prijatie **špecifickej a štandardnej ochrany**
- Zrušené oznámenia IS na Úrad
- **Povinnosť viesť záznamy** – evidencie IS
  - Naviac doba uloženia
- Výnimka – organizácia s menej ako 250 zamestnancov a zároveň nevykonáva vysoko rizikové spracúvanie údajov

Povinnosti prevádzkovateľa

- **Bezpečnosť osobných údajov**
  - Anonymizácia, psedonymizácia, šifrovanie
  - Priebežné kontroly bezpečnostných opatrení
  - Zálohovanie dát
  - Pravidelné testovanie bezpečnosti
  - Dodržiavanie Kódexu správania
- **Oznamovanie bezpečnostných incidentov Úradu – do 72 h**
  - Výnimka: ak nie je pravdepodobné, že incident povedie k riziku pre práva a slobody FO
  - Všetky bezpečnostné incidenty musia byť zaznamenané bez ohľadu na ich veľkosť a dopady
- **Oznamovanie bezpečnostných incidentov dotknutým osobám – bezodkladne**
  - Výnimka: riziko poškodenia je nepravdepodobné, nakoľko údaje boli distatočne chránené
  - Prevádzkovateľ prijal opatrenia na odvrátenie škody
  - Oznámenie by bolo nemožné

Povinnosti sprostredkovateľa

- **Písomná zmluva** o spracúvaní osobných údajov
  - Okrem základných náležitosti podľa súčasného zákona – povinnosť po skončení spracúvania vymazať alebo vrátiť údaje prevádzkovateľovi a poučenie o mlčanlivosti pre oprávnené osoby
- **Cloud, vzdialený server, webhosting** – ak sú osobné údaje ukladané a zálohované
- **Oznamovanie bezpečnostných incidentov** – bezodkladne prevádzkovateľovi
- Vykonáva úkony len v rozsahu poverenia, po prekročení poverenia koná akoby vo vlastnom mene
- **Povinnosť viesť záznamy**, tzn. evidencie o osobných údajoch, ktoré spracúva v mene prevádzkovateľov
- Bezpečnosť údajov v rozsahu ako prevádzkovateľ
- Dotknutá osoba môže podať sťažnosť aj priamo sprostredkovateľovi

Zodpovedná osoba

- Prevádzkovateľ /sprostredkovateľ **je povinný ustanoviť zodpovednú osobu** v prípadoch:
  - Ide o orgán verejnej moci
  - Pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu
  - Spracúvanie osobitnej kategórie osobných údajov vo veľkom rozsahu
- ZO – musí mať expertné znalosti z práva a praxe ochrany osobných údajov
- ZO – môže byť zamestnanec alebo externá osoba na základe zmluvy
- Školenie/skúška nie je určená (?)

Cezhraničný prenos

- **Prenos v rámci EHS** – voľný pohyb osobných údajov je zaručený, nie sú stanovené žiadne osobitné požiadavky
- **Prenos do tretích krajín** zakázaný, ak nie sú splnené určité podmienky:
- A) prenos do tretích krajín, ktoré zaručujú primeranú ochranu – na základe **rozhodnutia Komisie**
- B) **záväzné vnútropodnikové pravidlá** – musia byť schválené Úradom
- C) **štandardné zmluvné doložky** schválené Komisiou

Cezhraničný prenos

- D) schválený **Kódex správania** – záväzné a vymáhateľné záväzky poskytnúť primerané záruky, nie je potrebné schválenie Úradom
- E) schválený **certifikačný mechanizmus** - záväzné a vymáhateľné záväzky importéra aplikovať certifikáciu na prenášané údaje, nevyžaduje sa schválenie Úradom
- F) **zmluvné doložky schválené Úradom** – národná alternatíva k štandardným zmluvným doložkám
- G) **ad hoc doložky** – schválené Úradom
- H) **EÚ – US Privacy Shield**

Cezhraničný prenos

- **Výnimky pre osobitné situácie:**
- A) výslovný informovaný **súhlas**
- B) **plnenie zmluvy** alebo predzmluvné obtrenia
- C) **zmluva v prospech dotknutej osoby**
- D) **verejný záujem**
- E) preukazovanie, uplatňovanie, obhajovanie **právnych nárokov**
- F) **životne** dôležité záujmy
- G) údaje z **verejných registrov**

- Národná legislatíva môže obmedziť niektoré formy cezhraničného prenosu

Kódexy správania a certifikácie

- Kódexy správania – asociácie a komory môžu pre svojich členov vypracovať Kódexy správania, v ktorých určia postupy spracúvania a bezpečnostné opatrenia, ktoré sú príznačné pre danú oblasť
- Prijatím Kódexu správania prevádzkovateľ / sprostredkovateľ preukáže, ž dodržiava pravidlá ochrany osobných údajov
- Certifikácia – dobrovoľný dôkaz plnenia pravidiel podľa Nariadenia
- Doteraz nejasné, podmienky určia členské štáty

Pokuty

- Dohľad nad dodržiavaním Nariadenia vykonávajú členské úrady – Úrad na ochranu osobných údajov
- Pri porušení uloží povinnosť odstrániť závadný stav a nariadi nápravné opatrenie.
- Pokuty ukladá popri nápravných opatreniach
- Maximálna pokuta **20 mil. eur** alebo **4% z ročného celkového obratu**

Príprava na účinnosť Nariadenia

- Audit súčasného stavu spracúvania osobných údajov
- Aké údaje sa spracúvajú, na aký účel, plnenie informačnej povinnosti voči dotknutým osobám, písomné zmluvy so sprostredkovateľmi
- Zabezpečiť súlad – prijatím technických, organizačných a personálnych opatrení

FIREMNÉ PORADENSTVO

Ďakujem za pozornosť

JUDr. Lucia Semančínová

E: lucia.semancinova@firemne-poradenstvo.sk

T: 0917 523 986

www.firemne-poradenstvo.sk

Firemné poradenstvo s.r.o., Polus Tower I, Vajnorksá 100/A, Bratislava

SEMANČÍN & PARTNERS