

Marec – jún 2017

Škola ochrany osobných údajov

advokátskej kancelárie Balcar, Polanský & Spol. s.r.o.

Nariadenie EP a Rady (EÚ) 2016/679 z 27. apríla 2016, tzv. Všeobecné nariadenie o ochrane údajov („Nariadenie“) zrušilo smernicu 95/46/ES („Smernica“), ktorá je momentálne pretransformovaná aj do slovenského právneho poriadku prostredníctvom zákona č. 122/2013 Z. z. o ochrane osobných údajov. Nariadenie nadobudne účinnosť dňom 25. mája 2018, kedy bude priamo účinné aj na Slovensku a dotkne sa všetkých, ktorí osobné údaje spracúvajú, ako aj fyzických osôb, ktorých osobné údaje sú predmetom spracúvania, teda takmer každého.

Vzhľadom na doposiaľ najvýznamnejšiu legislatívnu zmenu európskeho rozmeru v oblasti ochrany osobných údajov Vám na týždennej báze prinášame pravidelné informácie, aby ste sa mohli ľahšie a efektívnejšie zorientovať v spleti povinností, ktoré Nariadenie prináša.

Lekcia 1 z 16

Vecná a územná pôsobnosť Nariadenia

V texte sa dozviete:

Dôležité zmeny

- Bude mať podstatne širší dosah na tých ktorí údaje spracúvajú
- Bude sa vzťahovať aj na spoločnosti / inštitúcie, ktoré nie sú usadené priamo v EÚ, ak
 - budú spracúvať osobné údaje dotknutých osôb nachádzajúcich sa v EÚ v súvislosti s ponukou tovaru alebo služieb; alebo
 - ak pôjde o sledovanie správania dotknutých osôb v rámci EÚ (napr. prostredníctvom technických zariadení ako sú *cookies*).

Compliance: Akčný plán

- Spoločnosti/inštitúcie by mali posúdiť, či sa na nich nové Nariadenie vzťahuje
- Ak áno, sledujte nás ďalej na účely zistenia, ako zabezpečiť *compliance* a minimalizovať riziko vysokých pokút
- Ak nie, odporúča sa zaviesť priebežné monitorovacie procesy na zaistenie tohto statusu aj do budúcnosti

Vecná pôsobnosť

Nariadenie sa bude vzťahovať predovšetkým na spracúvanie osobných údajov:

- vykonávané úplne alebo čiastočne automatizovanými prostriedkami (prostredníctvom IT techniky), a na
- spracúvanie inými než automatizovanými prostriedkami (napr. záznamy v papierovej forme) v prípade osobných údajov, ktoré:
 - tvoria súčasť informačného systému (t.j. databázy údajov), alebo
 - sú určené na to, aby tvorili súčasť takej databázy.

Nariadenie sa nebude vzťahovať na určité druhy spracúvania, ako napr. pre osobné a domáce účely, spracúvanie súvisiace s vnútornou bezpečnosťou štátov EÚ a podobne.

Väčšina spracovateľských operácií vo verejnej a najmä komerčnej sfére však bude podliehať Nariadeniu.

Územná pôsobnosť

Prevádzkovatelia alebo sprostredkovatelia „usadení“ v EÚ

Nariadenie sa bude vzťahovať v prvom rade na osoby a spoločnosti, ktoré sú „usadené“ v EÚ, ak v rámci svojej činnosti spracúvajú osobné údaje. Je to široko koncipované pravidlo zabezpečujúce, aby sa Nariadenie vzťahovalo tak na prevádzkovateľov¹, ako aj na sprostredkovateľov² spracúvajúcich osobné údaje, pokiaľ sú usadení v EÚ, a to bez ohľadu na to, či sa samotné spracúvanie bude vykonávať v Únii alebo mimo nej.

¹ ten, kto sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov

² ten, kto spracúva osobné údaje v mene prevádzkovateľa

Novinkou je skutočnosť, že Nariadenie rozšírilo svoju pôsobnosť práve o sprostredkovateľov usadených v Únii. Podľa pôvodnej právnej úpravy platí, že ak prevádzkovateľ nie je usadený v EÚ, avšak spracúvaním osobných údajov poveril sprostredkovateľa, ktorý v EÚ usadený je, také spracúvanie nepodliehalo úprave Smernice.

Dôležité pritom je, že koncept „usadenia sa“ spoločnosti v Únii bol v poslednej dobe jasnejšie zdefinovaný prostredníctvom rozhodnutí ESD. Prevratné v tomto ohľade je rozhodnutie ESD vo veci *Weltimmo v. NAIH* z roku 2015 (C-230/14), ktoré má význam najmä pre osoby podnikajúce prostredníctvom internetu vo viacerých štátoch EÚ. Spoločnosť Weltimmo mala sídlo na Slovensku, avšak cezhranične poskytovala prostredníctvom internetu služby aj obyvateľom Maďarska. ESD rozhodol, že slovenská spoločnosť, napriek tomu, že nemá pobočku ani inú formu zastúpenia v Maďarsku, podlieha právomoci orgánu dohľadu nad ochranou osobných údajov v Maďarsku. ESD vyslovil, že ak spoločnosť ponúka služby v oficiálnom jazyku krajiny (v tomto prípade v maďarčine) a v danej krajine má zástupcu – fyzickú osobu, v takom prípade podlieha kontrolnej právomoci orgánov dohľadu v tejto krajine bez ohľadu na to, že nie je zapísaná v tamojšom obchodnom registri. Podľa ESD existencia pobočky spoločnosti v určitom štáte nie je nevyhnutným kritériom pri určovaní, či spoločnosť je alebo nie je usadená v určitom štáte. Naopak, o usadenie sa môže jednať tam, kde spoločnosť vykonáva hoci minimálnu, avšak reálnu a efektívnu činnosť prostredníctvom napr. webovej stránky v lokálnom jazyku, zástupcu operujúceho na danom území, a prípadne poštovej adresy či bankového účtu, ako to bolo v prípade Weltimmo.

Spoločnosti neusadené v EÚ

Rozšírenie územnej pôsobnosti Nariadenia aj na tie organizácie, ktoré nie sú usadené v členskom štáte EÚ, avšak spracúvajú osobné údaje dotknutých osôb nachádzajúcich sa v Únii, je jednou z najvýznamnejších zmien, ktoré Nariadenie prináša. Ak Spoločnosť alebo inštitúcia so sídlom mimo EÚ spĺňa jednu z podmienok ustanovených Nariadením, automaticky sa na ňu bude Nariadenie vzťahovať. Taká spoločnosť bude povinný dodržiavať princípy spracúvania a zaviesť opatrenia na zabezpečenie ochrany osobných údajov stanovené Nariadením, bude podliehať dozorným orgánom určeným Nariadením a bude znášať nimi uložené sankcie.

Nariadenie sa bude na mimoeurópske spoločnosti vzťahovať, ak tieto spracúvajú osobné údaje dotknutých osôb nachádzajúcich sa v Únii, a ak ich spracovateľská činnosť súvisí:

- s ponukou tovaru alebo služieb týmto dotknutým osobám bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo
- so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie.

Čo presne sa rozumie „dotknutými osobami, ktoré sa nachádzajú v Únii“, zatiaľ nie je celkom jasné. Dá sa však predpokladať, že pôjde o široký koncept a bude tendencia vykladať ho tak, aby zahrnul čo najviac dotknutých osôb pod „dáždnik“ ochrany, ktoré Nariadenie chce poskytnúť. Smerodajným pri výklade tohto pojmu by mohli byť miesto fyzickej prítomnosti a miesto pobytu dotknutej osoby.

Po prvýkrát je pôsobnosť Nariadenia založená na skutočnosti, či spoločnosť sleduje správanie dotknutých osôb na území Únie. O sledovanie pôjde najčastejšie prostredníctvom internetu použitím malých textových súborov odosielaných tým, kto údaje získava, do zariadenia dotknutej osoby (počítač, smartfón atď.), tzv. *cookies*.

V podmienkach predošlej právnej úpravy podľa Smernice sa dozorné orgány snažili založiť svoju právomoc vykonávať dohľad nad mimoeurópskymi podnikmi spracúvajúcimi osobné údaje obyvateľov Únie cez tú skutočnosť, že spoločnosti využívali technické zariadenia nachádzajúce sa na území EÚ na spracúvanie osobných údajov, pričom za technické zariadenie sa považovali práve *cookies*. Podľa Nariadenia sa tieto snahy nahradia jednoznačným ustanovením o aplikovateľnosti Nariadenia v prípade, ak spoločnosť bude sledovať správanie dotknutých osôb v Únii. Relevantné pritom bude aj ďalšie spracúvanie, napr. profilovanie, ktorým sa rozumie akákoľvek forma automatizovaného spracúvania osobných údajov, ktorým sa sleduje analýza alebo predvídanie

aspektov súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

Pri určovaní, toho, či sa mimoeurópska spoločnosť považuje za usadenú v Únii, budú smerodajné kritériá vyslovené vyššie uvedeným rozhodnutím ESD vo veci *Weltimmo*. To znamená, že napríklad samotná skutočnosť, že určitú webovú stránku je možné otvoriť z krajiny EÚ, nebude postačovať na vytvorenie záveru o existencii usadenia v Únii. Musí byť preukázané, že aktivity spoločnosti majú byť zacielené na dotknuté osoby v EÚ. Ak by napríklad stránky existovali v niektorých z lokálnych jazykov štátov EÚ, obsahovali by ceny v menách štátov EÚ (napr. EUR, GBP, CZK), obsahovali by kontaktné údaje (napr. telefónne čísla) s európskymi predvoľbami, také okolnosti by boli relevantné pre záver o usadení spoločnosti v Únii.

Do akej miery bude dohľad európskych orgánov dozoru nad spracúvaním osobných údajov spoločnosťami mimo Únie efektívny, zatiaľ nebolo otestované a reálna vykonateľnosť ich rozhodnutí mimo EÚ (napr. rozhodnutia Úradu na ochranu osobných údajov SR o uložení pokuty spoločnosti so sídlom v Číne) ostáva do veľkej miery otvorenou otázkou. Uvedený koncept ochrany dotknutých osôb v Únii vo vzťahu k spoločnostiam mimo EÚ je však prelomový. Dôvodom pre jeho zavedenie bolo presvedčenie, že dotknuté osoby v EÚ by nemali byť zbavené ochrany pri spracúvaní ich osobných údajov iba preto, že spoločnosť si zriadi sídlo mimo EÚ.

Čo ďalej

Na začiatok by spoločnosti a inštitúcie mali zistiť, či sa na nich Nariadenie bude vzťahovať vzhľadom na rozšírenú územnú pôsobnosť. Pre mimoeurópske spoločnosti sa odporúča obozretnosť pri zisťovaní, či sa považujú za „usadené“ v EÚ.

Ak aktivity spoločnosti či inštitúcie budú spadať do pôsobnosti Nariadenia, bude potrebné sa oboznámiť s početnými povinnosťami ukladanými Nariadením a oboznámiť s nimi aj osoby, ktoré budú v mene spoločnosti či inštitúcie nakladať s osobnými údajmi. Povinnosti prevádzkovateľov a práva dotknutých osôb, ako aj princípy spracúvania osobných údajov, budú predmetom ďalších lekcí Školy ochrany osobných údajov.

Ďalšie informácie

Vecná pôsobnosť: Recitály 6-18 Nariadenia; článok 2 Nariadenia

Územná pôsobnosť: Recitály 22-24 Nariadenia; článok 3 Nariadenia

Lekcia 2 z 16

Zásady ochrany osobných údajov

V texte sa dozviete:

Dôležité zmeny

- V dôsledku novozavedenej zásady zodpovednosti budú spoločnosti / inštitúcie spracujúce osobné údaje vo vlastnom mene (prevádzkovatelia) povinné nie len dodržať, ale aj vedieť preukázať, že osobné údaje spracúvajú v súlade so zásadami ochrany osobných údajov

Compliance: Akčný plán

Prevádzkovatelia by mali pred nadobudnutím účinnosti Nariadenia:

- vykonať audit spracúvania osobných údajov so zameraním na nové povinnosti;
- vytvoriť (resp. aktualizovať existujúce) interné predpisy upravujúce spracúvanie, aktualizovať pracovný poriadok v rozsahu monitorovania zamestnancov a ochrany ich osobných údajov, zrevidovať pracovné zmluvy zamestnancov oprávnených spracúvať osobné údaje, ako aj všetky ostatné dokumenty týkajúce sa spracúvania;
- zabezpečiť a vedieť preukázať vyškolenie svojich zamestnancov, majúcich prístup k osobným údajom, ohľadne ich práv a povinností, a poučiť ich o následkoch porušenia ich povinností.

K zásadám ochrany osobných údajov

Zásady ochrany osobných údajov v zmysle Nariadenia sú podobné tým, ktoré upravovala Smernica a ktoré obsahuje aj aktuálne znenie zákona č. 122/2013 Z. z. o ochrane osobných údajov. Nariadenie ich však podrobnejšie špecifikuje a rozširuje.

Zákonnosť, spravodlivosť, transparentnosť

Osobné údaje musia byť vo vzťahu k dotknutej osobe spracúvané zákonným spôsobom, spravodlivo a transparentne.

Pre účely splnenia podmienky transparentnosti sa spoločnosti / inštitúcie budú musieť vysporiadať s povinnosťou poskytnúť dotknutým osobám, ktorých osobné údaje spracúvajú, rozsiahly balík informácií. Mali by dostatočne jasne a zrozumiteľne informovať dotknuté osoby o podmienkach spracúvania a o právach, ktoré majú v tejto súvislosti³.

Zoznam informácií, ktoré prevádzkovatelia budú povinní preukázateľne oznámiť dotknutým osobám pred začatím spracúvania, je v porovnaní so Smernicou podstatne širší a zahŕňa okrem iného právo na vymazanie (t.j. „právo byť zabudnutý“⁴), právo namietať spracúvanie alebo podať sťažnosť

³ Za nelegitímne spracúvanie je z logiky veci považované utajené a neviditeľné inštalovanie spywaru (viď. prípad prevádzkovateľa webových stránok, ktorý zverejňoval e-mailové adresy účastníkov internetovej diskusie; WP 29 - Pracovná skupina pre ochranu jednotlivcov v súvislosti so spracovaním (čl. 29)

⁴ Dopusiaľ zmienené iba prostredníctvom judikatúry SDEU, viď. vec C-131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Spor medzi skupinou Google a p. Gonzalez, ktorý si prial vymazať z verejného povedomia nepríjemnú epizódu, kedy bola v tlači zverejnená informácia o nútenom predaji jeho nehnuteľnosti z dôvodu nesplateného dlhu na sociálnom poistení, ktorý bol následne zaplatený. Španielsky úrad nariadil spoločnosti Google Inc., aby prijala opatrenia k odstráneniu osobných údajov týkajúcich sa p. Gonzáleza zo svojho indexu a zabránila prístupu k týmto údajom v budúcnosti.

dozornému orgánu, či právo, aby sa na dotknutú osobu nevzťahovalo rozhodnutie založené výlučne na automatizovanom spracúvaní vrátane profilovania⁵. Samozrejme, popri poučení o svojich právach musia byť dotknuté osoby informované o osobitostiach spracúvania, vrátane toho, na aké účely sa údaje budú spracúvať a na základe akého právneho základu (napr. súhlas, zákonné ustanovenie a pod.). Oznamovacej povinnosti sa budeme podrobnejšie venovať v samostatnej lekcii.

Obmedzenie účelu

Osobné údaje musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Ďalšie spracúvanie na inom účelom než tým, na ktorý boli osobné údaje získané, bude na rozdiel od aktuálnej právnej úpravy za istých podmienok dovolené. Toto je podstatnou zmenou v slovenských podmienkach spracúvania a znamená, že aj keď prevádzkovateľ získa osobné údaje na konkrétny účel, za splnenia určených podmienok môže tieto údaje spracúvať aj na iné než pôvodné účely.

Ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v zmysle Nariadenia nepovažuje za nezlučiteľné s pôvodným účelom za predpokladu, ak osoba spracujúca údaje zabezpečí primerané záruky pre práva a slobody dotknutej osoby. Prevádzkovateľ by mal za tým účelom zaviesť technické a organizačné opatrenia, ktoré môžu zahŕňať minimalizáciu údajov, pseudonymizáciu⁶ či anonymizáciu.

Za nezlučiteľné s primárnym účelom bude podľa nášho názoru naďalej považované spracúvanie osobných údajov získaných pri prejednaní priestupku na sekundárny účel, ktorým bude napr. zverejnenie v miestnom periodiku alebo prostredníctvom internetu, alebo zverejnenie údajov o existencii dlhu majiteľa bytu, spracúvaných primárne v súvislosti so správou bytového domu, alebo sprístupnenie získaných osobných údajov jednotlivých účastníkov zájazdu bez ich súhlasu všetkým ostatným cestujúcim, atď.

Minimalizácia údajov

Osobné údaje musia byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.

Primeranosť osobných údajov vo vzťahu k účelu spracúvania nie je vždy jednoznačne určiteľná. Zistenie, či je spracúvanie konkrétnych osobných údajov primerané, bude vyžadovať posúdenie, či zásah do práv dotknutej osoby, ku ktorému v dôsledku spracúvania dôjde, je primeraný legitímnemu účelu spracúvania. Ak sa spracúvanie konkrétneho osobného údajá na určitý účel ukáže ako nadbytočné, také spracúvanie by nebolo súladné s Nariadením. Pre ilustráciu, zjavne neprimerané by bolo spracúvanie rodného čísla dotknutej osoby na účely marketingu, keďže na tento účel nie je nevyhnutné tento údaj spracúvať.

Správnosť

Osobné údaje musia byť správne a podľa potreby aktualizované. Prevádzkovateľ je povinný zabezpečiť, aby sa osobné údaje, ktoré sú nesprávne, bezodkladne vymazali alebo opravili.

⁵ Vid'. čl. 4 ods. 4 Nariadenia, t.j. „akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom“.

⁶ Vid'. čl. 4 ods. 5 Nariadenia, t.j. „spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe“.

Minimalizácia uchovávania

Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných Nariadením na ochranu práv a slobôd dotknutých osôb.

Integrita a dôvernosť

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.

Zodpovednosť

Prevádzkovateľ je zodpovedný za spracúvanie osobných údajov v súlade s vyššie uvedenými zásadami, pričom musí vedieť tento súlad aj preukázať. Na preukázanie súladu je možné napr. vypracovať písomné podklady o tom, že všetky aspekty spracovateľských operácií v rámci spoločnosti či inštitúcie boli interne posúdené, pričom výsledkom tohto posúdenia je súlad s ustanoveniami Nariadenia.

Nariadenie zavádza nový koncept ochrany osobných údajov, a to špecificky navrhnutú („*data protection by design*“) a štandardnú („*data protection by default*“) ochranu osobných údajov.

Špecificky navrhnutá ochrana osobných údajov znamená, že prevádzkovateľ, so zreteľom na rôzne aspekty spracúvania (napr. najnovšie poznatky, povahu, rozsah a účely spracúvania, riziká vyplývajúce pre práva dotknutých osôb), je povinný pred začatím spracúvania prijať primerané technické a organizačné opatrenia a záruky na ochranu osobných údajov, a tieto priebežne adaptovať na aktuálne podmienky spracúvania. Inými slovami, tento koncept zaväzuje všetky spoločnosti / inštitúcie spracujúce osobné údaje, aby vykonali interný audit spracúvania osobných údajov. Je nevyhnutné, aby sa ochranou osobných údajov aktívne zaoberali, vyčlenili si ľudské, finančné a technické zdroje na účely posúdenia zákonnosti spracúvania a zaviedli opatrenia na ich ochranu.

Štandardná ochrana osobných údajov znamená, že prevádzkovateľ zabezpečí, aby sa spracúvali len osobné údaje nevyhnutné pre každý konkrétny účel spracúvania. Je povinný tiež zabezpečiť, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

Ak prevádzkovateľ spracúva osobné údaje prostredníctvom inej osoby (sprostredkovateľ), tento je oprávnený spracúvať osobné údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to vyžaduje podľa práva Únie alebo práva členského štátu.

Čo ďalej

Spoločnosti / inštitúcie, ktorých sa to týka, sú povinné vykonať audit spracúvania osobných údajov a zabezpečiť jednak súlad, ale aj schopnosť preukázania, že osobné údaje spracúvajú zákonne a s odbornou starostlivosťou, a za týmto účelom prijali organizačné a technické opatrenia a záruky. Návrhy na zabezpečenie uvedeného nájdete v časti *Compliance* vyššie.

Ďalšie informácie

Recitály 39, 40, 22

Články 5, 6, 24, 25, 29, 89 ods. 1

Lekcia 3 z 16

Zákonnosť spracúvania a ďalšieho spracúvania

V texte sa dozviete:

Dôležité zmeny

- Nariadením sa zmení okruh právnych základov spracúvania osobných údajov
- V určitých prípadoch bude spracúvanie na iný účel, než na ktorý boli osobné údaje pôvodne získané, prípustné
- Zavádzajú sa kritériá pre test kompatibility účelov spracúvania

Compliance: Akčný plán

- Kontrola právnych základov spracúvania osobných údajov a zabezpečenie, že tieto budú aktuálne aj po nadobudnutí účinnosti Nariadenia
- Zabezpečenie preukázateľnosti vykonania testu kompatibility, ak sa osobné údaje spracúvajú na iný než pôvodný účel

K zákonnosti spracúvania

Ako sme uviedli v Lekcii 2, jednou zo zásad spracúvania osobných údajov je zákonný spôsob spracúvania⁷. Pojem „zákonný spôsob“ je značne široký a bez ďalšej konkretizácie by bol vágny a právne neurčitý. Nariadenie ho však bližšie upravuje v článku 6.

Podmienka zákonnosti spracúvania stanovuje, že ak sa na spracúvanie nevzťahuje niektorá z výnimiek upravených Nariadením, je prevádzkovateľ vždy povinný disponovať súhlasom dotknutej osoby so spracúvaním osobných údajov. Okrem súhlasu dotknutej osoby, ktorému sa budeme osobitne venovať v samostatnej lekcii, je teda spracúvanie zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok (tzv. „právny základ spracúvania“)⁸: spracúvanie je nevyhnutné

- a) na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy⁹;
- b) na splnenie zákonnej povinnosti prevádzkovateľa¹⁰;
- c) aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby¹¹;
- d) na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi¹²;

⁷ Čl. 5 ods. 1 Nariadenia: *Osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe.*

⁸ Zákonnosťou spracúvania citlivých osobných údajov sa budeme venovať v samostatnej lekcii.

⁹ Napr. spotrebiteľ si objedná tovar v on-line obchode, predávajúci pre účely doručenia musí spracúvať jeho meno, priezvisko a adresu, prípadne iný kontaktný údaj.

¹⁰ Základ pre spracúvanie musí byť stanovený buď právom Únie alebo právom členského štátu vzťahujúceho sa na prevádzkovateľa. Taký právny predpis môže upravovať konkrétne okolnosti spracúvania ako sú všeobecné podmienky vzťahujúce sa na zákonnosť spracúvania prevádzkovateľom, typy spracúvaných údajov, dotknuté osoby; subjekty, ktorým sa môžu osobné údaje poskytnúť, účely, na ktoré ich možno poskytnúť, obmedzenia účelu, doby uchovávanía, a spracovateľské operácie a postupy vrátane opatrení na zabezpečenie zákonného a spravodlivého spracúvania.

¹¹ Spracúvanie osobných údajov na účel životne dôležitého záujmu inej fyzickej osoby by sa malo uskutočniť len vtedy, keď sa takéto spracúvanie nemôže zakladať na inom právnom základe.

- e) na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa¹³.

V podmienkach obchodných spoločností bude okrem súhlasu dotknutých osôb relevantný najmä právny základ spracúvania uvedený v bodoch a), b) a e) vyššie.

Nariadenie deleguje štáty Únie, aby si upravili špecifické požiadavky a implementovali opatrenia na konkretizovanie dôvodov spracúvania uvedených v bodoch b) a d) vyššie. Rovnako to platí aj o špecifických typoch spracúvania¹⁴.

Nové právne základy spracúvania osobných údajov po nadobudnutí účinnosti Nariadenia, budú aj:

- v nadväznosti na čl. 85 Nariadenia, spracúvanie osobných údajov nevyhnutné na účely akademické, umelecké, literárne alebo žurnalistické, ak to prevádzkovateľovi vyplýva z predmetu jeho činnosti, okrem ak by také spracúvanie porušilo právo dotknutej osoby na ochranu jej osobnosti a súkromia alebo takéto spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný zákon alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná;
- v nadväznosti na čl. 88 Nariadenia, sprístupnenie, poskytovanie alebo zverejnenie osobných údajov v rozsahu titul, meno, priezvisko, pracovné, služobné alebo funkčné zaradenie, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo alebo elektronická pošta na pracovisko a identifikačné údaje zamestnávateľa, ak je prevádzkovateľ zamestnávateľom dotknutej osoby;
- vo vzťahu k čl. 87 Nariadenia, možnosť využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania a zároveň dotknutá osoba dala písomný alebo inak hodnoverne preukázateľný súhlas na jeho spracúvanie;
- vo vzťahu k čl. 89 Nariadenia, spracúvanie na účely archivácie vo verejnom záujme, vedecký, historický výskum a na štatistické účely;
- vo vzťahu k čl. 49 ods. 5 Nariadenia, oprávnenie uskutočnenia prenosu osobitnej kategórie osobných údajov a všeobecne použiteľného identifikátora tretej strane so sídlom v tretej krajine, ktorá nezaručuje primeranú úroveň ochrany osobných údajov, iba s predchádzajúcim výslovným súhlasom dotknutej osoby, ak osobitný zákon neustanovuje inak;
- vo vzťahu k čl. 9 ods. 4 Nariadenia, spracúvanie genetických údajov, biometrických údajov a údajov týkajúcich sa zdravia, ak je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa.

Bude povinnosťou štátov, aby v týchto špeciálnych prípadoch zabezpečili súlad ochrany osobných údajov s právom na slobodu slova a na informácie.

Štáty sú tiež povinné oboznámiť Komisiu pred tým, ako Nariadenie nadobudne účinnosť, o prijatých pravidlách, nuansách a výnimkách pri spracúvaní osobných údajov na novinárske účely a pre účely akademické, umelecké a literárne, ako aj na účely spracúvania v rámci pracovnoprávných vzťahov a v kontexte zákonnej povinnosti mlčanlivosti.

¹² Vid'. pozn. 4.

¹³ Existencia oprávneného záujmu si vyžaduje dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie.

¹⁴ Ako je uvedené v kapitole IX Nariadenia.

Obsolétne právne základy

V porovnaní s aktuálnou právnou úpravou¹⁵ („zákon“) sa dňom účinnosti Nariadenia zrušia nasledovné právne základy spracúvania:

- právny základ podľa § 10 ods. 3 písm. d) zákona „priamy marketing v poštovom styku“; pri dodržaní podmienok určených Nariadením, najmä zásady proporcionality s ohľadom na primerané očakávania dotknutých osôb a existencie oprávneného záujmu prevádzkovateľa, bude možné priamy marketing považovať za oprávnený záujem (t.j. právny základ uvedený v bode e) vyššie);
- právny základ podľa § 10 ods. 3 písm. e) zákona „ďalšie spracúvanie už zverejnených osobných údajov“; tento právny základ je v rozpore so zásadou zákonnosti, spravodlivosti a transparentnosti a zásadou obmedzenia účelu a kompatibility účelu; pre spracúvanie už zverejnených osobných údajov bude musieť prevádzkovateľ disponovať iným primeraným právnym základom; a
- právny základ podľa § 15 ods. 4 zákona „jednorazový vstup“ a právny základ podľa § 15 ods. 7 zákona „monitorovanie priestorov prístupných verejnosti“; prevádzkovateľ bude musieť disponovať iným primeraným právnym základom, napríklad zákonná povinnosť podľa bodu b) vyššie alebo oprávnený záujem podľa bodu e) vyššie.

K zákonnosti ďalšieho spracúvania

Ako sme uviedli v Lekcii 2, ďalšou zo zásad spracúvania osobných údajov je zásada obmedzenia účelu, ktorý ukladá prevádzkovateľom povinnosť získavať údaje na konkrétny, výslovne určený a legitímny účel, a zakazuje im spracúvať osobné údaje v rozpore s takto určeným účelom.¹⁶ Nariadenie však ustanovením článku 6 ods. 4 dovoľuje, aby sa osobné údaje získané na určitý účel za určitých podmienok spracúvali aj na iný než pôvodný účel (tzv. „ďalšie spracúvanie“). Ide o spracúvanie na iný, avšak kompatibilný účel s pôvodným účelom, na tom istom právnom základe (t.j. účel spracúvania sa mení, právny základ nie).

Uvedeným ustanovením Nariadenie takpovediac vnáša svetlo do šedej zóny, ktorá existovala v otázke ďalšieho spracúvania v podmienkach predošlej právnej úpravy. Okrem toho, že Nariadenie explicitne upravuje, že ďalšie spracúvanie na tzv. privilegované účely (t.j. archivácia vo verejnom záujme, vedecký alebo historický výskum či štatistické účely) sa nepovažuje za nezlučiteľné s pôvodným účelom, ak prevádzkovateľ zabezpečí primerané záruky pre práva a slobody dotknutej osoby¹⁷, Nariadenie upravuje aj pravidlá týkajúce sa faktorov, ktoré prevádzkovatelia musia vziať do úvahy pri zisťovaní, či nový účel je kompatibilný s účelom, na ktorý údaje boli pôvodne získané.

Inými slovami, ak prevádzkovateľ zvažuje, či môže osobné údaje spracúvať aj na iný účel, než na ktorý boli pôvodne získané, je povinný vykonať tzv. test kompatibility účelov spracúvania. Test kompatibility sa vykoná podľa konkrétnych určených podmienok, ktorými sú:

- akékoľvek prepojenie medzi účelmi, na ktoré sa osobné údaje získali, a účelmi zamýšľaného ďalšieho spracúvania;
- okolnosti, za akých sa osobné údaje získali (najmä týkajúce sa vzťahu medzi dotknutými osobami a prevádzkovateľom);
- povaha osobných údajov (najmä či sa spracúvajú osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky);

¹⁵ Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

¹⁶ Čl. 5 ods. 1 písm. b) Nariadenia: *Osobné údaje musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi.*

¹⁷ Prevádzkovateľ by mal za tým účelom zaviesť technické a organizačné opatrenia, ktoré môžu zahŕňať minimalizáciu údajov, pseudonymizáciu či anonymizáciu.

- možné následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby;
- existencia primeraných záruk (napr. šifrovanie alebo pseudonymizácia).

Nariadenie uvedené kritériá uvádza za slovným spojením „okrem iného“, to znamená, že pre účely testu kompatibility je možné zvážiť aj ďalšie vhodné kritériá. Ak je však spracúvanie na pôvodný účel založené na súhlase dotknutej osoby alebo na osobitnom právnom predpise (upravujúcom napr. verejný záujem, národnú alebo verejnú bezpečnosť a pod.), mal by mať prevádzkovateľ možnosť osobné údaje ďalej spracúvať bez ohľadu na zlučiteľnosť účelov.

Vyššie uvedené podmienky pre prípustnosť ďalšieho spracúvania sa vzťahujú iba na pôvodného prevádzkovateľa. Ak by spracovateľskou operáciou malo dôjsť k poskytnutiu osobných údajov inému prevádzkovateľovi, tento by musel disponovať právnym základom na takéto spracúvanie. Prevádzkovateľ je zároveň povinný vopred informovať dotknutú osobu o prípadnom ďalšom spracúvaní.

Čo ďalej

V zmysle vyššie uvedeného je potrebné, aby spoločnosti a inštitúcie pred nadobudnutím účinnosti Nariadenia overili, že spracúvajú osobné údaje na základe právnych základov upravených Nariadením.

Pre účely zabezpečenia zákonnosti ďalšieho spracúvania bude tiež potrebné vykonať test kompatibility podľa stanovených kritérií.

Ďalšie informácie

Recitály 40, 41, 44 - 47, 50, 153, 155

Články 5 ods. 1 písm. a) a b), 6, 23 ods. 1, kapitola IX (čl. 85-91)

Lekcia 4 z 16

Súhlas so spracúvaním osobných údajov Spracúvanie osobných údajov maloletých

V texte sa dozviete:

Dôležité zmeny

- Nariadenie prináša nové požiadavky pre udelenie súhlasu so spracúvaním osobných údajov
- Špecifické požiadavky sa kladú na spracúvanie osobných údajov osôb v súvislosti s vedeckým výskumom a osobných údajov maloletých¹⁸

Compliance: Akčný plán

- Spoločnosti/inštitúcie by mali zabezpečiť, aby osobné údaje spracúvali na základe správnych a existujúcich právnych základov
- Ak sa osobné údaje spracúvajú na základe súhlasu, je nutné zabezpečiť najmä, aby:
 - súhlas bol daný aktívnym úkonom dotknutej osoby, nie mlčaním, nečinnosťou alebo vopred označenými políčkami;
 - súhlas bol odlíšiteľný od iných dojednaní, konkrétny a jasný;
 - dotknuté osoby boli informované o možnosti súhlas odvolať a odvolanie súhlasu bolo rovnako jednoduché ako jeho poskytnutie;
 - poskytnutie služieb nebolo podmienené súhlasom so spracúvaním údajov, ktoré nie sú nevyhnutné;
 - osobitný súhlas bol udelený na osobitné spracovateľské operácie;
 - súhlas nebol udelený v podmienkach závažnej nerovnováhy v postavení prevádzkovateľa a dotknutej osoby (napr. v prípade verejného orgánu)

K súhlasu so spracúvaním osobných údajov

Ako sme uviedli v Lekcii 3, ak sa na spracúvanie osobných údajov nevzťahuje žiadna z výnimiek ustanovených Nariadením, prevádzkovateľ musí vždy disponovať súhlasom dotknutej osoby so spracúvaním jej osobných údajov. Nariadenie definuje súhlas ako akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka¹⁹.

Podľa aktuálnej slovenskej právnej úpravy²⁰ je súhlas definovaný ako akýkoľvek slobodne daný, výslovný a zrozumiteľný prejav vôle, a teda nová právna úprava sa od tej aktuálnej odlišuje okrem iného aj v tom, že po novom sa nebude vyžadovať, aby súhlas bol daný výslovne. To znamená, že súhlas bude teda môcť byť udelený aj konkludentne (napr. určitým konaním, ale nie nekonaním), avšak slobodne, konkrétne, jednoznačne a na základe úplných a zrozumiteľných informácií poskytnutých dotknutej osobe. Na spracúvanie citlivých osobných údajov sa však bude vyžadovať výslovný súhlas dotknutej osoby, (ak nebude existovať iná výnimka).

¹⁸ Nariadenie používa pojem „dieťa“, my používame pojmy „maloletý“ a „dieťa“ zameniteľne, v rovnakom význame.

¹⁹ Čl. 4 ods. 11 Nariadenia

²⁰ § 4 ods. 3 písm. d) zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Požiadavky na udelenie súhlasu

Nariadenie ustanovuje, že prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov. Inými slovami, dôkazné bremeno preukázania, že súhlas bol udelený a že bol udelený platne, je na prevádzkovateľovi. Formálne a obsahové podmienky platnosti udelenia súhlasu Nariadenie upravuje v čl. 7 nasledovne:

- *Sloboda prejavu, určitosť, informovanosť, jednoznačnosť:* súhlas vyžaduje jasný prejav vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením dotknutej osoby, že súhlasí so spracúvaním osobných údajov, ktoré sa jej týkajú.

Aby sa zabezpečilo, že súhlas sa poskytol slobodne, prevádzkovateľ by sa nemal spoliehať na súhlas vtedy, ak medzi jeho postavením a postavením dotknutej osoby existuje jednoznačný nepomer, najmä ak je prevádzkovateľ orgánom verejnej moci, a preto nie je pravdepodobné, že sa súhlas poskytol slobodne.

Za slobodne daný súhlas sa nepovažuje, ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu alebo nemôže odmietnuť či odvolať súhlas bez nepriaznivých následkov.

Požiadavka informovanosti vyžaduje, aby si dotknutá osoba bola vedomá, že dáva súhlas a v akom rozsahu ho udeľuje, a mala by si byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov.

- *Osobitné uvedenie účelov:* súhlas sa musí vzťahovať na všetky spracovateľské činnosti vykonávané na ten istý účel alebo účely a ak sa spracúvanie vykonáva na viaceré účely, súhlas sa má udeliť, resp. má byť uvedený na dané účely samostatne, aby bola zachovaná reálna možnosť dotknutej osoby odmietnuť udelenie súhlasu na hociktorý z uvedených účelov.

Súhlas sa nepovažuje za poskytnutý slobodne, ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov napriek tomu, že by to bolo v konkrétnom prípade vhodné.

V praxi nebude prijateľný „plošne“ udelený súhlas, v ktorom budú skombinované rôzne nesúvisiace účely spracúvania.

- *Odlíšiteľnosť, jasnosť, jednoduchosť:* ak sa súhlas udeľuje v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola ľahko odlíšiteľná od iných skutočností, a musí byť formulovaná jasne a jednoducho; porušenie tohto ustanovenia má za následok neplatnosť udelenia súhlasu.

V praxi to bude znamenať, že časť dokumentu obsahujúca žiadosť o súhlas bude musieť byť nezávislá napr. od zmluvných dojednaní, textu objednávok, vyhlásení, atď.

- *Zrozumiteľnosť, dostupnosť:* súhlas má byť formulovaný v zrozumiteľnej a ľahko dostupnej forme, jasne a jednoducho.

Táto požiadavka môže byť osobitne ťažko splniteľná najmä s ohľadom na rozsah informácií, ktoré je prevádzkovateľ povinný dotknutej osobe poskytnúť (viac k informačnej povinnosti prevádzkovateľa v samostatnej lekcii).

- *Odvolateľnosť:* odvolanie súhlasu musí byť rovnako jednoduché, ako jeho poskytnutie; o možnosti kedykoľvek súhlas odvolať musí byť dotknutá osoba informovaná pred jeho poskytnutím.

V praxi sa bude od spoločností a inštitúcií požadovať, aby umožnili odvolanie súhlasu rovnakou cestou, akou sa súhlas udelil (napr. webová stránka, e-mail, nastavenie ochrany súkromia v aplikácii a pod.). Nariadenie ustanovuje, že odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním (t.j. zákaz retroaktivity), avšak o tomto by mali byť dotknuté osoby informované pred udelením súhlasu.

- *Zákaz nenáležitého podmieňovania:* plnenie zmluvy sa nesmie podmieňovať súhlasom so spracúvaním osobných údajov, ktoré nie je nevyhnutné na plnenie zmluvy (napr. splnenie kúpnej zmluvy uzatvorenej on-line sa nesmie podmieniť súhlasom na spracúvanie osobných údajov na marketingové účely). V opačnom prípade by existovala dôvodná pochybnosť o slobodnom prejave vôle, a teda o platnosti súhlasu.

Súhlas sa nepovažuje za poskytnutý slobodne, ak sa plnenie zmluvy vrátane poskytnutia služby podmieňuje takýmto súhlasom, aj keď to na takéto plnenie nie je takýto súhlas nevyhnutný.

Recitál 32 Nariadenia uvádza, že súhlas sa môže vyjadriť napríklad písomným vyhlásením vrátane vyhlásenia prostredníctvom elektronických prostriedkov alebo ústnym vyhlásením. Súhlas je možné udeliť aj inak než výslovne, a to napr. označením políčka pri návšteve internetového webového sídla (princíp *opt-in*), zvolením technických nastavení služieb informačnej spoločnosti (napr. nastavením pravidiel ochrany osobných údajov na sociálnych sieťach) alebo akýmkoľvek iným vyhlásením či úkonom, ktorý v tomto kontexte jasne znamená, že dotknutá osoba súhlasí s navrhovaným spracúvaním jej osobných údajov. Mlčanie, vopred označené políčka alebo nečinnosť sa nepovažujú za súhlas.

Súhlas na účely vedeckého výskumu

Nariadenie pripúšťa, že ak sa majú osobné údaje spracúvať na účely vedeckého výskumu, často nie je možné v čase získavania údajov úplne určiť účel spracúvania osobných údajov. Preto by sa dotknutým osobám malo umožniť udeliť svoj súhlas pre určité oblasti vedeckého výskumu, pokiaľ sú dodržané uznávané etické normy vedeckého výskumu. Dotknuté osoby by mali mať možnosť udeliť svoj súhlas iba na určité oblasti výskumu alebo časti výskumných projektov v rozsahu, ktorý umožňuje zamýšľaný účel.

Na vyslovenie súhlasu s účasťou vo vedeckom výskume v rámci klinických štúdií sa bude aplikovať osobitné nariadenie.²¹

K spracúvaniu osobných údajov maloletých

Nariadenie na viacerých miestach upravuje špecifické podmienky pre spracúvanie osobných údajov maloletých. Konkrétne v recitáli 38 uvádza, že osobitnú ochranu osobných údajov si zasluhujú deti, keďže si môžu byť v menšej miere vedomé rizík, dôsledkov a dotknutých záruk a svojich práv súvisiacich so spracúvaním osobných údajov.

Spracúvanie osobných údajov maloletých na základe súhlasu

Nariadenie upravuje určité špecifiká týkajúce sa spracúvania osobných údajov maloletých na základe súhlasu, a to nasledovne:

- ak prevádzkovateľ spracúva osobné údaje dotknutej osoby na základe jej súhlasu, v súvislosti s ponukou služieb informačnej spoločnosti (napr. sociálnych médií) adresovanou maloletému je spracúvanie osobných údajov maloletého zákonné, len ak má maloletý aspoň 16 rokov²²;
- ak má maloletý menej než 16 rokov, takéto spracúvanie je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil zákonný zástupca alebo zákonný opatrovník maloletého;

²¹ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 536/2014 z 16. 4. 2014 o klinickom skúšaní liekov na humánne použitie.

²² Členské štáty môžu právnym predpisom stanoviť na tieto účely nižšiu vekovú hranicu za predpokladu, že takáto nižšia veková hranica nie je menej než 13 rokov.

- prevádzkovateľ je povinný vynaložiť primerané úsilie, aby si v takýchto prípadoch overil, že zákonný zástupca alebo zákonný opatrovník maloletého vyjadril súhlas alebo ho schválil, pričom zohľadní dostupnú technológiu.

Uvedené podmienky sa vzťahujú na osobné údaje poskytované prostredníctvom internetu, t.j. na off-line dáta sa tieto podmienky nevzťahujú. Rovnako sa nevzťahujú na osobné údaje, ktoré sa spracúvajú na inom právnom základe, než je súhlas. Vyššie uvedené ustanovenia tiež nebudú mať vplyv na vnútroštátne všeobecné zmluvné právo členských štátov, napríklad pravidlá platnosti, uzatvárania alebo účinkov zmluvy vo vzťahu k maloletému.

Súhlas zákonného zástupcu alebo zákonného opatrovníka sa nebude vyžadovať v súvislosti s preventívnymi alebo poradenskými službami, ktoré sú ponúkané priamo maloletému (napr. linky pomoci smerované na maloletých).²³

Iné špecifiká týkajúce sa maloletých

Nariadenie ustanovuje, že osobitnú ochranu osobných údajov požívajú maloletí. Takáto ochrana sa vzťahuje najmä na využívanie osobných údajov maloletých na účely marketingu alebo vytvorenia osobného alebo používateľského profilu a získavanie osobných údajov o maloletých pri používaní služieb poskytovaných priamo im.

S ohľadom na vyššie uvedené všetky informácie a každá komunikácia, pri ktorej sa spracúvanie zameriava na maloletého, by mali byť formulované jasne a jednoducho, aby boli ľahko pochopiteľné. Osobitný význam nadobúda právo na opravu osobných údajov a „právo byť zabudnutý“ v prípadoch, kedy bol daný súhlas v maloletosti, kedy si subjekt nebol plne vedomý všetkých rizík spojených so spracúvaním a neskôr chce svoje údaje, najmä na internete, odstrániť.²⁴

Ak prevádzkovateľ spracúva osobné údaje na základe oprávneného záujmu²⁵, musí vedieť preukázať, že zodpovedne a objektívne posúdil, že záujmy alebo základné práva a slobody maloletého, ktorého osobné údaje spracúva, neprevažujú nad oprávneným záujmom sledovaným prevádzkovateľom.

Podľa čl. 40 ods. 2 Nariadenia združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov môžu vypracovať kódexy správania na účely spresnenia uplatňovania Nariadenia aj v súvislosti s informovaním a ochranou maloletých a spôsobom získania súhlasu nositeľov rodičovských práv a povinností. Okrem toho, každý dozorný orgán, t.j. aj Úrad na ochranu osobných údajov SR, je povinný na svojom území zvyšovať povedomie verejnosti a jej chápanie rizík, pravidiel, záruk a práv súvisiacich so spracúvaním. Osobitná pozornosť sa pritom má venovať činnostiam špecificky zameraným na maloletých.

Čo ďalej

Prevádzkovatelia by mali zabezpečiť, aby osobné údaje spracúvali na základe relevantných a Nariadením upravených právnych základov. Ak osobné údaje budú spracúvané na základe súhlasu so spracúvaním osobných údajov, formálne a obsahové podmienky súhlasu, ako aj okolnosti jeho poskytnutia, by mali zodpovedať novej právnej úprave. Pri spracúvaní osobných údajov v súvislosti s výskumom, resp. v súvislosti s maloletými, je potrebné spĺňať ďalšie špecifické povinnosti.

²³ Recitál 38, posledná veta Nariadenia

²⁴ Recitál 65 Nariadenia

²⁵ Čl. 6 ods. 1 písm. f) Nariadenia

Ďalšie informácie

Súhlas so spracúvaním osobných údajov:

Recitály 32, 33, 40, 42, 43

Články 6 ods. 1, 7

Spracúvanie osobných údajov maloletých:

Recitály 38, 58, 65, 71

Články 6, ods. 1, 8, 40 ods. 2, 57 ods. 1 písm. b)

Lekcia 5 z 16

Oprávnený záujem

V texte sa dozviete:

Dôležité zmeny

- Orgány verejnej moci nebudú môcť spracúvať osobné údaje na základe právneho základu „legitímny záujem“ pri výkone ich úloh.
- Prevádzkovatelia, ktorí spracúvajú osobné údaje na základe „oprávneného záujmu“, by mali venovať náležitú pozornosť posúdeniu, či záujmy alebo práva a slobody dotknutých osôb neprevažujú nad oprávneným záujmom, ktorý prevádzkovateľ takým spracúvaním sleduje.

Compliance: Akčný plán

Ak prevádzkovateľ spracúva osobné údaje na právnom základe oprávneného záujmu, mal by zabezpečiť, aby:

- spracúvanie bolo aj po nadobudnutí účinnosti Nariadenia vykonávané zákonným spôsobom (viď. Lekcia 3 – Zákonnosť spracúvania a ďalšieho spracúvania), a aby tento právny základ bol relevantný pre dané okolnosti;
- pre účely preukázateľnosti viedol evidenciu o tom, ako sa vysporiadal s právami a slobodami oprávnených osôb, do ktorých sa spracúvaním ich osobných údajov zasiahne;
- oprávnené osoby boli informované o tom, že ich osobné údaje budú spracúvané na tomto konkrétnom právnom základe.

K špecifikám právneho základu oprávneného záujmu

Nariadenie upravuje, že spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z ďalej uvedených podmienok. Ako jedna z podmienok sa uvádza: spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa²⁶.

Pre porovnanie, aktuálna slovenská právna úprava²⁷ („Zákon“) hovorí, že prevádzkovateľ spracúva osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany, najmä osobné údaje spracúvané v rámci ochrany majetku, finančných alebo iných záujmov prevádzkovateľa a osobné údaje spracúvané na zabezpečenie bezpečnosti prevádzkovateľa prostredníctvom kamier alebo obdobných systémov. To neplatí, ak pri takomto spracúvaní osobných údajov prevažujú základné práva a slobody dotknutej osoby, ktoré podliehajú ochrane podľa tohto zákona.

Oproti aktuálnej právnej úprave je znenie Nariadenia širšie a odlišuje sa v nasledovnom:

- kým Zákon legitimizuje spracúvanie osobných údajov bez súhlasu dotknutej osoby na účel *ochrany práv a právom chránených záujmov* prevádzkovateľa alebo tretej strany, Nariadenie uvádza, že osobné údaje je možné spracúvať bez súhlasu dotknutej osoby, ak je to nevyhnutné na účely *oprávnených záujmov* prevádzkovateľa alebo tretej strany.

²⁶ Článok 6 ods. 1 písm. f) Nariadenia

²⁷ § 10 ods. 3 písm. g) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

Z uvedeného vyplýva, že výnimka z povinnosti disponovať súhlasom dotknutej osoby upravená Nariadením je širšia než tá, ktorú upravuje Zákon, a teda dá sa pod ňu zahrnúť viacero spracovateľských operácií.

Kým podľa aktuálnej právnej úpravy musí byť splnená podmienka spracúvania osobných údajov na účel *ochrany* práv a právom chránených záujmov (t.j. musí ísť o výslovne o zámer chrániť práva prevádzkovateľa alebo tretej strany), Nariadenie takúto požiadavku neukladá. Naopak, podľa Nariadenia postačí, ak sa osobné údaje budú spracúvať na účely oprávnených záujmov prevádzkovateľa alebo tretej strany, bez ochranného faktora.

Pod nový koncept oprávneného záujmu tak bude spadať napríklad aj spracúvanie osobných údajov na účel priameho marketingu či jednorazového vstupu do budovy, ktoré účely nemajú výslovne ochranný charakter.

- Nariadenie oproti pôvodnej právnej úprave ukladá, aby posúdenie vyváženeosti oprávneného záujmu sledovaného prevádzkovateľom, a záujmov a základných práv a slobôd dotknutých osôb, do ktorých sa bude spracúvaním ich osobných údajov zasahovať, bolo vykonané s osobitným ohľadom na maloletých²⁸.

Nariadenie tak sleduje zvýšenú mieru ochrany základných práv a slobôd maloletých, keďže si môžu byť v menšej miere vedomí rizík, dôsledkov a dotknutých záruk a svojich práv súvisiacich so spracúvaním osobných údajov. Nariadenie ukladá prevádzkovateľovi povinnosť starostlivo zdokumentovať to, akým spôsobom a s akým výsledkom sa vykonalo posúdenie vyváženeosti oprávneného záujmu prevádzkovateľa (príp. tretej strany) a základných práv a slobôd maloletého, ktoré budú spracúvaním dotknuté.

Pre účely posúdenia, či práva a slobody dotknutých osôb (nie len maloletých) neprevažujú nad oprávnenými záujmami prevádzkovateľa, je potrebné zohľadniť primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Existencia oprávneného záujmu vyžaduje dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie.

- Napokon, Nariadenie špecificky ustanovuje, že o oprávnený záujem sa nebudú môcť oprieť orgány verejnej moci pri výkone svojich úloh. Na tento účel bude potrebné zvážiť aplikáciu iného právneho základu²⁹.

Oprávnený záujem

Nariadenie uvádza príklady, aké účely spracúvania sa dajú subsumovať pod „oprávnený záujem“, nasledovne:

- predchádzanie podvodom;
- priamy marketing;
- ak je prevádzkovateľ súčasťou skupiny podnikov alebo inštitúcií, ktoré sú prepojené s ústredným subjektom, môže mať oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov alebo zamestnancov;
- zabránenie neoprávnenému prístupu k elektronickým komunikačným sieťam a šíreniu škodlivých programových kódov, ako aj zastavenie útokov sledujúcich cieľené preťaženie serverov („denial of service“) a poškodzovanie počítačových a elektronických komunikačných systémov;

²⁸ Vid' Lekcia 4.

²⁹ Napr. čl. 6 ods. 1 písm. c) alebo e) Nariadenia

- oznámenie možných trestných činov alebo ohrozenia verejnej bezpečnosti prevádzkovateľom a poskytnutie relevantných osobných príslušnému orgánu.

Účel spracúvania, vrátane ak ním sú oprávnené záujmy, by mali byť riadne oznámené dotknutej osobe pred začatím spracúvania (informačnou povinnosťou sa budeme zaoberať v samostatnej lekcii).

Nariadenie ďalej výslovne upravuje³⁰, že združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov môžu vypracovať kódexy správania na účely spresnenia uplatňovania tohto nariadenia, ako napríklad v súvislosti s oprávnenými záujmami, ktoré prevádzkovatelia sledujú v konkrétnych situáciách. Prevádzkovatelia by si mali overiť, či existuje kódex správania, ktorý by sa vzťahoval na nimi vykonávané spracovateľské operácie.

Čo ďalej

Prevádzkovateľ by mal zabezpečiť, aby v prípade, ak spracúva osobné údaje na účel oprávneného záujmu sledovaného ním alebo treťou stranou, záujmy a základné práva a slobody dotknutých osôb neprevažovali nad oprávnenými záujmami, osobitne v prípadoch, kedy dotknutou osobou je maloletý. Ďalej je potrebné zabezpečiť, aby prevádzkovateľ bol schopný preukázať, akým spôsobom sa vysporiadal s posúdením vyváženosti ním sledovaných oprávnených záujmov a práv a slobôd dotknutých osôb.

Ďalšie informácie

Recitály 47 - 50

Články 6 ods. 1 písm. f), 13 ods. 1 písm. d), 14 ods. 2 písm. b), 40 ods. 2 písm. b)

³⁰ Čl. 40 ods. 2 písm. b) Nariadenia

Lekcia 6 z 16

Osobitná kategória osobných údajov

V texte sa dozviete:

Dôležité zmeny

- Nariadenie pod osobitnú kategóriu osobných údajov (ďalej aj "citlivé údaje") zahŕňa vyslovene aj genetické údaje a tiež biometrické údaje, ak sa spracúvajú na účel jedinečnej identifikácie osoby;
- Právne základy spracúvania citlivých údajov sa mierne odlišujú od aktuálnej právnej úpravy;
- Členské štáty budú môcť prijať vlastné modifikácie spracúvania citlivých údajov.

Compliance: Akčný plán

- Ak prevádzkovateľ spracúva citlivé údaje, je potrebné správne zdefinovať právny základ, na základe ktorého tak robí;
- Ak je právnym základom súhlas dotknutej osoby, je potrebné, aby spĺňal požadované obsahové náležitosti.

Spracúvanie osobitnej kategórie osobných údajov

Nariadenie medzi citlivé osobné údaje zahŕňa predovšetkým také osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách. Ďalej, ako citlivé osobné údaje Nariadenie výslovne uvádza aj genetické údaje³¹, biometrické údaje³² na individuálnu identifikáciu fyzickej osoby, údaje týkajúce sa zdravia³³ alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

Nariadenie uznáva, že citlivé údaje si zasluhujú osobitnú ochranu, keďže z kontextu ich spracúvania by mohli pre základné práva a slobody vyplývať významné riziká. Nariadenie preto zakotvuje v článku 9 ods. 1 všeobecný zákaz ich spracúvania, ktorý môže byť prelomený iba spôsobmi uvedenými v článku 9 ods. 2. Prelomenie všeobecného zákazu spracúvania citlivých údajov Nariadenie upravuje taxatívnym spôsobom, teda uvedené okolnosti, za ktorých je spracúvanie citlivých údajov zákonné, nie je možné rozširovať.

Výnimky zo zákazu spracúvania citlivých údajov

Všeobecný zákaz spracúvania citlivých údajov sa nebude uplatňovať, ak bude platiť niektorá z týchto podmienok:

- a) *dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz nemôže dotknutá osoba zrušiť;*

³¹ Osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

³² Osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

³³ Osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

Ohľadne požiadaviek na platné udelenie súhlasu odkazujeme na Lekciu 4, avšak upozorňujeme na špecifikum týkajúce sa udelenia súhlasu na spracúvanie citlivých údajov, a to, že súhlas musí byť výslovný (ktorá požiadavka sa neuplatní, pokiaľ nejde o citlivé údaje).

Spracúvať citlivé údaje na základe súhlasu nie je možné vtedy, ak právny predpis ustanovuje, že ani výslovný súhlas dotknutej osoby nie je spôsobilý prelomiť zákaz spracúvania citlivých údajov.

- b) *spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby;*

Tento právny základ rozširuje aktuálnu právu úpravu, keď výslovne uvádza, že spracúvanie citlivých údajov je zákonné, pokiaľ je to nevyhnutné pre plnenie povinností vyplývajúcich z kolektívnej zmluvy.

Spracúvanie citlivých údajov na účely pracovného práva, práva sociálneho poistenia a sociálneho zabezpečenia je možné aj podľa aktuálnej právnej úpravy.³⁴

- c) *spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas;*

Porovnateľný právny základ je obsiahnutý aj v aktuálnej právnej úprave.³⁵

- d) *spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu;*

Porovnateľný právny základ je obsiahnutý aj v aktuálnej právnej úprave.³⁶

- e) *spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;*

a

- f) *spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;*

Porovnateľný právny základ je obsiahnutý aj v aktuálnej právnej úprave.³⁷

- g) *spracúvanie je nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby;*

Ide o rozšírenie a špecifikáciu právneho základu uvedeného v § 14 písm. b) Zákona.

- h) *spracúvanie je nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo*

³⁴ § 14 písm. g) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

³⁵ § 14 písm. c) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

³⁶ § 14 písm. d) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

³⁷ § 14 písm. e) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom;

a

- i) spracúvanie je nevyhnutné z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok, na základe práva Únie alebo práva členského štátu, ktorým sa stanovujú vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby, najmä profesijné tajomstvo;

Tieto dve ustanovenia rozširujú a bližšie špecifikujú právny základ uvedený v aktuálnej právnej úprave.³⁸

Citlivé údaje sa môžu spracúvať na účely uvedené v písm. h), ak tieto údaje spracúva odborník, alebo ak sa spracúvajú v rámci zodpovednosti odborníka, ktorý podlieha povinnosti zachovávať profesijné tajomstvo podľa práva Únie alebo práva členského štátu alebo podľa pravidiel, ktoré stanovili príslušné vnútroštátne orgány, alebo ak údaje spracúva iná osoba, ktorá tiež podlieha povinnosti mlčanlivosti podľa práva Únie alebo práva členského štátu alebo pravidiel, ktoré stanovili príslušné vnútroštátne orgány.

- j) spracúvanie je nevyhnutné na účely archivácie vo verejnom záujme, alebo na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1 na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a určujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

Ide o nové ustanovenie, podľa ktorého je spracúvanie citlivých údajov na uvedené účely zákonné, ak nie je neprimerané vzhľadom na práva dotknutej osoby, a určia sa opatrenia na ich ochranu (napr. minimalizácia údajov, pseudonymizácia a pod.; viď Lekcia 3).

Členské štáty sú oprávnené zachovať alebo zaviesť ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia. Z uvedeného dôvodu môžu vzniknúť odlišnosti v podmienkach spracúvania týchto údajov v právnych poriadkoch rôznych členských štátov, preto subjekty spracúvajúce také údaje v rôznych štátoch by mali venovať náležitú pozornosť týmto nuansám.

Zmeny v spracúvaní citlivých údajov

V súvislosti so spracúvaním citlivých osobných údajov sa povinnosti prevádzkovateľa menia nasledovne:

- v podmienkach slovenskej právnej úpravy je novinkou, že spracúvanie fotografie dotknutej osoby alebo grafického zobrazenia podpisu sa už nebude považovať za spracúvanie osobitných kategórií osobných údajov, pokiaľ sa nebudú spracúvať ako biometrické údaje, t.j. na jedinečnú identifikáciu alebo autentifikáciu osoby (napr. pre účely biometrických cestovných pasov);
- prevádzkovateľ nebude mať oznamovaciu a registračnú povinnosť podľa § 33 a nasl. Zákona³⁹, namiesto toho bude potrebné viesť záznamy podľa čl. 30 Nariadenia;
- v prípade spracúvania osobitnej kategórie osobných údajov vo veľkom rozsahu⁴⁰ bude prevádzkovateľ povinný posúdiť vplyv na ochranu osobných údajov a ustanoviť zodpovednú osobu;

³⁸ § 14 písm. f) zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov

³⁹ Zákon č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov.

⁴⁰ Pojem "vo veľkom rozsahu" nie je definovaný v GDPR, a vzhľadom na priamu aplikovateľnosť Nariadenia Úrad na ochranu osobných údajov nie je oprávnený navrhnuť definíciu tohto pojmu do vnútroštátnej právnej

- prenos osobitnej kategórie osobných údajov tretej strane so sídlom v tretej krajine, ktorá nezaručuje primeranú úroveň ochrany osobných údajov, bude dovolené len s predchádzajúcim výslovným súhlasom dotknutej osoby, ak osobitný zákon neustanovuje inak.

Registre trestov / údaje o priestupkoch

Tieto údaje Nariadenie nekategorizuje ako citlivé údaje. Aj naďalej platí, že prevádzkovateľom na účely spracúvania osobných údajov týkajúcich sa:

- uznania viny za trestné činy a priestupky alebo súvisiacich bezpečnostných opatrení; alebo
- spracúvania osobných údajov v registri trestov podľa osobitného predpisu

môže byť len príslušný štátny orgán ustanovený zákonom.

Každý komplexný register uznania viny za trestné činy sa vedie iba pod kontrolou orgánu verejnej moci.

Spracúvanie národného identifikačného čísla

Členské štáty môžu stanoviť podrobnejšie osobitné podmienky spracúvania národného identifikačného čísla alebo akéhokoľvek iného identifikátora všeobecného uplatnenia (napr. rodné číslo). V uvedenom prípade sa národné identifikačné číslo alebo akýkoľvek iný identifikátor všeobecného uplatnenia používajú len v rámci primeraných záruk v súvislosti s právami a slobodami dotknutej osoby podľa Nariadenia.

Čo ďalej

Ak prevádzkovateľ spracúva citlivé údaje, je nevyhnutné preveriť, že tak robí na základe relevantného právneho základu podľa Nariadenia. Ak je právnym základom súhlas dotknutej osoby, znenie a spôsob udelenia súhlasu je potrebné revidovať a aktualizovať podľa nových podmienok.

Ďalšie informácie

Recitály 51 – 56, 91, 97

Články 4 ods. 13 - 15, 9, 10, 87

úpravy. Zatiaľ sa možno oprieť pri výklade tohto pojmu o recitály 91 a 97 Nariadenia, pokiaľ nebudú publikované usmernenia pracovnej skupiny WP 29 k aplikácii tohto pojmu.

Lekcia 7 z 16

Informačná povinnosť prevádzkovateľa

V texte sa dozviete:

Dôležité zmeny

- Nariadenie podrobnejšie upravuje rozsah informácií, ktoré majú byť poskytnuté dotknutým osobám;
- Nová právna úprava kladie dôraz na jasnosť a zrozumiteľnosť informovania dotknutých osôb.

Compliance: Akčný plán

Prevádzkovatelia by mali:

- revidovať existujúce znenia oboznámení o spracúvaní osobných údajov a zosúladiť ich znenie s Nariadením;
- preukázateľne oboznámiť dotknuté osoby s informáciami požadovanými Nariadením;
- zabezpečiť, aby oboznámenie dotknutých osôb bolo vykonané včas, úplne a zrozumiteľne.

K povinnosti prevádzkovateľa informovať dotknuté osoby

Jednou zo základných zásad spracúvania osobných údajov je zásada transparentnosti. Nariadenie preto ukladá prevádzkovateľom povinnosť prijať vhodné opatrenia s cieľom poskytnúť dotknutým osobám všetky informácie týkajúce sa spracúvania, ktorých okruh Nariadenie taxatívne upravuje.

Zásada transparentnosti si vyžaduje, aby všetky informácie určené verejnosti alebo dotknutej osobe boli stručné, ľahko prístupné a ľahko pochopiteľné, formulované jasne a jednoducho, a navyše ak je to vhodné, ľahko zrakovo vnímateľné. Ak sú informácie určené verejnosti, môžu sa poskytnúť v elektronickej podobe, napríklad prostredníctvom webového sídla. Týka sa to najmä situácií ako je napríklad online reklama, v ktorých veľký počet účastníkov a technologická zložitosť činnosti sťažujú dotknutej osobe zistiť a pochopiť, či osobné údaje, ktoré sa jej týkajú, boli získané, kým a na aké účely.

Informačná povinnosť je upravená pomerne široko, pričom právny rámec poskytovania informácií dotknutej osobe je upravený nasledovne⁴¹:

- informácie sa poskytnú v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho;
- informácie sa môžu podať písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne;
- informácie sa poskytnú dotknutej osobe bezplatne, v prípade neopodstatnených alebo neprimeraných žiadostí dotknutých osôb má však prevádzkovateľ možnosť účtovať primeraný poplatok alebo nekonať (avšak vtedy znáša dôkazné bremeno preukázania, že žiadosť je neopodstatnená alebo neprimeraná);
- prevádzkovateľ je oprávnený žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby;
- určité informácie možno podať v kombinácii so štandardizovanými ikonami, ktoré môže zaviesť Komisia vykonávacím aktom, a ktorých používanie by sa malo vyprofilovať praxou neskôr.

⁴¹ Článok 12 Nariadenia.

Aké informácie je potrebné poskytnúť

V porovnaní s aktuálnou právnou úpravou⁴² budú prevádzkovatelia povinní poskytnúť dotknutým osobám navyše aj tieto informácie⁴³:

- kontaktné údaje⁴⁴ prevádzkovateľa, eventuálne jeho zástupcu a zodpovednej osoby, ak je ustanovená;
- právny základ spracúvania, a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) Nariadenia⁴⁵, aj uvedenie oprávnených záujmov prevádzkovateľa alebo tretej strany;
- doba uchovávanía osobných údajov, prípadne kritériá na jej určenie;
- informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
- konkretizácia práv dotknutej osoby (pre úplnosť uvádzame všetky práva priznané Nariadením dotknutej osobe, t.j. nie len tie, ktoré predošlá právna úprava neobsahovala):
 - právo požadovať od prevádzkovateľa prístup k svojim osobným údajom;
 - právo na opravu, doplnenie, vymazanie alebo obmedzenie spracúvania osobných údajov;
 - právo namietat' proti spracúvaniu;
 - právo na prenosnosť údajov;
 - ak je spracúvanie založené na súhlase, právo kedykoľvek súhlas odvolať;
 - právo podať sťažnosť na príslušný úrad;
 - právo na informáciu o existencii automatizovaného rozhodovania vrátane profilovania.

Zároveň už nie je potrebné informovať dotknutú osobu o sprostredkovateľovi samotným sprostredkovateľom a o forme zverejnenia, ak mali byť osobné údaje zverejnené.

Nariadenie mení aktuálnu slovenskú právnú úpravu⁴⁶ aj v tom, že ak prevádzkovateľ získa osobné údaje priamo od dotknutej osoby na právnom základe osobitného právneho predpisu, na základe medzinárodnej zmluvy alebo na základe priamo vykonateľného právne záväzného aktu Európskej únie (v praxi pôjde napr. o získavanie osobných údajov na pracovnoprávne účely), bude povinný poskytnúť informácie tejto dotknutej osobe. Doteraz platila výnimka z informačnej povinnosti, ktorá sa už nebude uplatňovať.

Kedy sa informácie poskytujú?

Ak prevádzkovateľ získava osobné údaje od dotknutej osoby, informuje ju pri získaní údajov.

⁴² § 15 ods. 1 zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov („Zákon“), upravujúci povinnosť poskytnúť informáciu o totožnosti a kontaktných údajoch prevádzkovateľa, prípadne jeho zástupcu, o účeloch spracúvania, príjemcoch, a prenose údajov do tretích krajín.

⁴³ Článok 13 a 14 Nariadenia.

⁴⁴ Dopusiaľ bola zakotvená povinnosť poskytnúť identifikačné údaje (viď. čl. 10 písm. a), čl. 11 ods. 1, prvé tiré Smernice), transformovaná do Zákona náležitou „identifikačné údaje“ (§ 15 ods. 1 písm. a) Zákona). Táto identifikácia osoby prevádzkovateľa alebo sprostredkovateľa sa rozumela ako požiadavka uviesť u právnickej osoby obchodné meno, IČO a adresu sídla, u fyzických osôb meno, priezvisko a bydlisko, resp. miesto podnikania.

⁴⁵ „Spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa“.

⁴⁶ § 15 ods. 3 Zákona.

Ak prevádzkovateľ nezískava osobné údaje priamo od dotknutej osoby, tieto údaje poskytne:

- v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú;
- ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, najneskôr v čase prvej komunikácie s touto dotknutou osobou; alebo
- ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi, najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú.

V takom prípade je prevádzkovateľ povinný okrem vyššie uvedených informácií dotknutej osobe oznámiť aj informácie o kategóriách osobných údajov, ktoré o nej spracúva, a to, z akého zdroja osobné údaje pochádzajú, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov.

Výnimky z informačnej povinnosti

Prevádzkovateľ nemá povinnosť informovať dotknutú osobu, ak:

- dotknutá osoba už má dané informácie;
- sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, alebo pokiaľ je pravdepodobné, že realizácia informačnej povinnosti znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania; v takých prípadoch prijme prevádzkovateľ vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných informácií verejnosti;
- sa získanie alebo poskytnutie výslovne stanovuje v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a v ktorom sa stanovujú primerané opatrenia na ochranu oprávnených záujmov dotknutej osoby⁴⁷; alebo
- v prípade, keď osobné údaje musia zostať dôverné na základe povinnosti zachovávaní profesijného tajomstva upravenej právom Únie alebo právom členského štátu vrátane povinnosti zachovávať mlčanlivosť vyplývajúcej zo štatútu; ako aj
- v prípadoch, kedy sa na spracúvanie osobných údajov Nariadenie nevzťahuje, tzn.:
 - spracúvanie vykonávané členskými štátmi pri výkone činností, spadajúcich do oblasti spoločnej zahraničnej a bezpečnostnej politiky podľa hlavy V, kapitoly 2 Zmluvy o EÚ;
 - príslušnými orgánmi za účelom prevencie, vyšetrovania, odhaľovania či stíhania trestných činov alebo výkonu trestu, vrátane ochrany pred hrozbami pred verejnú bezpečnosť a ich predchádzania, vid' Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 zo dňa 27. apríla 2016.

Ďalšie spracúvanie

Ak prevádzkovateľ zamýšľa ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli osobné údaje získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a akékoľvek ďalšie relevantné informácie podľa vyššie uvedených informácií. (Pre viac informácií ohľadne zákonnosti ďalšieho spracúvania vid' Lekciu 3.)

⁴⁷ Výluka je doposiaľ zakotvená napr. v § 10 ods. 1 a 2 alebo § 15 ods. 3 Zákona. Subjekty vykonávajúce činnosť podľa osobitných zákonov nie sú vyňaté z pôsobnosti Zákona ako celku, avšak iba z povinností určujúcich základné parametre spracúvania osobných údajov a z povinností vo vzťahu k dotknutým osobám, t.j. z uvedenej informačnej povinnosti a povinnosti súvisiacej s právom dotknutých osôb na prístup k údajom. Napr. väčšina úkonov Polície SR by bola ťažko realizovateľná pri aplikácii povinnosti dotyčnou osobou informovať ihneď pri získaní údajov, alebo na jej žiadosť jej kedykoľvek oznámiť, aké osobné údaje o nej spracúva.

Čo ďalej

Informačná povinnosť prevádzkovateľov voči dotknutým osobám reflektuje na jednu zo základných zásad spracúvania osobných údajov, a to zásadu transparentnosti. Pre zabezpečenie transparentnosti spracúvania je potrebné, aby prevádzkovatelia zrozumiteľným a úplným spôsobom informovali dotknuté osoby o okolnostiach spracúvania. Rozsah informačnej povinnosti je upravený priamo Nariadením, pričom bude výzvou skombinovať povinnosť poskytnúť rozsiahle informácií s požiadavkou Nariadenia, aby oznámenie bolo stručné.

Podľa nášho názoru bude i v budúcnosti pretrvávať istá výkladová náročnosť ustanovenia o informačnej povinnosti, lebo ukladané povinnosti a výnimky z nich pre určité druhy spracúvania alebo prevádzkovateľov nie sú upravené celkom jednoznačne a ich vzájomná previazanosť môže vyvolávať aj naďalej aplikačné nejasnosti.

Ďalšie informácie

Recitály 58, 60 – 63

Články 12 – 14

Lekcia 8 z 16

Práva dotknutých osôb (1. časť)

V texte sa dozviete:

Dôležité zmeny

Prevádzkovatelia budú mať povinnosť:

- oboznámiť sa s obsahom nových práv dotknutých osôb, ktoré im priznáva Nariadenie;
- zaviesť efektívne interné postupy na spracúvanie žiadostí dotknutých osôb, týkajúcich sa spracúvania (napr. povinnosť im na žiadosť vydať kópiu osobných údajov, ktoré o nich spracúvajú a preukázať, že osobné údaje spracúvajú zákonne);
- pripraviť smernice a materiály informujúce o tom, akým spôsobom môžu dotknuté osoby uplatniť svoje práva u prevádzkovateľa.

Dotknuté osoby môžu okrem iného požadovať:

- vymazanie svojich osobných údajov, ak spracúvanie nie je zákonné alebo ak odvolajú súhlas so spracúvaním;
 - ak prevádzkovateľ spracúvané údaje zverejnil (napr. v súvislosti so službami sociálnych sietí), v prípade opodstatnenej žiadosti o vymazanie je povinný postúpiť žiadosť všetkým, ktorí zverejnené údaje spracúvajú. Ide o mimoriadne široko koncipovanú povinnosť, ktorej praktické uplatnenie bude zrejme predmetom testovania;
- obmedzenie spracúvania svojich údajov, napr. počas vybavenia sťažnosti týkajúcej sa spracúvania, alebo ak dotknutá osoba z iného dôvodu nežiada vymazanie.

Compliance: Akčný plán

Prevádzkovatelia by mali:

- vytvoriť interné postupy na včasné vybavovanie žiadostí dotknutých osôb, týkajúcich sa zákonnosti spracúvania ich osobných údajov (najmä zákazníkov, prípadne zamestnancov);
- zaškoliť tím zamestnancov vybavujúci žiadosti dotknutých osôb ohľadne ich práv a povinností;
- pripraviť štandardizované vzory odpovedí na žiadosti, vytvoriť procesy na dodržanie zákonných lehôt pri vybavovaní, zabezpečiť, aby dotknutým osobám boli poskytnuté všetky informácie, na ktoré majú nárok;
- zabezpečiť, aby spôsob vybavovania žiadostí spĺňal technické požiadavky podľa Nariadenia;
- preveriť, či v dôsledku informačnej povinnosti nebude porušené právo na súkromie inej dotknutej osoby a vytvoriť procesy na minimalizovanie takých rizík;
- zabezpečiť, aby bolo technicky a organizačne možné vybaviť žiadosť o vymazanie alebo obmedzenie spracúvania osobných údajov v systémoch prevádzkovateľa.

K právam dotknutej osoby

Nariadenie rozširuje a spresňuje práva dotknutých osôb. Pre úplnosť uvádzame zoznam všetkých práv dotknutých osôb tak, ako ich uvádza Nariadenie v Kapitole III a pre rozsah matérie sa budeme právam dotknutých osôb venovať v dvoch lekciách.

Právo na prístup k údajom

Na rozdiel od informačnej povinnosti prevádzkovateľa, o ktorej sme informovali v Lekcii 7, právo na prístup k údajom je koncipované odlišne: kým informačná povinnosť sa vzťahuje na prevádzkovateľa a ukladá mu, aby automaticky, t.j. bez osobitnej žiadosti dotknutej osoby, jej poskytol určité údaje, právo na prístup k údajom je koncipované nezávisle od toho, či prevádzkovateľ splnil svoju informačnú povinnosť, a toto právo garantuje dotknutej osobe jednak prístup k svojim údajom a jednak doplňujúce informácie o nich, a to na základe jej žiadosti.

Obsahom práva na prístup k údajom je právo dotknutej osoby získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak áno, má právo získať prístup k svojim osobným údajom (t.j. ich kópiu) a ďalšie informácie⁴⁸ týkajúce sa spracúvania.

Kópiu osobných údajov, ktoré sa spracúvajú, prevádzkovateľ poskytne bezplatne. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom s tým spojeným. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob. Uvedená požiadavka by mohla spôsobiť navýšenie nákladov pre osoby, ktoré spracúvajú údaje v papierovej podobe alebo v špeciálnych formátoch, ktoré bude potrebné konvertovať do všeobecne čitateľnej elektronickej formy. V súvislosti s tým môžu teda vzniknúť náklady na softvérové a hardvérové vybavenie, administratívny personál a pod.

Podľa recitálu 63 prevádzkovateľ môže poskytnúť prístup na diaľku k bezpečnému systému, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom. To znamená, že ak napr. prevádzkovateľ predpokladá väčšiu frekvenciu žiadostí dotknutých osôb o prístup k údajom, môže túto povinnosť splniť tak, že vytvorí bezpečnú databázu údajov, do ktorej bude mať dotknutá osoba prístup v rozsahu vlastných osobných údajov. Uvedený návrh má však skôr odporúčací než záväzný charakter.

Právo dotknutej osoby na prístup k svojim osobným údajom zodpovedá povinnosti prevádzkovateľa, aby zaviedol interné postupy a organizačné a technické opatrenia na to, aby žiadostiam dotknutých osôb bol schopný vyhovieť v zákonnej lehote, ktorá je určená „bez zbytočného odkladu“, avšak spravidla 1 mesiac od doručenia žiadosti a ktorá sa v odôvodnených prípadoch môže predĺžiť o ďalšie dva mesiace.

Prevádzkovatelia by mali preto okrem iného zaviesť pracovné postupy, ako v týchto prípadoch postupovať, zaškoliť personál na vybavovanie žiadostí, poučiť personál o povinnostiach súvisiacich s ochranou osobných údajov, napr. povinnosti mlčanlivosti, a zabezpečiť, aby mal zodpovedajúce technické a organizačné vybavenie na to, aby bol schopný vybavovať žiadosti vo všeobecne čitateľnej elektronickej forme.

Výnimky z práva na prístup k údajom

Nariadenie ďalej upravuje určité výnimky z práva na prístup k údajom:

- v prvom rade, právo získať kópiu údajov nesmie mať nepriaznivé dôsledky na práva a slobody iných, ani obchodné tajomstvo alebo práva duševného vlastníctva/autorské práva týkajúce sa softvéru. Ak by sa splnením práva na prístup k údajom mali porušiť práva inej

⁴⁸ Tzn.: a. účely spracúvania; b. kategórie dotknutých osobných údajov; c. príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie; d. ak je to možné, predpokladaná doba uchovávaní osobných údajov alebo, ak to nie je možné, kritériá na jej určenie; e. existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietat proti takémuto spracúvaniu; f. právo podať sťažnosť dozornému orgánu; g. ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj; h. existencia automatizovaného rozhodovania vrátane profilovania informácie o použítom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu; i. ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách.

osoby, je potrebné prijať také organizačné a technické opatrenia, aby k porušeniu nedošlo. Výsledkom zohľadnenia týchto prvkov by však nemalo byť odmietnutie poskytnutia akýchkoľvek informácií dotknutej osobe. Keďže tu proti sebe stoja minimálne dve rovnocenné práva alebo slobody⁴⁹, v prípade sporu je oprávnený s konečnou platnosťou rozhodnúť príslušný súd.

- ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií, môže požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka; uvedené však neznamena, že ak by vybavenie žiadosti dotknutej osoby malo byť časovo a rozsahovo náročné, že by prevádzkovateľ nemal byť povinný vyhovieť aj takej žiadosti;
- žiadosť dotknutej osoby by mala byť motivovaná zistením zákonnosti spracúvania jej osobných údajov; žiadosti podanej na iný účel než kvôli ochrane jej osobných údajov by prevádzkovateľ nemusel vyhovieť.

Prevádzkovateľ by mal použiť všetky primerané opatrenia na overenie totožnosti dotknutej osoby, ktorá žiada o prístup k údajom, najmä v súvislosti s on-line službami a on-line identifikátormi. Prevádzkovateľ by však nemal uchovávať osobné údaje len preto, aby bol schopný reagovať na prípadné žiadosti.

Právo na opravu

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a za týmto účelom môže poskytnúť doplnkové vyhlásenie.

Právo na vymazanie (právo „byť zabudnutý“)

Právo „byť zabudnutý“ vyvolalo ešte počas legislatívneho procesu prípravy Nariadenia mnoho emócií, a to predovšetkým v súvislosti s poskytovaním služieb informačnej spoločnosti spoločnosťami ako Google, Facebook atď. Služby poskytované týmito a inými spoločnosťami sú špecifické v tom, že spracúvajú veľmi veľké množstvo osobných údajov dotknutých osôb, pričom ich ukladajú na svojich serveroch, ďalej s nimi nakladajú a vzhľadom na rozsah údajov a spracovateľských operácií predpokladali mnoho úskalí súvisiacich s právom byť zabudnutý. Právo byť zabudnutý, doteraz upravené len judikatúrne,⁵⁰ sa však do finálneho znenia Nariadenia dostalo, a to v nasledovnom obsahu:

Dotknutá osoba má právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, ak sú splnené podmienky upravené Nariadením. Tomuto právu zodpovedá povinnosť prevádzkovateľa bez zbytočného odkladu vymazať osobné údaje dotknutej osoby, ak je splnený niektorý z týchto dôvodov:

- osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
Podľa tejto premisy, ak sa osobné údaje získali alebo spracúvali napr. na účel priameho marketingu, ale prevádzkovateľ zmenil obchodnú činnosť a viac neorientuje svoje marketingové aktivity na dotknutú osobu, jej osobné údaje by mal vymazať.
- dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva⁵¹, a ak neexistuje iný právny základ pre spracúvanie;

⁴⁹ Právo dotknutej osoby na prístup k údajom a právo inej osoby napr. na ochranu osobnosti, na súkromie, listové tajomstvo, obchodné tajomstvo, autorské právo a pod.

⁵⁰ Na úrovni EU vid' najmä rozsudok SDEU (veľkého senátu) z 13. 5. 2014, vo veci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

⁵¹ Podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a) Nariadenia.

Odvolaie súhlasu nespôsobuje nezákonnosť spracúvania, ku ktorému došlo pred jeho odvolaním. (Viac k súhlasu pozri Lekciu 4.)

- dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 Nariadenia⁵² a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2 Nariadenia⁵³;

Právom namietat' spracúvanie sa budeme zaoberat' v ďalšej lekcii.

- osobné údaje sa spracúvali nezákonne;

Uvedený dôvod je značne všeobecný a natoľko široko koncipovaný, že bude pod neho možné subsumovať veľké množstvo žiadostí dotknutých osôb o vymazanie údajov. Riziko s ním spojené spočíva v tom, že bude na prevádzkovateľovi, aby preukázal, že údaje spracúva zákonne (k zákonnosti spracúvania pozri Lekciu 3). Teda to, že dotknutá osoba bude tvrdiť, že údaje sa spracúvajú nezákonne, bude postačovať na to, aby dôkazné bremeno preukázania opaku sa presunulo na prevádzkovateľa. Ten by preto mal zabezpečiť, aby nemal dôkaznú núdzu na preukázanie zákonnosti, a aby o spracúvaní a právnych základoch vzťahujúcich sa naň viedol dostatočnú evidenciu.

Bude zaujímavé sledovať, ako sa členské štáty postavia k implementácii výnimiek⁵⁴ do vlastných právnych poriadkov. Je samozrejmosťou, že prevádzkovatelia, ktorí budú spracúvať údaje na cezhraničnej báze, by mali byť s týmito lokálnymi špecifikami oboznámení, aby zabezpečili zákonnosť spracúvania v každom štáte Únie.

- osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;

Uvedené by sa vzťahovalo napr. na prípad, ak doposiaľ spracúvané údaje majú byť podľa právneho poriadku vymazané po uplynutí určitej doby (a zároveň sa neaplikuje výnimka oprávňujúca spracúvanie napr. na účely archivácie vo verejnom záujme – vid'. nižšie).

- osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 Nariadenia.

Uvedené právo je relevantné najmä v situácii, kedy dotknutá osoba dala súhlas na spracúvanie osobných údajov ako dieťa, a nebola si plne vedomá rizík spojených so spracúvaním, a neskôr chce takéto osobné údaje odstrániť, najmä z internetu. Dotknutá osoba by mala mať možnosť uplatniť uvedené právo bez ohľadu na skutočnosť, že už nie je dieťa.

Špecifiká súvisiace so zverejnenými údajmi

Ak prevádzkovateľ zverejnil osobné údaje a zároveň je povinný vymazať osobné údaje vzhľadom na vyššie uvedené pravidlá, je povinný prijať primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky. Uvedené opatrenia sa prijímú so zreteľom na dostupnú technológiu a náklady.

⁵² Dotknutá osoba má právo kedykoľvek namietat' z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané z dôvodu, že spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi alebo z dôvodu, že spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa, vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach.

⁵³ Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietat' proti spracúvaniu osobných údajov, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom.

⁵⁴ Článok 23 Nariadenia.

Uvedené ustanovenie odzrkadľuje snáď jednu z najrevolučnejších zmien v spracúvaní osobných údajov, ktoré Nariadenie prináša. Toto ustanovenie v zásade ukladá povinnosť prevádzkovateľovi, ktorý spracúval osobné údaje dotknutej osoby, a v rámci tohto spracúvania došlo aj k ich zverejneniu, aby v prípade, ak dotknutá osoba odôvodnene požiadala o vymazanie svojich údajov,

- aktívne prijal zodpovedajúce opatrenia, vrátane technických opatrení, a
- účinne informoval prevádzkovateľov, ktorí predmetné údaje spracúvajú, že dotknutá osoba požaduje vymazanie svojich údajov, ich kópie a repliky,
- to všetko s ohľadom na dostupnú technológiu a náklady.

Podľa recitálu 66 bolo uvedené opatrenie prijaté v neposlednom rade na posilnenie práva byť zabudnutý on-line prostredím internetu. Nie je však zatiaľ celkom zrejmé, akým spôsobom prevádzkovateľ vôbec určí okruh prevádzkovateľov, ktorí spracúvajú osobné údaje, ktoré sa stali verejnými⁵⁵, teda akým spôsobom identifikuje konkrétnych prevádzkovateľov, ktorých by mal o žiadosti o vymazanie údajov notifikovať. Bude teda otázkou ďalšieho testovania aplikácie tohto ustanovenia v praxi, akým spôsobom bude dodržiavanie toto ustanovenia vykonateľné, a do akej miery bude právo dotknutej osoby zodpovedajúce tejto povinnosti skutočne realizovateľné.

Výnimky z práva na vymazanie

Vyššie uvedené povinnosti prevádzkovateľov sa neuplatnia, pokiaľ je spracúvanie potrebné:

- na uplatnenie práva na slobodu prejavu a na informácie;
- na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- z dôvodov verejného záujmu v oblasti verejného zdravia⁵⁶;
- na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1 Nariadenia, pokiaľ je pravdepodobné, že právo na vymazanie znemožní alebo závažným spôsobom sťažuje dosiahnutie cieľov takejto spracúvania, alebo
- na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov⁵⁷.

Právo na obmedzenie spracúvania

Obmedzenie spracúvania⁵⁸ znamená, že prevádzkovateľ je oprávnený osobné údaje iba uchovávať, bez toho, aby ich akokoľvek inak spracúval. Ak sa údaje spracúvajú automatizovane, je potrebné prijať adekvátne technické opatrenia za týmto účelom (napr. stiahnutie z on-line prostredia). Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:

- dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov;

⁵⁵ Pre úplnosť uvádzame, že po účinnosti Nariadenia už nebude zákonné spracúvanie už zverejnených údajov podľa doterajšieho ustanovenia § 10 ods. 3 písm. e) zákona č. 122/2013 Z.z. Podľa Nariadenia je spracúvanie zverejnených údajov, ak nebude existovať iný primeraný právny základ pre spracúvanie takých údajov, v rozpore so zásadou zákonnosti, spravodlivosti a transparentnosti a zásadou obmedzenia účelu a kompatibility účelu.

⁵⁶ V súlade s článkom 9 ods. 2 písm. h) a i) Nariadenia, ako aj článkom 9 ods. 3 Nariadenia.

⁵⁷ Slovenský oficiálny preklad, publikovaný EU, znie „na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov“; nezdá sa však presný, nevystihuje vecnú podstatu a miestnu odbornú terminológiu.

⁵⁸ Článok 4 ods. 3 Nariadenia.

- spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
- prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;
- dotknutá osoba namietala voči spracúvaniu podľa článku 21 ods. 1 Nariadenia, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sa spracúvanie obmedzilo podľa vyššie uvedených pravidiel, takéto osobné údaje sa s výnimkou uchovávanía spracúvajú len so súhlasom dotknutej osoby alebo na preukázovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo na ochranu práv inej fyzickej alebo právnickej osoby, alebo z dôvodov dôležitého verejného záujmu Únie alebo členského štátu.

Dotknutú osobu, ktorá dosiahla obmedzenie spracúvania, prevádzkovateľ informuje pred tým, ako bude obmedzenie spracúvania zrušené.

Okrem toho

V súvislosti s právom na opravu, vymazanie aj obmedzenie je prevádzkovateľ povinný oznámiť každému príjemcovi, ktorému osobné údaje poskytol, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania. Uvedenú povinnosť nemá, pokiaľ sa to ukáže ako nemožné alebo si to vyžaduje neprimerané úsilie. Prevádzkovateľ o týchto príjemcoch informuje dotknutú osobu, ak to dotknutá osoba požaduje.

Čo ďalej

V súvislosti s uvedenými oprávneniami má prevádzkovateľ extenzívne povinnosti, na ktoré odkazujeme v časti *Compliance: Akčný plán* vyššie. Za účelom zabezpečenia súladu s Nariadením sa prevádzkovateľom odporúča konzultovať vnútorné procesy spracúvania osobných údajov s právnymi poradcami, prípadne IT odborníkmi.

Ďalšie informácie

Recitály 63 - 69

Články 15 - 19

Lekcia 9 z 16

Práva dotknutých osôb (2. časť)

V texte sa dozviete:

Dôležité zmeny

- Právo na prenosnosť údajov oprávňuje dotknutú osobu, aby prevádzkovateľ preniesol jej osobné údaje priamo k inému prevádzkovateľovi;
- Obsah práva dotknutých osôb namietaj voči spracúvaniu u prevádzkovateľa sa mení; o tomto práve musia byť dotknuté osoby riadne informované;
- Dotknutá osoba má právo, aby sa na ňu nevzťahovalo rozhodnutie, ktoré:
 - je založené iba na automatizovanom spracúvaní (vrátane profilovania); a
 - má pre ňu právne účinky alebo porovnateľne významné účinky.

Compliance: Akčný plán

Prevádzkovatelia majú:

- zabezpečiť, aby nimi spracúvané osobné údaje boli jednoducho prenositeľné v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte;
- overiť, že dotknuté osoby boli riadne a pri prvej komunikácii informované o práve namietaj spracúvanie;
- preveriť, či dochádza k profilovaniu a ak áno, zabezpečiť, aby preň existoval relevantný právny základ.

K právam dotknutej osoby

Právo na prenosnosť údajov

Právo na prenosnosť údajov Nariadenie zakotvuje jednak ako právo dotknutej osoby:

- na získanie svojich osobných údajov a na ich následný prenos inému prevádzkovateľovi⁵⁹; a tiež
- na prenos osobných údajov jedným prevádzkovateľom priamo druhému prevádzkovateľovi.

V prvom prípade právo na získanie osobných údajov môže pripomínať skôr spomínané *právo na prístup k údajom* (pozri Lekciu 8). Právo na získanie údajov je však upravené špecifickejšie, s týmito rozdielmi:

- kým právo na prístup k údajom oprávňuje dotknutú osobu na prístup k svojim údajom (t.j. okrem iného aj na získanie ich kópie) v bežne používanej elektronickej forme,
- právo na prenosnosť je koncipované užšie a detailnejšie v tom zmysle, že oprávňuje dotknutú osobu na získanie svojich údajov v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte. Po technickej stránke je teda špecifickejšie a náročnejšie pre prevádzkovateľa, pretože musí zabezpečiť, aby osobné údaje odovzdal v štruktúrovanom, t.j. systematickom, organizovanom, formáte⁶⁰.

⁵⁹ Uplatňovaním tohto práva nie je dotknutý článok 17 Nariadenia, upravujúci právo na vymazanie. Takisto, uvedené právo sa nevzťahuje na spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

⁶⁰ Recitál 68 spomína aj „interoperabilný formát“, avšak ide zrejme skôr o odporúčanie, než o záväzný charakter tejto dikcie.

Právo na prenosnosť údajov sa však môže uplatniť iba vtedy, ak:

- ide o údaje, ktoré dotknutá osoba sama poskytla prevádzkovateľovi;
- spracúvanie sa zakladá na súhlase alebo výslovnom súhlase (pri osobitných kategóriách údajov), prípadne je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy, a
- ak sa spracúvanie vykonáva automatizovanými prostriedkami (t.j. nie v listinnej forme; pre porovnanie – právo na prístup k údajom sa vzťahuje aj na údaje spracúvané v listinnej forme).

Ak nie sú splnené vyššie uvedené podmienky, dotknutá osoba sa nemôže tohto práva domáhať. Ak by napr. prevádzkovateľ získal osobné údaje od iného prevádzkovateľa, a nie priamo od dotknutej osoby, tak dotknutá osoba by nemala právo na prenosnosť údajov, ale iba právo na prístup k údajom.⁶¹

Ak dotknutá osoba získa svoje osobné údaje v rámci práva na prenosnosť údajov, je oprávnená ich následne sama preniesť ďalšiemu prevádzkovateľovi. To však nesmie mať nepriaznivé dôsledky na práva a slobody iných. To znamená, že ak by právo na prenosnosť údajov malo negatívny efekt na práva a slobody iných, k prenosu (resp. k poskytnutiu osobných údajov dotknutej osobe) by nemalo dôjsť. Táto situácia by mohla nastať napríklad v reáliách sociálnych sietí, kedy popri údajoch dotknutej osoby sa spracúvajú osobné údaje iných osôb (napr. v rámci vzájomnej komunikácie). Pri uplatnení práva na prenosnosť nesmú byť dotknuté práva inej osoby.

Podstatná zmena vnesená novým konceptom práva na prenosnosť údajov tkvie v tom, že dotknutá osoba môže tiež prevádzkovateľa žiadať, aby osobné údaje neodovzdal jej, ale aby ich preniesol priamo k inému prevádzkovateľovi. V praxi je toto právo využiteľné napr. vtedy, ak dotknutá osoba zmení dodávateľa určitých (napr. telekomunikačných) služieb. V takom prípade je dotknutá osoba zbavená administratívnej a technickej záťaže spojenej s prenosom svojich osobných údajov k inému prevádzkovateľovi, keďže túto povinnosť má priamo pôvodný prevádzkovateľ, a to v „štruktúrovanom, bežne používanom a strojovo čitateľnom formáte“. Podmienkou je tu iba technická zrealizovateľnosť tejto požiadavky.

Právo namietať spracúvanie osobných údajov

Právo namietať spracúvanie osobných údajov Nariadenie priznáva dotknutej osobe iba v určitých špecifických prípadoch. Dotknutá osoba nie je oprávnená namietať akékoľvek spracúvanie, ale iba v prípadoch, ak ide o:

1. spracúvanie, ktoré je nevyhnutné:
 - a. na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi; alebo
 - b. na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana; vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach.

V týchto prípadoch je dotknutá osoba oprávnená kedykoľvek namietať spracúvanie, avšak iba „z dôvodov týkajúcich sa jej konkrétnej situácie“. Bremeno tvrdenia, prečo by spracúvanie malo byť zastavené, je tak na strane dotknutej osoby, ktorá musí uviesť špecifické okolnosti týkajúce sa konkrétne jej osoby alebo situácie.

⁶¹ Pre praktický život však tento formalistický prístup komunitárnej či inej normotvorby nemá zásadný význam a je samoučelom. Dotknutá osoba má a bude mať nárok – cez dikciu aktuálneho slovenského zákona v § 15 – na spracúvané osobné údaje, a nie iba na informáciu, že je spracúvané jej meno, priezvisko, dátum narodenia, bydlisko atď. Nič teda nebráni tomu, aby dotknutá osoba takto získané údaje sama poskytla, „preniesla“, inému prevádzkovateľovi.

Ak dotknutá osoba podala námietku a uviedla relevantné dôvody, prevádzkovateľ ďalej nesmie spracúvať osobné údaje, iba ak by preukázal

- nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo
- dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

V takom prípade by prevádzkovateľ mohol v spracúvaní pokračovať. To znamená, že ak oprávnená osoba podá námietku z vyššie uvedených dôvodov, dôkazné bremeno sa presúva na prevádzkovateľa, aby preukázal existenciu dôvodov, ktoré ho oprávňujú ďalej spracúvať osobné údaje na dané účely.

O práve namietať z vyššie uvedených dôvodov sa musí dotknutá osoba výslovne upozorniť, a to najneskôr pri prvej komunikácii. Toto právo musí byť uvedené jasne a oddelene od akýchkoľvek iných informácií prevádzkovateľa.

2. spracúvanie na účely priameho marketingu;

Dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré sa jej týkajú, pre účely priameho marketingu, vrátane profilovania v rozsahu, v akom s ním súvisí.

Jedná sa o absolútne právo dotknutej osoby, a to bez toho, aby bola povinná čokoľvek ďalšie tvrdiť alebo preukazovať. Inými slovami, ak si dotknutá osoba nepraje, aby sa jej osobné údaje spracúvali na tento účel, stačí, že podá námietku u prevádzkovateľa, ktorý je bez ďalšieho povinný spracúvanie na tento účel ukončiť. Dotknutá osoba nemá povinnosť tvrdiť dôvody alebo situácie hodné osobitného zreteľa, ako je to v bode 1 vyššie. Zároveň neexistuje spôsob, ktorým by sa prevádzkovateľ mohol tejto námietke účinne brániť (napr. tvrdením, že jeho oprávnený záujem prevažuje nad právami a záujmami dotknutej osoby). Akonáhle teda dotknutá osoba doručí prevádzkovateľovi námietku týkajúcu sa spracúvania osobných údajov na účel priameho marketingu, prevádzkovateľ nesmie v spracúvaní na tento účel ďalej pokračovať. Ak však príslušné údaje spracúva na iný účel na základe iného príliehavého právneho základu, také spracúvanie dotknuté nie je.

Podobne ako v bode 1, prevádzkovateľ musí dotknutú osobu na uvedené právo výslovne upozorniť, a to najneskôr pri prvej komunikácii s ňou, pričom toto právo sa má prezentovať jasne a oddelene od akýchkoľvek iných informácií;

3. spracúvanie na účely vedeckého alebo historického výskumu či na štatistické účely;

Ak sa osobné údaje spracúvajú na uvedené účely, má dotknutá osoba právo namietať z dôvodov týkajúcich sa jej konkrétnej situácie. Toto právo však nemá, ak je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

Podobne ako v bode 1 musí dotknutá osoba uviesť relevantné dôvody týkajúce sa jej konkrétnej situácie, aby spracúvanie bolo ukončené.

Na rozdiel od námietok z dôvodov uvedených v bodoch 1 a 2, nemusí byť dotknutá osoba na právo namietať z tohto dôvodu upozornená. Námietku je možné vzniesť aj automatizovanými prostriedkami s použitím technických špecifikácií.

Automatizované individuálne rozhodovanie⁶² a profilovanie⁶³

Nariadenie poskytuje dotknutým osobám ochranu pred rizikom potenciálne nepriaznivého rozhodnutia, ktoré bolo prijaté bez akejkoľvek ľudskej intervencie, t.j. výlučne na základe automatizovaného spracúvania⁶⁴. Recitál 71 uvádza ako príklad takého rozhodnutia automatické zamietnutie on-line žiadosti o úver alebo elektronické postupy prijímania pracovníkov bez akéhokoľvek ľudského zásahu. Nariadenie priznáva dotknutej osobe právo, aby sa na ňu nevzťahovalo rozhodnutie, ktoré

- je založené výlučne na automatizovanom spracúvaní, vrátane profilovania; a
- ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.

Uvedená ochrana proti automatizovanému individuálnemu rozhodovaniu sa neuplatní, ak

- a) také rozhodovanie je nevyhnutné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom;
- b) povolené právom Únie alebo právom členského štátu, ktorému prevádzkovateľ podlieha a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby⁶⁵, alebo
- c) založené na výslovnom súhlase dotknutej osoby.

V prípadoch sub a) a c) je prevádzkovateľ povinný zaviesť vhodné opatrenia za účelom ochrany práv dotknutej osoby. Minimálnym štandardom je, že zabezpečí, aspoň možnosť ľudskej intervencie zo strany prevádzkovateľa, t.j. aby rozhodnutie, ktoré bolo prijaté automatizovane, mohol preveriť človek, aby dotknutá osoba mohla vyjadriť svoje stanovisko k okolnostiam prijatia rozhodnutia, aby jej bolo poskytnuté odôvodnenie rozhodnutia a aby mohla právne napadnúť jeho správnosť.

Automatizované rozhodovanie však nesmie byť založené na osobitných kategóriách osobných údajov (t.j. odhaľujúcich rasový či etnický pôvod, politické názory, náboženské vierovyznanie čo filozofické presvedčenie alebo členstvo v odboroch, zdravotný stav, sexuálny život či orientáciu, vid'. čl. 9 ods. 1 Nariadenia), s výnimkou prípadov, kedy by k nemu dochádzalo na základe

- výslovného súhlasu dotknutej osoby, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že uvedený zákaz nemôže dotknutá osoba zrušiť;
- významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby;

⁶² O automatizované individuálne rozhodovanie ide vtedy, ak sa o určitej skutočnosti rozhoduje automatizovaným spôsobom, t.j. bez zásahu ľudského faktora, napr. na základe určitých vopred určených algoritmov.

⁶³ Profilovanie je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom (čl. 4 ods. 4 Nariadenia). Podľa recitálu 71 Nariadenia by mal prevádzkovateľ používať na účely profilovania primerané matematické alebo štatistické postupy, prijať technické a organizačné opatrenia vhodné na to, aby sa predovšetkým zabezpečilo, že faktory, ktoré vedú k nesprávnosti osobných údajov, sa opraví a riziko chýb sa minimalizuje, zabezpečiť osobné údaje tak, aby sa zohľadnili súvisiace potenciálne riziká pre záujmy a práva dotknutej osoby a aby sa okrem iného zabránilo diskriminačným účinkom na fyzické osoby na základe rasového alebo etnického pôvodu, politického názoru, náboženstva alebo presvedčenia, členstva v odborových organizáciách, genetického alebo zdravotného stavu či sexuálnej orientácie, alebo účinkom, ktoré vedú k opatreniam majúcim takéto účinky.

⁶⁴ Zatiaľ upravené v čl. 15 Smernice v podobe zákazu rozhodnutia prijatého výlučne na automatizovanom spracúvaní údajov určených k hodnoteniu určitých rysov osobnosti dotknutej osoby, napr. pracovného výkonu, dôveryhodnosti, spoľahlivosti, správania atď. Výnimka je umožnená pre rozhodnutia v rámci uzavierania alebo plnenia zmluvy z podnetu dotknutej osoby alebo ak je to povolené právnym predpisom, ktorý tiež upresňuje opatrenia zabezpečujúce ochranu oprávnených záujmov dotknutej osoby.

⁶⁵ Napr. na účely monitorovania podvodov a daňových únikov a ich predchádzania, ktoré sa uskutočňuje v súlade s právnym predpismi, normami a odporúčaniami inštitúcií Únie alebo vnútroštátnych orgánov dozoru, a na zaistenie bezpečnosti a spoľahlivosti služby poskytovanej zo strany prevádzkovateľa

a pokiaľ boli zavedené vhodné opatrenia na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby.

Čo ďalej

Prevádzkovatelia by sa mali na zabezpečenie súladu s Nariadením v rozsahu práva na prenosnosť, práva namietat' a práv spojených s automatizovaným rozhodovaním a profilovaním ubezpečiť, nakoľko budú tejto úprave podliehať (napr. do akej miery využívajú profilovanie), a podľa toho nastaviť vnútorné procesy týkajúce sa spracúvania, ako aj procesy komunikácie s dotknutými osobami.

Tiež bude potrebné sledovať ďalšiu Únijnú a vnútroštátnu legislatívu, pretože rozsah práv a oprávnení dotknutých osôb a zodpovedajúcich povinností prevádzkovateľov môže byť modifikovaný v záujme o.i. ochrany dotknutých osôb alebo práv iných, či s cieľom zabezpečiť vymáhanie občianskoprávných nárokov.

Ďalšie informácie

Recitály 68 – 72

Články 4 ods. 4, 20 – 23

Lekcia 10 z 16

Bezpečnosť osobných údajov a porušenie ich ochrany

V texte sa dozviete:

Dôležité zmeny

- Prevádzkovatelia budú mať dvojakú oznamovaciu povinnosť v prípade porušenia ochrany osobných údajov, a to jednak voči dozornému úradu, a tiež voči dotknutým osobám;
- Prevádzkovatelia budú povinní viesť evidenciu porušení ochrany osobných údajov.

Compliance: Akčný plán

- Prevádzkovatelia aj sprostredkovatelia musia zaviesť vhodné bezpečnostné opatrenia na ochranu dát pri spracúvaní;
- Za týmto účelom je potrebné dôsledne posúdiť okolností spracúvania, a to v spolupráci s IT technikmi (napr. pre účely zavedenia šifrovania údajov);
- Odporúča sa zaviesť interné smernice pre prípad zistenia porušenia ochrany údajov;
- Odporúča sa zvážiť poistenie následkov prípadného porušenia ochrany osobných údajov;
- Zmluvy s dodávateľmi, ak zahŕňajú spracúvanie osobných údajov (napr. výplatné pásky, účtovníctvo), by mali obsahovať zodpovednosť za bezpečnosť osobných údajov⁶⁶.

Bezpečnosť osobných údajov

Nariadenie stanovuje minimálny štandard ochrany osobných údajov pri ich spracúvaní prostredníctvom niekoľkých inštitútov, resp. opatrení, ktoré je prevádzkovateľ povinný prijať⁶⁷. Z Nariadením sledovaného zámeru je zrejmé, že hlavným účelom novej legislatívy upravujúcej spracúvanie osobných údajov je zabezpečenie ich bezpečnosti pri spracúvaní a minimalizácia rizík – nielen pred následkami ľudského konania (úmyselného, nedbanlivostného, interného u prevádzkovateľa či sprostredkovateľa alebo vonkajšieho, mimo týchto subjektov), ale i prírodných síl alebo zlyhania techniky – spojených s rôznymi spracovateľskými operáciami.

Nariadenie upravuje povinnosti prevádzkovateľa súvisiace s bezpečnosťou osobných údajov tak, že prevádzkovateľ (a tiež sprostredkovateľ) je povinný prijať vhodné technické a organizačné opatrenia s cieľom zaistiť náležitú úroveň bezpečnosti, vrátane dôvernosti, zodpovedajúcu tomuto riziku. Tieto opatrenia môžu zahŕňať aj:

- pseudonymizáciu a šifrovanie osobných údajov;
- schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Nariadenie uvádza vyššie uvedené bezpečnostné opatrenia výlučne ako príklady, t.j. prevádzkovateľ môže určiť aj iné vhodnejšie opatrenia na zabezpečenie bezpečnosti údajov, podľa

⁶⁶ Zmluva o spracúvaní sa považuje za súčasť bezpečnostných opatrení.

⁶⁷ Ide najmä o povinnosť viesť záznamy o spracovateľských činnostiach, povinnosť prijať primerané technické a organizačné opatrenia, oznamovaciu povinnosť v prípade porušenia ochrany osobných údajov, posúdenie vplyvu na ochranu osobných údajov; predchádzajúce konzultácie s dozorným orgánom a pod.

jeho špecifických podmienok. Nariadenie stanovuje, aký stav musia prevádzkovatelia a sprostredkovatelia docieľiť, ale nie, akými prostriedkami. Tieto opatrenia však musí zaviesť so zreteľom na:

- *najnovšie poznatky techniky* – za účelom zistenia, aké možnosti ochrany osobných údajov v momente určovania bezpečnostných opatrení existujú, je vhodné, aby prevádzkovateľ konzultoval aktuálne prostriedky ochrany s IT špecialistami. Opatrenia musia vykazovať náležitú odbornú úroveň. Tieto je potom vhodné v pravidelných intervaloch obnovovať; ak by sa totiž v priebehu spracúvania osobných údajov úroveň poznatkov o prostriedkoch ochrany rozvinula, prevádzkovateľ by z dôvodu obsolétosti ochranných systémov nemusel mať zabezpečený súlad s Nariadením;
- *náklady na vykonanie opatrení* – pri prijímaní konkrétnych opatrení prevádzkovateľ zvažuje aj ich nákladovosť. Argumentom nie je, že bezpečnostné opatrenia neboli prijaté vzhľadom na ich finančnú, personálnu či časovú náročnosť;
- *povahu, rozsah, kontext a účely spracúvania* – pri určovaní, aké bezpečnostné opatrenia prevádzkovateľ prijme, samozrejme musí dôkladne zvážiť všetky okolnosti spracúvania osobných údajov v čase, kedy k spracúvaniu dochádza; tieto okolnosti je potrebné priebežne prehodnocovať vzhľadom na meniace sa podmienky spracúvania;
- *riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb* – ide o dôležitý aspekt spracúvania, pričom od prevádzkovateľa sa vyžaduje, aby urobil vyhodnotenie akýchkoľvek možných bezpečnostných rizík spojených so spracúvaním, ktoré by mohli mať negatívny dopad na práva a slobody fyzických osôb. Toto posúdenie rizík by sa malo vykonať najmä s ohľadom na riziká vyplývajúce z automatizovaného spracúvania (napr. hackerské útoky, zlyhanie IT techniky, neoprávnené alebo neodborné zásahy tretích osôb do spracovateľského procesu), ako aj s ohľadom na riziká spojené s okolím, v ktorom sa dáta nachádzajú (napr. zabezpečenie budov a priestorov, protipožiarna ochrana, dostupnosť serverov a iných úložísk dát a pod.). Pri posudzovaní primeranej úrovne bezpečnosti sa totiž 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 údajom⁶⁸.

Z uvedeného je zrejmé, že to, aké konkrétne bezpečnostné opatrenia prevádzkovateľ v konečnom dôsledku prijme, by malo byť výsledkom dôsledného posúdenia okolností spracúvania v konkrétnych podmienkach toho – ktorého prevádzkovateľa alebo sprostredkovateľa.

Účinnosťou Nariadenia nastáva podstatná zmena v tom, že prevádzkovatelia už nebudú musieť vypracovať bezpečnostné projekty⁶⁹ alebo dokumentáciu, ako tomu bolo doteraz. Namiesto toho bude potrebné – ak je pravdepodobné, že určitý druh spracovania bude mať za následok vysoké riziko pre práva a slobody fyzických osôb – vykonať pred spracúvaním posúdenie vplyvu ochrany údajov („*privacy impact assessment*“, „*PIA*“), prípadne požiadať Úrad o konzultáciu podľa čl. 35 a 36 Nariadenia. Táto povinnosť sa bude aplikovať v špecifických prípadoch, napr. pri systematickom monitorovaní verejne prístupných miest vo veľkom rozsahu, ak prevádzkovateľ bude spracúvať osobné údaje o uznanie viny za trestné činy a priestupky, profilovanie či automatizované individuálne rozhodovanie a pod.

Pre účely zabezpečenia a preukázania prijatia vhodných bezpečnostných opatrení je možné, aby prevádzkovateľ pristúpil k dodržiavaniu schváleného kódexu správania⁷⁰ alebo schváleného certifikačného mechanizmu⁷¹. Tiež, prevádzkovateľ je povinný zabezpečiť, aby každá fyzická osoba konajúca na základe poverenia prevádzkovateľa, ktorá má prístup k osobným údajom (momentálne

⁶⁸ Čl. 32 ods. 2 Nariadenia.

⁶⁹ § 20 zákona č. 122/2013 Z.z. o ochrane osobných údajov.

⁷⁰ Čl. 40 Nariadenia.

⁷¹ Čl. 42 Nariadenia.

tzv. oprávnená osoba), spracúvala tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Únie alebo práva členského štátu.

Podstatnou povinnosťou prevádzkovateľa a sprostredkovateľa bude dôsledná kontrola plnenia prijatých opatrení a povinností zodpovedných osôb. Samotná PIA či konzultácia Úradu a následné prijatie bezpečnostných technických a organizačných opatrení teda nebude postačovať.⁷²

Oznámenie porušenia ochrany osobných údajov

Akokoľvek zodpovedne prevádzkovateľ pristupuje k ochrane osobných údajov, ktoré spracúva, zrejme nebude možné úplne vylúčiť riziko porušenia ochrany osobných údajov („*data breach*“). Takým porušením sa rozumie najmä náhodné alebo nezákonné zničenie, strata, zmena, neoprávnené poskytnutie osobných údajov, ktoré sa prenášajú, uchováajú alebo inak spracúvajú, alebo neoprávnený prístup k takýmto údajom⁷³.

Nariadenie upravuje v súvislosti s porušením ochrany osobných údajov dva druhy oznamovacej povinnosti prevádzkovateľov:

a) Oznámenie porušenia príslušnému dozornému orgánu

V prípade porušenia ochrany osobných údajov je prevádzkovateľ v prvom rade povinný oznámiť túto skutočnosť dozornému orgánu príslušnému podľa článku 55 Nariadenia. Toto oznámenie je potrebné vykonať bez zbytočného odkladu, avšak podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti prevádzkovateľ dozvedel. Ak oznámenie nebolo predložené v stanovenej dobe, pripojí sa k nemu zdôvodnenie tohto omeškania.

Ak prevádzkovateľ nie je schopný z objektívnych príčin poskytnúť dozornému orgánu informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

Oznámenie musí obsahovať aspoň:

- opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
- opis pravdepodobných následkov porušenia ochrany osobných údajov;
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Prevádzkovateľ nie je povinný oznamovať porušenie dozornému orgánu, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

b) Oznámenie porušenia ochrany osobných údajov dotknutej osobe

Ak dôjde k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ je povinný oznámiť porušenie

⁷² Kontrola nemusí byť špecializovaná na ochranu osobných údajov, môže byť súčasťou uplatňovania práv a povinností vedúcich zamestnancov kontrolovať v rámci pracovno-právnych vzťahov prácu podriadených zamestnancov. Možnosťou je tiež využitie už štandardných automatizovaných prostriedkov, napr. tzv. logov (záznam o prístupe konkrétnej osoby do systému).

⁷³ Čl. 32 ods. 2 Nariadenia.

ochrany osobných údajov aj dotknutej osobe. Toto oznámenie je povinný vykonať bez zbytočného odkladu.

V oznámení prevádzkovateľ uvedie jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň tieto informácie a opatrenia:

- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
- opis pravdepodobných následkov porušenia ochrany osobných údajov; a
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Aj v tomto prípade Nariadenie upravuje výnimku, kedy prevádzkovateľ nie je povinný porušenie oznamovať dotknutej osobe. Oznámenie sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:

- prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie;
- prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky;
- by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, dozorný orgán môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil.

Zdokumentovanie porušenia ochrany osobných údajov

Okrem uvedenej oznamovacej povinnosti je prevádzkovateľ povinný aj interne zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu, a tieto dokumenty uchovávať.

Okrem toho prevádzkovateľ musí splniť aj určitý komunikačný (t.j. dokumentačný) štandard pri oznamovaní porušenia dozornému orgánu a dotknutým osobám (náležitosti takých oznámení vid' vyššie).

Čo ďalej

Prevádzkovatelia a sprostredkovatelia by mali pred účinnosťou Nariadenia preveriť svoje doterajšie interné technické a organizačné opatrenia z hľadiska nových požiadaviek, vyhodnotiť mieru rizík s ohľadom na súčasný stav techniky, nákladovosť opatrení a povahu spracovávaných osobných údajov, aktualizovať svoje súčasné bezpečnostné opatrenia a kontrolné a zodpovednostné mechanizmy, zabezpečiť riadnu evidenciu a postupy pre včasné hlásenie prípadných bezpečnostných incidentov. Ak zistia vysoké riziko pre práva a slobody fyzických osôb, je potrebné vykonať PIA, prípadne konzultovať Úrad. Uvedené kroky by mali byť tiež schopní spätne doložiť a zdôvodniť v záujme preukázateľnosti a svojej liberácie z prípadnej súkromnoprávnej zodpovednosti (za škodu spôsobenú dotknutej osobe), ako aj verejnoprávnej (za správny delikt) či trestnoprávnej (napr. trestný čin neoprávneného nakladania s osobnými údajmi).

Ďalšie informácie

Recitály 83 - 94

Články 32 - 34

Lekcia 11 z 16

Kódexy správania a certifikácia

V texte sa dozviete:

Dôležité zmeny

- Nariadenie prináša nové inštitúty na zabezpečenie a preukázanie, že spracúvanie je v súlade s Nariadením, a to:
 - kódexy správania, a
 - certifikačné mechanizmy, pečate alebo značky;
- Prostredníctvom kódexov správania majú prevádzkovatelia a sprostredkovatelia možnosť ľahšie zabezpečiť a dodržať súlad s Nariadením;
- Dodržiavanie kódexov správania budú monitorovať akreditované subjekty; ak sa u prevádzkovateľa alebo sprostredkovateľa zistí porušenie kódexu, môže byť vylúčený z participácie na kódexe;
- Certifikačné mechanizmy, pečate a značky sa budú zavádzať za účelom dobrovoľnej „samoregulácie“ zo strany prevádzkovateľa alebo sprostredkovateľa;
- Ak prevádzkovateľ alebo sprostredkovateľ bude disponovať niektorým z týchto inštitútov, bude preukázaný súlad s Nariadením, a to po dobu 3 rokov (dobu platnosti certifikácie je možné následne predĺžiť);

Compliance: Akčný plán

Prevádzkovatelia a sprostredkovatelia by mali:

- monitorovať, či neexistujú v ich odvetví schválené kódexy správania platné či už v rámci SR alebo EÚ;
- zistiť, či existujú certifikačné mechanizmy, pečate alebo značky, ktoré by mohli získať a tak preukázať súlad s Nariadením;
- oboznámiť sa s certifikátmi, pečatami alebo značkami, ktoré sa budú priebežne zavádzať, a prihliadať na tieto inštitúty pri výbere svojich sprostredkovateľov alebo subdodávateľov.

Kódexy správania

Kódexy správania Nariadenie upravuje ako dokumenty vypracované združeniami alebo inými subjektmi zastupujúcimi kategórie prevádzkovateľov alebo sprostredkovateľov, ktoré upravujú spracúvanie osobných údajov špecifické pre tieto skupiny prevádzkovateľov alebo sprostredkovateľov. Kódexy majú prispieť k správne uplatňovaniu Nariadenia a majú brať do úvahy osobitné črty rôznych sektorov spracúvania a osobitné potreby mikropodnikov a malých a stredných podnikov.

Kódexy teda budú mať význam pre prevádzkovateľov a sprostredkovateľov, ktorí prostredníctvom ich dodržiavania budú môcť jednoduchšie a spoľahlivo jednak zabezpečiť, ale aj preukázať dozorným orgánom súlad s Nariadením.

To, že sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať schválený kódex správania, môže mať niekoľkonásobný pozitívny účinok:

- prostredníctvom kódexov sa zavedú odporúčané postupy, ako v danom sektore a v špecifickom kontexte spracúvania s osobnými údajmi nakladať;

- bude sa môcť spoľahnúť, že spracúvanie osobných údajov vykonáva zákonným spôsobom, čo mu môže ušetriť napr. náklady na odborných poradcov v tejto oblasti;
- participácia na schválenom kódexe bude požívať dôveru u dotknutých osôb, že ich osobné údaje sú spracúvané zákonným spôsobom;
- spolu so záväzkom importéra údajov sídliaceho mimo EÚ prijať primerané záruky budú kódexy použiteľné pri zabezpečovaní zákonnosti prenosu údajov mimo EÚ, podobne ako štandardné zmluvné doložky a záväzné vnútro podnikové pravidlá; a
- voči dozornému orgánu bude ľahko preukázateľný súlad s Nariadením.

Združenie alebo iný subjekt zastupujúci kategórie prevádzkovateľov alebo sprostredkovateľov teda môže vypracovať kódex správania relevantný pre daný sektor alebo odvetvie. Kódex má slúžiť ako „návod“ pre spoločnosti pôsobiace v danom sektore, ako správne spracúvať osobné údaje špecifické pre ich odvetvie, napr. subjekty pôsobiace v sektore bankovníctva, zdravotníctva, školstva, farmaceutického priemyslu, maloobchodu, IT sektora a cloudových služieb a pod.

Kódexy môžu upravovať odporúčané postupy napríklad v súvislosti so spravodlivým a transparentným spracúvaním, oprávnenými záujmami, ktoré prevádzkovatelia sledujú v konkrétnych situáciách, získavaním osobných údajov, pseudonymizáciou osobných údajov, informovaním verejnosti a dotknutých osôb, uplatnením práv dotknutých osôb, informovaním a ochranou detí a spôsobom získania súhlasu nositeľov rodičovských práv a povinností, opatreniami a postupmi účelnými pre prijatie vhodných technických a organizačných opatrení a špecificky navrhnutej a štandardnej ochrany údajov, opatrení na zabezpečenie bezpečnosti údajov, oznámením porušenia ochrany osobných údajov dozorným orgánom a informovaním dotknutých osôb o takýchto porušeníach ochrany osobných údajov, prenosom osobných údajov do tretích krajín alebo medzinárodným organizáciám a mimosúdnym konaním a inými postupmi riešenia sporov zameranými na riešenie sporov medzi prevádzkovateľmi a dotknutými osobami v súvislosti so spracúvaním.

Schvaľovanie kódexov

Na to, aby mal kódex správania vyššie uvedené účinky, je potrebné, aby ho schválil kompetentný orgán dohľadu. Proces schválenia závisí od toho, či ide o kódex s vnútroštátnou platnosťou, alebo či má byť mať kódex všeobecnú platnosť v rámci Únie.

Ak ide o kódex, ktorý sa netýka spracovateľských operácií mimo určitého štátu (napr. SR), je potrebné jeho návrh predložiť príslušnému dozornému orgánu, (v tomto prípade Úradu na ochranu osobných údajov SR). Dozorný orgán vydá stanovisko, či je návrh kódexu v súlade s Nariadením a ak dôjde k záveru, že poskytuje dostatočné primerané záruky, takýto návrh kódexu schváli. V takom prípade dozorný orgán kódex aj zaregistruje a jeho znenie uverejní.

Naopak, ak ide o kódex, ktorý sa týka spracovateľských činností vo viacerých členských štátoch, príslušný dozorný orgán ho pred schválením návrhu kódexu predloží v rámci spolupráce dozorných orgánov štátov Únie a Komisie Európskemu výboru pre ochranu údajov („Výbor“), ktorý vydá stanovisko, či je návrh kódexu v súlade s Nariadením, alebo či poskytuje primerané záruky. Ak Výbor v stanovisku potvrdí, že návrh kódexu je v súlade s Nariadením alebo poskytuje primerané záruky, predloží svoje stanovisko Európskej komisii. Komisia môže prostredníctvom vykonávacích aktov rozhodnúť, že schválený kódex správania, ktoré jej boli predložené, majú všeobecnú platnosť v rámci Únie. Komisia zabezpečí zverejnenie schválených kódexov, o ktorých bolo rozhodnuté, že majú všeobecnú platnosť. Výbor zhromažďuje všetky schválené kódexy správania a primeraným spôsobom ich zverejňuje.

Monitorovanie dodržiavania kódexov

Okrem príslušného dozorného orgánu môže dodržiavanie kódexov správania monitorovať aj subjekt, ktorý má primeranú úroveň odborných znalostí a na tento účel je akreditovaný príslušným dozorným orgánom. Taký subjekt bude musieť:

- preukázať svoju nezávislosť a odborné znalosti vo vzťahu k predmetu úpravy kódexu;
- stanoviť postupy, ktoré mu umožňujú posúdiť oprávnenosť dotknutých prevádzkovateľov a sprostredkovateľov, pokiaľ ide o uplatňovanie kódexu, monitorovať, ako dodržiavajú ustanovenia kódexu a pravidelne preskúmať jeho fungovanie;
- stanoviť postupy a štruktúry na vybavovanie sťažností týkajúcich sa porušení kódexu alebo spôsobu, akým bol alebo je kódex vykonávaný prevádzkovateľom alebo sprostredkovateľom, a na dosiahnutie transparentnosti týchto postupov a štruktúr pre dotknuté osoby a verejnosť, a
- preukázať, že jeho úlohy a povinnosti nevedú ku konfliktu záujmov.

Kritériá na akreditáciu určí príslušný dozorný orgán po konzultácii s Európskym výborom pre ochranu údajov. Ak akreditovaný subjekt zistí porušenie kódexu, môže prevádzkovateľovi alebo sprostredkovateľovi uložiť sankciu v podobe primeraných opatrení, ktorými môžu byť aj pozastavenie členstva dotknutého prevádzkovateľa alebo sprostredkovateľa v kódexe alebo jeho vylúčenia z kódexu.

Certifikácia

Certifikačné mechanizmy, pečate a značky Nariadenie upravuje ako ďalšie nové inštitúty ochrany osobných údajov. Tieto mechanizmy majú slúžiť najmä na zvýšenie transparentnosti spracúvania, a majú pomôcť dotknutým osobám rýchlo posúdiť úroveň ochrany osobných údajov v prípade relevantných produktov a služieb. Ako príklad možno uviesť situáciu, kedy sa pre určitú službu, napr. poskytovanie cloudových služieb, zavedú napr. pečate alebo značky, ktoré budú znamenať, že subjekt, ktorý ich získa, spĺňa požiadavky Nariadenia pre zákonné spracúvanie⁷⁴.

Certifikácia spracúvania osobných údajov je dôležitým medzníkom pre vytvorenie spoľahlivého a transparentného rámca pre spracúvanie. Tieto mechanizmy môžu byť zavedené tak členskými štátmi, ako aj dozornými orgánmi, Výborom, či Komisiou. Mali by byť aplikovateľné predovšetkým na úrovni Únie, avšak nie je vylúčená ani vnútroštátna platnosť. Mali by sa pritom zohľadniť osobitné potreby mikropodnikov a malých a stredných podnikov.

Certifikácia je dobrovoľná, avšak neznižuje zodpovednosť prevádzkovateľa alebo sprostredkovateľa za dodržiavanie Nariadenia. Inými slovami, ak napr. prevádzkovateľ získa certifikáciu, ale napriek tomu spracúvaním údajov poruší Nariadenie, certifikácia ho nezabavuje zodpovednosti. Certifikácia sa vydá na obdobie maximálne troch rokov s možnosťou obnovenia po uplynutí tejto doby za rovnakých podmienok. Podobne, ak sa podmienky pre certifikáciu prestanú spĺňať, certifikácia môže byť subjektu odobraná.

Certifikácia môže mať nasledovné výhody pre prevádzkovateľov a sprostredkovateľov:

- prevádzkovatelia a sprostredkovatelia budú môcť ľahšie preukázať súlad s Nariadením, a to predovšetkým v súvislosti s prijatím primeraných technických a organizačných opatrení;
- dotknuté osoby, prípadne zákazníci, ktorí sa budú rozhodovať pre dodávateľa služieb, môžu na certifikáciu prihliadať ako na dôkaz vierohodnosti a profesionality poskytovateľa (napr. cloudových) služieb; a
- podobne ako v prípade kódexov, spolu so záväzkom importéra údajov sídliaceho mimo EÚ prijať primerané záruky budú certifikácie použiteľné pri zabezpečovaní zákonnosti prenosu

⁷⁴ Pre porozumenie možno uviesť napr. značku ISO, ktorá preukazuje, že subjekt v danej oblasti dosahuje kvalitu požadovanú týmto certifikátom.

údajov mimo EÚ, podobne ako štandardné zmluvné doložky a záväzné vnútro podnikové pravidlá.

Nariadenie priznáva právomoc vydávať certifikáciu okrem dozorných orgánov aj certifikačným subjektom, ktoré získajú akreditáciu pre túto činnosť. V slovenských podmienkach bude Úrad na ochranu osobných údajov oprávnený udeliť akreditáciu certifikačných subjektov. Pre získanie akreditácie certifikačného subjektu bude potrebné splniť kritériá stanovené Nariadením, okrem iného:

- preukázať nezávislosť a odborné znalosti vo vzťahu k predmetu certifikácie;
- zaviazat sa rešpektovať kritéria schválené Výborom alebo príslušným dozorným orgánom;
- stanoviť postupy na vydávanie, pravidelné preskúmanie a odoberanie certifikácie, pečatí a značiek ochrany údajov;
- stanoviť postupy a štruktúry na vybavovanie sťažností týkajúcich sa porušení certifikácie alebo spôsobu, akým bola alebo je certifikácia vykonávaná prevádzkovateľom alebo sprostredkovateľom, a tieto postupy a štruktúry stransparentniť pre dotknuté osoby a verejnosť, a
- preukázať, že úlohy a povinnosti žiadateľa o akreditáciu nevedú ku konfliktu záujmov.

Akreditácia certifikačných subjektov sa vydá na obdobie maximálne 5 rokov s možnosťou obnovenia.

Čo ďalej

Prevádzkovatelia a sprostredkovatelia môžu významne benefitovať z participácie na schválených kódexoch správania (platných vnútroštátne alebo v rámci Únie), alebo z certifikátov, značiek alebo pečatí, ktoré sa budú zavádzať priebežne po tom, čo Nariadenie nadobudne účinnosť. Z uvedeného dôvodu sa odporúča, aby prevádzkovatelia a sprostredkovatelia monitorovali zavádzanie týchto inštitútov do platnosti, aby sa vedeli včas rozhodnúť, či sa budú uchádzať o participáciu v nich, či ich získanie.

Ďalšie informácie

Recitály 77, 81, 98 – 100, 148, 166, 168,

Články 40 – 43, 57 ods. 1 písm. p), q), ods. 3 písm. e), 64 ods. 1 písm. c), 70 ods. 1 písm. o), p)

Lekcia 12 z 16

Prenos osobných údajov mimo EÚ/EHS

V texte sa dozviete:

Dôležité zmeny

- Požiadavky pre prenosi údajov sa budú týkať najmä nadnárodných spoločností alebo spoločností, ktoré využívajú služby zahŕňajúce prenos údajov do tretích krajín (napr. cloudové služby);
- V porovnaní s pôvodnou právnou úpravou sa zavádzajú nové možnosti, ako zabezpečiť zákonnosť pri prenose údajov mimo EÚ/EHS.

Compliance: Akčný plan

Prevádzkovatelia a sprostredkovatelia by mali:

- preveriť toky osobných údajov, ktoré spracúvajú;
- ak sa údaje prenášajú mimo EÚ/EHS, preveriť, či sú prijaté mechanizmy na zabezpečenie zákonnosti prenosu (napr. štandardné zmluvné doložky, záväzné vnútropodnikové pravidlá a pod.);
- preveriť, či a kam prenášajú osobné údaje dodávateľov služieb, ktorým prevádzkovatelia alebo sprostredkovatelia údaje poskytujú;
- ak sa prenosi uskutočňovali na základe "Bezpečného prístavu", určiť iný právny základ pre prenos, nakoľko Bezpečný prístav bol zrušený.

Prenos osobných údajov mimo EÚ/EHS

Podobne ako predchádzajúca právna úprava, aj Nariadenie upravuje podmienky prenosov osobných údajov do tretích krajín (mimo EÚ/EHS) a do medzinárodných organizácií⁷⁵. Dôvodom je skutočnosť, že len čo osobné údaje opustia územie, kde sa uplatňuje právny poriadok EÚ, stanú sa predmetom právnej úpravy cudzích právnych predpisov, ktoré nemusia zaručovať ochranu osobných údajov na úrovni porovnateľnej s právom EÚ. Táto problematika sa preto bude týkať najmä nadnárodných spoločností, alebo spoločností, ktoré využívajú služby dodávateľov pôsobiacich mimo Únie (napr. ak využívajú cloudové služby serverov umiestnených v tretích krajinách). Naopak, táto problematika sa nebude týkať spoločností, ktoré údaje neprenášajú, alebo ich prenášajú iba v rámci EÚ/EHS.

Východiskový bod pre porozumenie potreby úpravy prenosu údajov mimo EÚ uvádza recitál 101 Nariadenia, podľa ktorého toky osobných údajov do krajín mimo Únie a medzinárodným organizáciám aj z takýchto krajín a medzinárodných organizácií sú potrebné pre rozmach medzinárodného obchodu a medzinárodnú spoluprácu. Zvyšovanie takýchto tokov so sebou prinieslo nové výzvy a potreby týkajúce sa ochrany osobných údajov. Úroveň ochrany údajov fyzických osôb zaručovaná Úniou na základe Nariadenia by nemala byť ohrozená ani vtedy, keď sú osobné údaje prenášané z Únie prevádzkovateľom, sprostredkovateľom alebo iným príjemcom v tretích krajinách alebo medzinárodným organizáciám, a to ani v prípadoch následného prenosu osobných údajov z tretej krajiny alebo medzinárodnej organizácie prevádzkovateľom, sprostredkovateľom v rovnakej alebo inej tretej krajine alebo medzinárodnej organizácii.

Prenos osobných údajov do tretích krajín bude možný za splnenia niektorej z nasledovných podmienok:

⁷⁵ Čl. 4 ods. ods. 26 Nariadenia: *organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.*

Prenos na základe rozhodnutia o primeranosti

Európska komisia („Komisia“) môže rozhodnúť, že určitá tretia krajina, územie alebo jeden či viaceré určené sektory v danej tretej krajine alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany⁷⁶. Na prenos do takej krajiny potom nie je nutné žiadne osobitné povolenie. Preskúmanie okolností, na základe ktorých Komisia rozhodnutie vydala, sa koná najmenej raz za štyri roky.

Ak Komisia zistí, že podmienky majúce dopad na ochranu osobných údajov v tretej krajine (príp. medzinárodnej organizácii) sa negatívne zmenili, rozhodne, že taká krajina už nezaručuje primeranú úroveň ochrany. Také rozhodnutie však nemá retroaktívny účinok, teda je účinné najskôr v deň jeho prijatia. Preto otázkou ostáva bezpečnosť už prenesených údajov.

Zoznam tretích krajín a medzinárodných organizácií, ktoré podľa rozhodnutia Komisie zaručujú primeranú úroveň ochrany alebo ju už prestali zaručovať, Komisia uverejnení v Úradnom vestníku Európskej únie a na svojom webovom sídle⁷⁷. Momentálne krajiny zaručujúce primeranú úroveň ochrany údajov sú: Andora, Argentína, Kanada, Švajčiarsko, Faerské ostrovy, ostrovy Guernsey, Man a Jersey, Izrael, Nový Zéland a Uruguaj.

Prenos údajov do Spojených štátov Amerických má určité špecifiká. Do roku 2015 bol prenos do USA možný okrem iného aj prostredníctvom schémy tzv. Bezpečného prístavu⁷⁸, ktorá umožňovala prenášať osobné údaje subjektom nachádzajúcim sa v USA a registrovaným v Bezpečnom prístave bez ďalších opatrení a formalít. Dňa 6. októbra 2015 však Veľká komora SD EÚ vydala rozhodnutie⁷⁹, ktorým zrušila predmetné rozhodnutie Komisie upravujúce Bezpečný prístav, od kedy prenos osobných údajov do USA na základe tohto legislatívneho aktu už nie je považovaný za zákonný.⁸⁰

Táto schéma bola následne nahradená schémou tzv. „Privacy shield“⁸¹, ktorú Komisia chválila dňa 12. júla 2016. Zoznam spoločností, ktoré sa zaviazali dodržiavať zásady ochrany osobných údajov zavedené prostredníctvom Privacy shield, je zverejnený na stránke amerického Ministerstva obchodu (Department of Commerce)⁸².

Prenosy vyžadujúce primerané záruky

Ak neexistuje rozhodnutie Komisie uvedené vyššie, prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť len vtedy, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky, a za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva

⁷⁶ Pri posudzovaní primeranosti úrovne ochrany zohľadňuje Komisia skutočnosti ako napr. právny štát, dodržiavanie ľudských práv a základných slobôd, príslušné právne predpisy ako aj vykonávanie takýchto právnych predpisov, pravidiel ochrany údajov, profesionálnych pravidiel a bezpečnostných opatrení vrátane pravidiel pre následný prenos osobných údajov do ďalšej tretej krajiny alebo medzinárodnej organizácii, účinné správne a súdne prostriedky nápravy, existenciu a účinné pôsobenie nezávislých dozorných orgánov, medzinárodné záväzky a pod.

⁷⁷ http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

⁷⁸ Rozhodnutie Komisie 2000/520/EC z 26. júla 2000, ktoré obsahovalo zásady a požiadavky týkajúce sa ochrany osobných údajov, ktorým sa spoločnosti registrované v USA mohli dobrovoľne podriadiť a tak byť považované spoľahlivé ohľadne nakladania s osobnými údajmi.

⁷⁹ <http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=sk&lang2=EN&type=TXT&ancre=>

⁸⁰ Stalo sa tak na základe podnetu rakúskeho občana Maxa Schremsa, ktorý bol od roku 2008 užívateľom služieb Facebooku. Facebook pritom prenášal osobné údaje svojich užívateľov na servery nachádzajúce sa v USA, kde sa ďalej spracúvali. P. Schrems podal sťažnosť dozornému orgánu v Írsku, ktorej zmyslom bolo, že podľa informácií zverejnených Edwardom Snowdenom v roku 2013 ohľadne spôsobu, akým americké bezpečnostné zložky (najmä NSA – National Security Agency) nakladajú s osobnými údajmi v ich jurisdikcii (t.j. aj európskych užívateľov Facebooku), Spojené štáty Americké nezaručujú ochranu pred sledovaním zo strany amerických orgánov. Dozorný orgán v Írsku sťažnosť odmietol s odvolaním sa na záruky, ktoré sa subjekty USA zaviazali poskytnúť prostredníctvom Bezpečného prístavu. Po preskúmaní merita vecí SD EÚ schému Bezpečného prístavu zrušil.

⁸¹ http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

⁸² <https://www.privacyshield.gov/welcome>

a účinné právne prostriedky nápravy. Primerané záruky sa môžu ustanoviť bez toho, aby sa dozorný orgán žiadal o akékoľvek osobitné povolenie, prostredníctvom:

- právne záväzného a vykonateľného nástroja medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi;
- záväzných vnútropodnikových pravidiel;

Ak ide o holdingovú spoločnosť, ktorá má pobočky v Únii a v tretích krajinách, prenos údajov v rámci tohto holdingu sa môže vykonávať aj na základe záväzných vnútropodnikových pravidiel. Na to, aby boli záväzné, musia byť schválené príslušným dozorným orgánom, na základe ktorého sa stanú záväznými nie len v jurisdikcii dozorného orgánu, ktorý ich schválil, ale vo všetkých iných jurisdikciách, v ktorých má holding pobočky. Dozorný orgán pravidlá schváli, ak:

- sú právne záväzné a vzťahujú sa na každého dotknutého člena skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti vrátane ich zamestnancov, a títo členovia ich uplatňujú;
 - ak sa nimi výslovne udeľujú vymáhateľné práva dotknutým osobám, pokiaľ ide o spracúvanie ich osobných údajov; a
 - upravujú Nariadením určené náležitosti, medzi iným napr. štruktúru a kontaktné údaje skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti a každého z jej členov, prenosi údajov alebo súbor prenosov vrátane kategórií osobných údajov, typu spracúvania a jeho účelov, typu dotknutých osôb, ktorých sa spracúvanie týka, a identifikácia predmetnej tretej krajiny alebo krajín, ich právnu záväznosť, a to vnútorne a navonok, práva dotknutých osôb v súvislosti so spracúvaním a prostriedky na uplatnenie týchto práv, postupy týkajúce sa sťažností, mechanizmus spolupráce s dozorným orgánom na zabezpečenie dodržiavania pravidiel zo strany všetkých členov skupiny a pod.
- štandardných doložiek o ochrane údajov, ktoré prijala Komisia alebo ktoré prijal dozorný orgán a ktoré následne schválila Komisia; doložky, ktoré existovali pred prijatím Nariadenia, ostávajú v platnosti⁸³;

I keď prevádzkovatelia či sprostredkovatelia použijú na prenos mimo Únie štandardné zmluvné doložky, môžu ich zahrnúť do širšej zmluvy, ako napríklad zmluvy medzi sprostredkovateľom a ďalším sprostredkovateľom, alebo k nim pridať ďalšie doložky alebo dodatočné záruky, pokiaľ nie sú priamo alebo nepriamo v rozpore so štandardnými zmluvnými doložkami alebo pokiaľ sa nedotýkajú základných práv alebo slobôd dotknutých osôb.

- schváleného kódexu správania (ide o nový inštitút – vid'. Lekcia 11) spolu so záväznými a vymáhateľnými záväzkami prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcimi v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb, alebo
- schváleného certifikačného mechanizmu (ide o nový inštitút – vid'. Lekcia 11) spolu so záväzným a vymáhateľným záväzkom prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcim v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb.

Výnimky

Ak neexistuje rozhodnutie o primeranosti alebo ak neexistujú primerané záruky, prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť, ak je splnená niektorá z týchto podmienok:

⁸³ http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

- dotknutá osoba vyjadrila výslovný súhlas s navrhovaným prenosom;
- prenos je nevyhnutný na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom alebo na vykonanie predzmluvných opatrení prijatých na žiadosť dotknutej osoby;
- prenos je nevyhnutný pre uzatvorenie alebo plnenie zmluvy uzatvorenej v záujme dotknutej osoby medzi prevádzkovateľom a inou fyzickou alebo právnickou osobou;
- prenos je nevyhnutný z dôležitých dôvodov verejného záujmu;
- prenos je nevyhnutný na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov;
- prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby alebo iných osôb, ak je dotknutá osoba fyzicky alebo právne nespôsobilá vyjadriť súhlas;
- prenos sa uskutočňuje z registra, ktorý je podľa práva Únie alebo práva členského štátu určený na poskytovanie informácií verejnosti a ktorý je otvorený na nahliadanie verejnosti alebo akejkoľvek osobe, ktorá vie preukázať oprávnený záujem, ale len pokiaľ sú v tomto konkrétnom prípade splnené podmienky stanovené právom Únie alebo právom členského štátu na nahliadanie.

Prenos do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť tiež vtedy, ak prenos nie je opakujúcej sa povahy, týka sa len obmedzeného počtu dotknutých osôb, je nevyhnutný na účely závažných oprávnených záujmov, ktoré sleduje prevádzkovateľ a nad ktorými neprevažujú záujmy alebo práva a slobody dotknutej osoby, a prevádzkovateľ posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia poskytol vhodné záruky, pokiaľ ide o ochranu osobných údajov. V takom prípade však prevádzkovateľ musí informovať o prenose dozorný orgán.

Čo ďalej

Prevádzkovatelia a sprostredkovatelia musia preveriť, či prenášajú osobné údaje mimo EÚ/EHS, prípadne, či také prenosi realizujú ich dodávatelia služieb alebo tovarov. Následne je také prenosi potrebné založiť na niektorom z platných právnych základov pre prenosi, a to najmä na základe rozhodnutia o primeranosti alebo na základe primeraných záruk. Ak prenos nemožno odôvodniť niektorým z uvedených právnych základov, je potrebné preveriť, či sa na prenos môže aplikovať niektorá z výnimiek z tejto povinnosti.

Ďalšie informácie

Recitály 6, 23, 101 - 116

Články 44 - 49

Lekcia 13 z 16

Dozor nad spracúvaním osobných údajov

V texte sa dozviete:

Dôležité zmeny

- Prevádzkovatelia a sprostredkovatelia budú v určených prípadoch podliehať nielen dozornému orgánu na ochranu osobných údajov „vlastného“ štátu, ale môžu podliehať aj orgánu dozoru iného štátu Únie, ktorý bude mať postavenie vedúceho dozorného orgánu;
- Zriaďuje sa nový orgán EÚ - Európsky výbor pre ochranu údajov.

Compliance: Akčný plán

Prevádzkovatelia a sprostredkovatelia by sa mali:

- oboznámiť s rozsiahlymi kompetenciami dozorných orgánov;
- ak vykonávajú cezhraničné spracúvanie, odporúča sa oboznámiť so spôsobom fungovania a spolupráce vedúceho dozorného orgánu a lokálnych dozorných orgánov.

Dozor nad spracúvaním osobných údajov

Vykonávanie dozoru nad spracúvaním osobných údajov je ďalšou veľkou kapitolou problematiky osobných údajov. Podľa recitálu 117 Nariadenia, zriadenie dozorných orgánov v členských štátoch („ (...) je zásadným prvkom ochrany fyzických osôb pri spracúvaní ich osobných údajov“). Úlohou dozorných orgánov je teda vykonávať dohľad a prípadne autoritatívne zabezpečovať súlad s Nariadením za účelom ochrany práv a základných slobôd dotknutých osôb, ktorých údaje sa spracúvajú.

V oblasti dohľadu nad spracúvaním osobných údajov Nariadenie zavádza niekoľko nových konceptov, a dokonca aj jednu novú inštitúciu, v ktorej budú mať zastúpenie všetky štáty Únie. Pre prevádzkovateľov a sprostredkovateľov bude dôležité sa zorientovať, ktorým orgánom budú podliehať v rozsahu ktorých spracovateľských operácií, a prípadne, aké povinnosti budú mať voči týmto orgánom.

Vnútroštátne orgány dozoru

V prvom rade budú prevádzkovatelia a sprostredkovatelia podliehať vnútroštátnemu orgánu dohľadu na ochranu osobných údajov. V podmienkach SR ide o Úrad na ochranu osobných údajov SR⁸⁴.

Vnútroštátny dozorný orgán je príslušný vykonávať najmä dozor nad spracúvaním:

- v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa na území svojho členského štátu.

Vnútroštátny dozorný orgán nebude bez ďalšieho príslušný vykonávať dozor nad cezhraničným spracúvaním osobných údajov v rámci dvoch a viacerých štátov Únie (pre také spracúvanie vid'. časť „Vedúci dozorný orgán“ nižšie), ale iba pre spracovateľské operácie vykonávané v rámci jedného štátu (a to aj vtedy, ak ide o prevádzkovateľa alebo sprostredkovateľa, ktorý inak vykonáva aj cezhraničné spracúvanie);

- ktoré vykonávajú orgány verejnej moci alebo súkromnoprávne subjekty konajúce vo verejnom záujme.

⁸⁴ Webové sídlo: <https://dataprotection.gov.sk/uoou/> .

Štandardne pôjde napr. o spracovateľské operácie orgánov štátnej správy a samosprávy. Dozorné orgány však nie sú príslušné pre vykonávanie dozoru nad spracovateľskými operáciami na súdoch pri výkone ich súdnej právomoci;

- ktoré ovplyvňuje dotknuté osoby na jeho území.

Právomoc vnútroštátneho orgánu dozoru bude daná vždy, ak pôjde o práva dotknutej osoby nachádzajúcej sa na jeho území, t.j. bez ohľadu na to, či ide o vnútroštátne alebo cezhraničné spracúvanie (výnimka z pravidla uvedeného v prvom bode vyššie). Dozorný orgán je príslušný zaoberať sa jemu podanou sťažnosťou alebo prípadným porušením Nariadenia, ak sa skutková podstata týka iba prevádzkarne v jeho členskom štáte alebo podstatne ovplyvňuje dotknuté osoby iba v jeho členskom štáte;

- vykonávaným prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, ak je zacielený na dotknuté osoby s pobytom na území Únie.

Tento druh kontrolnej právomoci sa týka rozšírenej teritoriálnej pôsobnosti Nariadenia (viď Lekcia 1). Znamená to, že vnútroštátny orgán bude mať právomoc napr. nad čínskym prevádzkovateľom, ktorý nie je usadený v EÚ, avšak v niektorom štáte Únie ponúka tovar alebo služby.

Vedúci dozorný orgán

Ak prevádzkovateľ alebo sprostredkovateľ spracúva osobné údaje cezhranične (či už prostredníctvom jednej alebo niekoľkých pobočiek v rámci Únie), bude podliehať aj vedúcemu dozornému orgánu, ktorý je príslušný ako vedúci dozorný orgán pre cezhraničné spracúvanie. V rozsahu tých spracovateľských operácií, ktoré nezahŕňajú cezhraničný prvok, budú naďalej podliehať vnútroštátnemu dozornému orgánu, avšak ak pôjde o cezhraničné spracúvanie, príslušný bude vedúci dozorný orgán.

Každý (aj iný než vedúci) dozorný orgán je však príslušný zaoberať sa jemu podanou sťažnosťou alebo prípadným porušením Nariadenia, ak sa skutková podstata týka iba prevádzkarne v jeho členskom štáte alebo podstatne ovplyvňuje dotknuté osoby iba v jeho členskom štáte. To znamená, že aj keď ide o cezhraničné spracovanie, každý dozorný orgán môže konať za uvedených podmienok. Dozorný orgán však o tejto skutočnosti najskôr bezodkladne informuje vedúci dozorný orgán, ktorý rozhodne, či sa bude alebo nebude prípadom zaoberať.

Ak sa vedúci dozorný orgán rozhodne, že sa prípadom nebude zaoberať, príslušným bude vnútroštátny dozorný orgán. Ak vedúci dozorný orgán rozhodne, že sa prípadom bude zaoberať, dozorný orgán, ktorý informoval vedúci dozorný orgán, mu môže predložiť návrh rozhodnutia, a vedúci dozorný orgán bude postupovať podľa postupu spolupráce nasledovne:

Spolupráca medzi vedúcim dozorným orgánom a inými dotknutými dozornými orgánmi

- *Spolupráca a výmena informácií:* vedúci dozorný orgán spolupracuje s inými dotknutými dozornými orgánmi s cieľom dosiahnuť konsenzus. Vedúci dozorný orgán a dotknuté dozorné orgány si navzájom vymieňajú všetky relevantné informácie.
- *Predloženie návrhu rozhodnutia na vyjadrenie dotknutým dozorným orgánom:* vedúci dozorný orgán bezodkladne oznámi informácie týkajúce sa veci iným dotknutým dozorným orgánom. Bezodkladne predloží iným dotknutým dozorným orgánom návrh rozhodnutia, aby sa k nemu vyjadrili a aby sa náležite zohľadnili ich stanoviská.
 - *Predloženie veci Výboru:* ak ktorýkoľvek z iných dotknutých dozorných orgánov podá v lehote štyroch týždňov relevantnú a odôvodnenú námietku k návrhu rozhodnutia, vedúci dozorný orgán, ak s takou námietkou nesúhlasí alebo sa domnieva, že je nerelevantná alebo neodôvodnená, predloží záležitosť Európskemu výboru pre ochranu údajov („Výbor“).

- *Predloženie revidovaného návrhu na vyjadrenie dotknutým dozorným orgánom:* Ak má vedúci dozorný orgán v úmysle podanej relevantnej a odôvodnenej námietke vyhovieť, predloží iným dotknutým dozorným orgánom revidovaný návrh rozhodnutia na účely vyjadrenia stanoviska.
- *Vydanie rozhodnutia:* vedúci dozorný orgán rozhodnutie prijme a oznámi ho hlavnej prevádzkarni alebo jedinej prevádzkarni prevádzkovateľa, prípadne sprostredkovateľa, a o danom rozhodnutí vrátane zhrnutia relevantných faktov a dôvodov informuje iné dotknuté dozorné orgány a Výbor. Dozorný orgán, na ktorom sa sťažnosť podala, informuje sťažovateľa o rozhodnutí. Ak sa sťažnosť odmietne alebo sa jej nevyhovie, dozorný orgán, na ktorom sa sťažnosť podala, prijme rozhodnutie, oznámi ho sťažovateľovi a informuje prevádzkovateľa.
- *Zabezpečenie súladu:* vedúci dozorný orgán dohliadne na to, aby prevádzkovateľ alebo sprostredkovateľ prijali potrebné opatrenia na zabezpečenie súladu s rozhodnutím, pokiaľ ide o spracovateľské činnosti v súvislosti so *všetkými* svojimi prevádzkarňami v Únii. Prevádzkovateľ alebo sprostredkovateľ oznámia opatrenia prijaté na dodržanie rozhodnutia vedúcemu dozornému orgánu, ktorý o tom informuje iné dotknuté dozorné orgány.

Pravidlá pre určenie vedúceho dozorného orgánu prevádzkovateľov alebo sprostredkovateľov, vrátane širšieho vysvetlenia problematiky s príkladmi, obsahuje dokument, pripravený WP 29.⁸⁵

Európsky výbor pre ochranu údajov

Nariadenie upravuje postavenie nového nezávislého orgánu s vlastnou právnou subjektivitou – Európskeho výboru pre ochranu údajov („Výbor“). Výbor má postavenie orgánu Únie a je tvorený zástupcami dozorných orgánov jednotlivých štátov Únie a Európskym dozorným úradníkom pre ochranu údajov⁸⁶ („Úradník“).

I keď prevádzkovatelia a sprostredkovatelia nebudú priamo podliehať dohľadu Výboru, Výbor môže mať dosah na spracúvanie osobných údajov, ktoré vykonávajú. Výbor má zoznam úloh, avšak najmä zaisťuje konzistentné uplatňovanie Nariadenia. Na tento účel v rámci mechanizmu konzistentnosti spolupracuje s dozornými orgánmi členských štátov pri vydávaní rozhodnutí.

Čo ďalej

Pre prevádzkovateľov a sprostredkovateľov, ktorí spracúvajú osobné údaje iba v rámci jedného členského štátu, bude relevantný iba dohľad zo strany dozorného orgánu v tomto členskom štáte. Ak dochádza k cezhraničnému spracúvaniu údajov, je dôležité si uvedomiť, že tieto spracovateľské operácie môžu podliehať aj dohľadu vedúceho dozorného orgánu. Prevádzkovatelia a sprostredkovatelia by mali byť v tom prípade pripravení komunikovať aj s iným než lokálnym dozorným orgánom.

Ďalšie informácie

Recitály 117 - 140

Články kapitoly VI a VII

⁸⁵ Guidelines for identifying a controller or processor's lead supervisory authority; prijaté Article 29 Data Protection Working Party dňa 13. 12. 2016, revidované dňa 5. 4. 2017, WP 244 rev. 01.

⁸⁶ "European Data Protection Supervisor"

Lekcia 14 z 16

Prostriedky nápravy

V texte sa dozviete:

Dôležité zmeny

Dotknuté osoby (v niektorých prípadoch aj iné osoby, napr. prevádzkovatelia) majú k dispozícii nasledovné prostriedky nápravy:

- právo podať sťažnosť dozornému orgánu;
- právo podať žalobu na súde voči rozhodnutiu dozorného orgánu;
- právo podať žalobu na súde voči prevádzkovateľovi alebo sprostredkovateľovi;
- právo na náhradu majetkovej a nemajetkovej ujmy.

Compliance: Akčný plán

- Prevádzkovatelia a sprostredkovatelia by mali účinnými zmluvnými prostriedkami detailne medzi sebou vymedziť rozsah povinností, sankcie za ich porušenie, spôsob riešenia sporov a zodpovednostné vzťahy voči dotknutým osobám.
- Spoloční prevádzkovatelia by si mali dohodnúť rozsah ich povinností za účelom dosiahnutia súladu s Nariadením, rozsah zodpovednosti za porušenie Nariadenia, spôsob riešenia sporov a spôsob znášania zodpovednosti za škodu.

K prostriedkom nápravy

Právo podať sťažnosť dozornému orgánu

V prvom rade Nariadenie priznáva dotknutej osobe právo podať sťažnosť dozornému orgánu, ak sa domnieva, že spracúvanie jeho osobných údajov je v rozpore s Nariadením. Účelom tohto právneho prostriedku je chrániť práva, ktoré Nariadenie priznáva dotknutým osobám, pred porušovaním zo strany prevádzkovateľov alebo sprostredkovateľov.

Ako sme uviedli v Lekcii 13, spracovateľské operácie prevádzkovateľa môžu podliehať minimálne dvom dozorným orgánom, a to orgánu príslušnému podľa miesta sídla prevádzkovateľa, alebo vedúcemu dozornému orgánu príslušnému na dohľad nad spracovateľskými operáciami prevádzkovateľa alebo skupiny prevádzkovateľov v rámci Únie.

Pre uľahčenie prístupu dotknutých osôb k dozornému orgánu Nariadenie stanovuje, že dotknutá osoba môže podať sťažnosť dozornému orgánu predovšetkým v členskom štáte svojho obvyklého pobytu, v mieste výkonu práce alebo v mieste údajného porušenia.

Dozorný orgán je povinný prešetriť udalosť, ktorá je predmetom sťažnosti, t.j. zistiť, či k porušeniu skutočne došlo a ak áno, zabezpečiť nápravu. Dozorný orgán, ktorému sa sťažnosť podala, je následne povinný informovať sťažovateľa o postupe v riešení sťažnosti a o jeho výsledku, vrátane možnosti podať súdny prostriedok nápravy (viď nižšie).

Ak si vec vyžaduje ďalšie vyšetrovanie alebo koordináciu s iným dozorným orgánom, dotknutej osobe by sa mali poskytnúť priebežné informácie. Na účely uľahčenia podávania sťažností by mal každý dozorný orgán prijať opatrenia, ako napríklad poskytnúť formulár sťažnosti, ktorý je možné vyplniť aj elektronicky, nevyklučujúc pritom iné prostriedky komunikácie.

Právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu

Fyzické alebo právnické osoby

Nariadenie priznáva každej fyzickej alebo právnickej osobe (t.j. tiež prevádzkovateľom a sprostredkovateľom) právo na účinný súdny prostriedok nápravy (t.j. podanie žaloby) voči právne záväznému rozhodnutiu dozorného orgánu, ktoré sa jej týka. Účelom tohto prostriedku nápravy je súdne preskúmanie právoplatného rozhodnutia orgánu dozoru, ak sa osoba, ktorej sa rozhodnutie týka, domnieva, že rozhodnutie je nesprávne.

Osoba dotknutá právoplatným rozhodnutím dozorného orgánu ho môže napadnúť žalobou na príslušnom súde. Rozhodnutie sa môže týkať napr. výkonu vyšetrovacích, nápravných a povoľovacích právomocí dozorným orgánom alebo nevyhovenia či odmietnutia sťažností. Napadnúť však nemožno opatrenia dozorných orgánov, ktoré nie sú právne záväzné, ako napríklad stanoviská alebo poradenstvo, ktoré poskytol dozorný orgán. Návrh na začatie konania proti dozornému orgánu by sa mal podávať na súdoch členského štátu, v ktorom má dozorný orgán sídlo.

Ak má daný súd informáciu, že konanie týkajúce sa toho istého spracúvania⁸⁷ sa začalo pred príslušným súdom v inom členskom štáte, tento súd kontaktuje pre overenie informácie. Ak sa v inom členskom štáte alebo štátoch také konanie vedie, môže každý súd, ktorý nezačal konať ako prvý, svoje konanie prerušiť, a to zrejme až do právoplatného skončenia takého konania⁸⁸. Dané súdy sa tiež môžu na návrh niektorej zúčastnenej strany prehlásiť za nepríslušné, a to v prospech súdu, ktorý začal konať ako prvý a za predpokladu, že spojenie takých konaní je podľa právneho poriadku posledného menovaného súdu možné.⁸⁹

Podľa recitálu 143 má aj každá fyzická alebo právnická osoba, prípadne aj dotknutý dozorný orgán, ktorý je adresátom takýchto rozhodnutí, právo podať na Súdnom dvore EÚ žalobu o vyhlásenie rozhodnutí Výboru za neplatné.

Dotknuté osoby

Podľa Nariadenia, každá dotknutá osoba má právo na účinný súdny prostriedok nápravy, t.j. na podanie žaloby proti dozornému úradu na príslušnom súde, ak dozorný orgán jej sťažnosť nevybavil alebo neinformoval dotknutú osobu do troch mesiacov o postupe vo vybavení sťažnosti alebo výsledku sťažnosti. Účelom tohto právneho prostriedku je poskytnúť dotknutej osobe možnosť nápravy proti nečinnosti príslušného orgánu dozoru.

Návrh na začatie konania sa podáva na súde členského štátu, v ktorom je orgán zriadený.

Ak sa návrh na začatie konania podáva proti rozhodnutiu dozorného orgánu, ktorému predchádzalo stanovisko alebo rozhodnutie Výboru v rámci mechanizmu konzistentnosti, dozorný orgán takéto stanovisko alebo rozhodnutie postúpi súdu.

Právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi

Podľa Nariadenia má tiež každá dotknutá osoba právo podať žalobu na príslušnom súde, ak sa domnieva, že spracovaním jej osobných údajov v rozpore s Nariadením boli porušené jej práva.

Návrh na začatie konania proti prevádzkovateľovi alebo sprostredkovateľovi sa podáva na súdoch členského štátu, v ktorom má prevádzkovateľ alebo sprostredkovateľ prevádzkareň. Návrh možno podať aj na súdoch členského štátu, v ktorom má dotknutá osoba svoj obvyklý pobyt, pokiaľ

⁸⁷ Napríklad konania s rovnakým predmetom týkajúcim sa spracúvania rovnakým prevádzkovateľom alebo sprostredkovateľom alebo s rovnakým dôvodom žaloby.

⁸⁸ Vid'. čl. 11 ods. 2 Nariadenia; zásada brániaca viesť súbežne rovnaké súdne konania v rôznych členských štátoch a poprípade ich skončiť protikladnými rozhodnutiami.

⁸⁹ Vid'. čl. 81 ods. 3 Nariadenia.

prevádzkovateľom alebo sprostredkovateľom nie je orgán verejnej moci členského štátu konajúci v rámci výkonu verejnej moci.

Právo na náhradu škody a zodpovednosť

Nariadenie ďalej priznáva každej (nielen dotknutej) osobe, ktorá v dôsledku porušenia Nariadenia utrpela hmotnú alebo nehmotnú ujmu, právo na náhradu spôsobenej škody. Subjektom povinným nahradiť škodu bude prevádzkovateľ alebo sprostredkovateľ, a to podľa skutkových okolností prípadu.

Zodpovednosť prevádzkovateľa a sprostredkovateľa za spôsobenú škodu je vymedzená nasledovne:

- Každý *prevádzkovateľ*, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním v rozpore s Nariadením.
- Na druhej strane, *sprostredkovateľ* zodpovedá za škodu spôsobenú spracúvaním, len ak neboli splnené povinnosti, ktoré sa Nariadením ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom.
- Ak sa na tom istom spracúvaní zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ, prípadne prevádzkovateľ aj sprostredkovateľ spoločne, a pokiaľ nesú zodpovednosť za akúkoľvek škodu spôsobenú daným spracúvaním, je každý prevádzkovateľ alebo sprostredkovateľ zodpovedný za celú škodu spoločne a nerozdielne. To znamená, že dotknutá osoba je oprávnená si uplatniť nárok na náhradu škody u ktoréhokoľvek subjektu. Prevádzkovateľ alebo sprostredkovateľ, ktorý nahradil spôsobenú škodu v plnej výške, má právo žiadať od ostatných prevádzkovateľov alebo sprostredkovateľov zapojených do toho istého spracúvania tú časť náhrady škody, ktorá zodpovedá ich podielu na spôsobenej škode.

Prevádzkovateľ alebo sprostredkovateľ sa môžu zbaviť zodpovednosti za škodu, ak sa preukáže, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu.

Návrhy na začatie súdnych konaní na náhradu škody sa podávajú na súdy členského štátu, v ktorom má prevádzkovateľ alebo sprostredkovateľ prevádzkareň. Návrh na začatie takehoto konania možno podať aj na súdoch členského štátu, v ktorom má dotknutá osoba svoj obvyklý pobyt, pokiaľ prevádzkovateľom alebo sprostredkovateľom nie je orgán verejnej moci členského štátu konajúci v rámci výkonu verejnej moci.

Čo ďalej

Okrem samozrejmeho dodržiavania povinností, ktoré Nariadenie ukladá prevádzkovateľom a sprostredkovateľom v súvislosti so spracúvaním osobných údajov, prevádzkovatelia a sprostredkovatelia by mali dôsledne a detailne zmluvne upraviť ich vzájomné práva a povinnosti a z toho vyplývajúce zodpovednostné vzťahy.

Vzhľadom na solidárnu zodpovednosť za celú škodu voči poškodenému subjektu a vzhľadom na medzinárodnú povahu právnych vzťahov je dôležité venovať pozornosť monitorovaniu právnej existencie a ekonomického postavenia zúčastnených subjektov, signalizácii voči nim zahájených konaní a zabezpečeniu a efektívnej náhrade pomernej časti uhradenej škody ostatnými prevádzkovateľmi alebo sprostredkovateľmi.

Ďalšie informácie

Recitály 141 - 147

Články kapitoly VIII

Lekcia 15 z 16

Sankcie a odchýlky

V texte sa dozviete:

Dôležité zmeny

- Nariadenie prináša podstatné zvýšenie maximálnych pokút za porušenie povinností súvisiacich s ochranou osobných údajov:
 - v prípadoch závažnejšieho porušenia Nariadenia je maximálna výška pokuty 20.000.000,- EUR alebo 4% celkového svetového ročného obratu spoločnosti za predchádzajúci účtovný rok (podľa toho, ktorá suma je vyššia); doposiaľ max. do 200 tis. EUR;
 - v ostatných prípadoch je maximálna výška pokuty 10.000.000,- EUR alebo 2% celkového svetového ročného obratu spoločnosti za predchádzajúci účtovný rok (podľa toho, ktorá suma je vyššia); doposiaľ max. do 50 tis. EUR;
- Za porušenie Nariadenia dozorný orgán nie je povinný pokutu uložiť; ak je to však vzhľadom na okolnosti prípadu vhodné a účelné, môže uložiť aj iný druh sankcie (popri pokute alebo namiesto nej).

Compliance: Akčný plán

- Vykonanie auditu spracúvania osobných údajov pre zistenie, ktoré spracovateľské operácie nie sú v súlade s Nariadením;
- Identifikovanie najrizikovejších oblastí a vykonanie opatrení na zmiernenie rizika uloženia pokút;
- Zváženie možnosti uzavrieť poisťovnú zmluvu na poistenie rizík spojených so spracúvaním osobných údajov.

K sankciám

Správne pokuty

Dozorné orgány sú povinné pri rozhodovaní o uložení pokuty a jej výške náležite zohľadniť skutočnosti, ako napr. povaha, závažnosť a trvanie porušenia (pričom prihliada na povahu, rozsah alebo účel spracúvania, ako aj na počet dotknutých osôb, na ktoré malo vplyv a rozsah škody, ktorú utrpeli), úmyselný alebo nedbanlivostný charakter porušenia, kroky, ktoré prevádzkovateľ alebo sprostredkovateľ podnikol s cieľom zmierniť škodu, miera spolupráce s dozorným orgánom, kategórie osobných údajov, ktorých sa porušenie týka a pod.

Ak prevádzkovateľ alebo sprostredkovateľ úmyselne alebo z nedbanlivosti tými istými alebo súvisiacimi spracovateľskými operáciami poruší viacero ustanovení Nariadenia, celková suma správnej pokuty nesmie presiahnuť výšku stanovenú za najzávažnejšie porušenie.

V každom jednotlivom prípade musí byť ukládanie pokút účinné, primerané a odrádzajúce. Nariadenie kategorizuje rôzne druhy porušení do dvoch hlavných skupín, a to podľa závažnosti porušenia, ktorej zodpovedá rôzna maximálna výška správnej pokuty:

Správna pokuta do výšky 10.000.000,- EUR alebo 2% obratu

Do prvej kategórie Nariadenie zaraďuje druhy porušenia, ktorému zodpovedá sankcia v maximálnej výške 10.000.000,- EUR alebo v prípade spoločnosti až vo výške 2% celkového svetového ročného

obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia. Sem patria nasledovné delikty:

- spracúvanie osobných údajov maloletého v súvislosti so službami informačnej spoločnosti (čl. 8);
- spracúvanie bez potreby identifikácie (čl. 11);
- prijatie technických a organizačných opatrení za účelom zabezpečenia špecificky navrhnutých a štandardnej ochrany údajov (čl. 25);
- povinnosť spoločných prevádzkovateľov dohodnúť si vzájomnú zodpovednosť za plnenie povinnosti podľa Nariadenia (čl. 26);
- povinnosť ustanoviť zástupcu prevádzkovateľov alebo sprostredkovateľov, ktorí nie sú usadení v Únii (čl. 27);
- povinnosti spojené pri ustanovení sprostredkovateľov a povinnosti sprostredkovateľov (čl. 28 a 29);
- povinnosť uchovávať záznamy o spracovateľských činnostiach (čl. 30);
- povinnosť spolupracovať s dozornými orgánmi (čl. 31);
- povinnosť zabezpečiť bezpečnosť údajov a nahlasovať porušenie (čl. 32 - 36);
- povinnosti súvisiace s ustanovením zodpovednej osoby (čl. 37 - 39);
- povinnosti certifikačného subjektu (čl. 42 a 43); a
- povinnosti monitorujúceho subjektu (čl. 41 ods. 4).

Správna pokuta do výšky 20.000.000,- EUR alebo 4% obratu

Do druhej kategórie spadajú delikty, za ktoré Nariadenie umožňuje uložiť sankciu do výšky 20.000.000,- EUR alebo v prípade spoločnosti až do výšky 4% celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia. Sem patria nasledovné delikty:

- povinnosti súvisiace so zásadami spracúvania údajov vrátane súhlasu (čl. 5 – 7 a 9);
- porušenie práv dotknutých osôb (čl. 12 - 22);
- porušenie povinností pri prenose údajov do tretej krajiny alebo medzinárodnej organizácie (čl. 44 - 49);
- akékoľvek porušenie povinností podľa práva členského štátu prijatého podľa kapitoly IX; a
- nesplnenie príkazu súvisiaceho s tokom osobných údajov nariadeného dozorným orgánom a iné súvisiace delikty (čl. 58).

Zatiaľ ešte platná Smernica splnomocňuje členské štáty, aby prijali vhodné opatrenia na zabezpečenie jej uplatňovania a najmä aby stanovili sankcie za porušenie vnútroštátnych predpisov, prijatých na jej základe.⁹⁰

Slovenský zákonodarca tak učinil v IV. hlave „Sankcie a zverejnenie porušenia“, §§ 67 – 71 zákona o ochrane osobných údajov. Prevádzkovateľovi a sprostredkovateľovi môže byť za porušenie zákona uložená sankcia od 300 – 200.000,- EUR, a fyzickej osobe, ktorá nemá postavenie prevádzkovateľa ani sprostredkovateľa, môže byť uložená pokuta vo výške 150 – 2.000,- EUR.

⁹⁰ Čl. 24 Smernice.

Iné sankcie

Dozorný orgán má okrem právomoci uložiť pokutu podľa vyššie uvedených zásad k dispozícii aj možnosť uloženia iných druhov sankcií, a to:

- upozornenie prevádzkovateľa alebo sprostredkovateľa na to, že plánované spracovateľské operácie pravdepodobne porušia ustanovenia Nariadenia;
- napomenutie prevádzkovateľov alebo sprostredkovateľov, ak spracovateľské operácie porušili ustanovenia Nariadenia;
- nariadenie prevádzkovateľovi alebo sprostredkovateľovi, aby vyhovel žiadostiam dotknutej osoby o uplatnenie jej práv podľa Nariadenia;
- nariadenie prevádzkovateľovi alebo sprostredkovateľovi, aby svoje spracovateľské operácie zosúladiť podľa potreby určeným spôsobom a v rámci určenej lehoty s ustanoveniami Nariadenia;
- nariadenie prevádzkovateľovi, aby porušenie ochrany osobných údajov oznámil dotknutej osobe;
- nariadenie dočasného alebo trvalého obmedzenia vrátane zákazu spracúvania;
- nariadenie opravy alebo vymazania osobných údajov alebo obmedzenia spracúvania a informovanie príjemcov, ktorým boli osobné údaje poskytnuté, o takýchto opatreniach;
- odňatie certifikácie alebo nariadenie certifikačnému subjektu, aby odňal certifikáciu, alebo nariadenie certifikačnému subjektu, aby nevydal certifikáciu, ak nie sú splnené alebo už nie sú splnené požiadavky na certifikáciu;
- nariadenie pozastavenia toku údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii.

Trestný postih

Nariadenie v čl. 84 a v recitáli 149 ukladá členským štátom povinnosť stanoviť pravidlá pre iné, aj trestné sankcie, za porušenie ustanovení Nariadenia,⁹¹ vrátane sankcie odobratia ziskov, získaných porušením Nariadenia. Vždy by však mala byť rešpektovaná zásada zákazu uloženia dvoch a viac sankcií za rovnaké konanie porušujúce Nariadenie.

Slovenský trestný zákon⁹² už teraz zakotvuje skutkovú podstatu neoprávneného nakladania s osobnými údajmi s trestom odňatia slobody až na dva roky⁹³.

Odchýlky a osobitné situácie spracúvania

Nariadenie priznáva členským štátom právo odchýliť sa od znenia Nariadenia, resp. (kde Nariadenie príslušné ustanovenia neobsahuje) prijať vlastnú právnu úpravu ohľadne nasledovných záležitostí:

- oblasť vnútornej bezpečnosti, predchádzania a zisťovania trestných činov;
- oblasť slobody prejavu a práva na informácie;
- oblasť prístupu verejnosti k úradným dokumentom;
- spracúvanie národného identifikačného čísla (rodné číslo);

⁹¹ Čl. 84 Nariadenia.

⁹² Zákon č. 300/2005 Z.z. trestný zákon.

⁹³ Ustanovenie § 374 trestného zákona: „(1) Kto neoprávnené poskytne, sprístupní alebo zverejní osobné údaje o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo osobné údaje o inom získané v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie a tým poruší všeobecne záväzným právnym predpisom ustanovenú povinnosť, potrestá sa odňatím slobody až na jeden rok. (2)...“

- spracúvanie osobných údajov v pracovnoprávných vzťahoch;
- oblasť archivácie vo verejnom záujme, vedeckého alebo historického výskumu alebo štatistické účely; a
- mlčanlivosť súvisiaca s profesijným tajomstvom.

Čo ďalej

Prevádzkovateľom a sprostredkovateľom odporúčame vykonať audit pre identifikáciu najrizikovejších oblastí spracovateľských operácií a následne stanoviť prioritu krokov na zmiernenie rizika uloženia správnych pokút alebo iných sankcií. Za týmto účelom je vhodné tiež posúdiť povinnosť náhrady škody v súvislosti so zmluvami s obchodnými partnermi, zákazníkmi alebo dodávateľmi, ktorých sú prevádzkovatelia alebo sprostredkovatelia zmluvnými stranami, a prípadne upraviť zodpovednostné vzťahy medzi stranami.

Pre účely prenesenia rizík je možné zvážiť poistenie zodpovednosti za škodu spôsobenú spracovateľskou činnosťou.

Ďalšie informácie

Recitály 148 - 165

Články 83 – 84 a články kapitoly IX

Lekcia 16 z 16

Praktické kroky pre zabezpečenie súladu a minimalizáciu rizika sankcií

Zhrnutie Školy ochrany osobných údajov

Počas uplynulých mesiacov sme Vám prinášali pravidelné informácie ohľadne novej právnej úpravy spracúvania osobných údajov, ktorá podstatne mení podmienky zákonnosti spracúvania. Nariadenie okrem iného rozširuje teritoriálny dosah európskeho štandardu ochrany osobných údajov, pričom ambíciou novej právnej úpravy je zabezpečiť, aby sa ochrana osobných údajov vzťahovala na dotknuté osoby nachádzajúce sa v Únii aj v prípade, ak sa ich údaje spracúvajú mimo štátov Únie subjektmi usadenými mimo Únie.

Nariadenie ďalej najmä:

- ukladá prevádzkovateľom, aby pristupovali k zabezpečeniu zákonnosti spracúvania proaktívne a boli schopní dozorným orgánom preukázať, že vykonali všetky potrebné kroky na zabezpečenie súladu s Nariadením;
- upravuje zásady, ktorými sa majú prevádzkovatelia riadiť pri spracúvaní osobných údajov pri začatí spracúvania a kedykoľvek počas neho;
- mení podmienky pre platné udelenie súhlasu dotknutej osoby so spracúvaním osobných údajov;
- podstatne rozširuje práva dotknutých osôb (napr. o právo na výmaz údajov z on-line prostredia alebo o právo na prenosnosť údajov);
- ukladá prevádzkovateľom extenzívnu informačnú povinnosť voči dotknutým osobám a povinnosť aktívne komunikovať s dotknutými osobami v odôvodnených prípadoch;
- zvyšuje štandard bezpečnostných opatrení na ochranu údajov a ukladá prevádzkovateľom aj sprostredkovateľom povinnosť oznámiť dozornému orgánu a prípadne dotknutým osobám porušenie Nariadenia;
- prináša nové inštitúty, ktorými prevádzkovatelia môžu zabezpečiť a preukázať súlad, a to kódexy správania a certifikáciu;
- upravuje povinnosť uchovávať záznamy o spracovateľských činnostiach, vykonať posúdenie vplyvu na ochranu údajov a vopred konzultovať spracúvanie s dozorným orgánom;
- upravuje podmienky prenosu údajov do tretích krajín a rozširuje možnosti pre zabezpečenie súladu prenosu;
- zavádza systém jednotného kontaktného dozorného úradu pre cezhraničné spracúvanie, ktoré prevádzkovateľ vykonáva v rámci Únie;
- zakotvuje podstatne vyššie sankcie za porušenie Nariadenia oproti pôvodnej právnej úprave.

Časový harmonogram praktických krokov na dosiahnutie súladu

Nariadenie nadobudne účinnosť o necelých 12 mesiacov, presnejšie dňa 25. mája 2018. S ohľadom na závažnosť zmien, rozsiahlosť problematiky a výšku hroziacich sankcií sa odporúča prevádzkovateľom, ktorí osobné údaje spracúvajú (t.j. napr. ktorí zamestnávajú fyzické osoby), bezodkladne pristúpiť k praktickým krokom, ktoré sú nevyhnutné na implementovanie požiadaviek Nariadenia do vnútorných spracovateľských procesov.

Zoznam nevyhnutných krokov, ako aj návrh realistického časového harmonogramu, uvádzame nižšie. Odporúča sa riadne zdokumentovať priebeh celého projektu zabezpečovania súladu s Nariadením pre účely prípadnej potreby preukázať odbornú starostlivosť dozornému úradu.

✓ **Čo: Určenie tímu zamestnancov a finančných a technických prostriedkov pre účely projektu**

Kedy: júl – august 2017

Ako: Najskôr je nevyhnutné poveriť zamestnanca / zamestnancov, ktorý/-í bude/-ú mať na zodpovednosti (a v náplni práce) zabezpečenie súladu spracovateľských operácií prevádzkovateľa s Nariadením. Uvedené platí aj vtedy, ak prevádzkovateľ mieni poveriť vypracovaním projektu súladu externého dodávateľa; v tom prípade bude za prevádzkovateľa tento zodpovedný zamestnanec komunikovať s dodávateľom služieb. Typicky môže ísť o pracovníka právneho alebo HR oddelenia, pričom na technickú podporu bude účelné zabezpečiť súčinnosť a informovanosť IT špecialistu.

Tomuto projektovému tímu bude potrebné zabezpečiť všetky potrebné informácie a školenia na to, aby sa vedel zorientovať v problematike a poznal svoje úlohy.

Nadnárodné organizácie alebo spoločnosti určia, či súlad s Nariadením budú riešiť na lokálnej (národnej) úrovni, alebo lokálny tím bude spolupracovať s centrárou.

✓ **Čo: Zistenie spracovateľských operácií**

Kedy: august – október 2017

Ako: Prevádzkovateľ je povinný zmapovať (i) aké osobné údaje spracúva, (ii) aké kategórie dotknutých osôb sú pre neho relevantné a (iii) aké spracovateľské operácie s osobnými údajmi vykonáva. Tieto vstupné informácie je nevyhnutné zistiť s dôrazom na detail, presnosť, aktuálnosť a úplnosť a je potrebné tieto výstupy zachytiť písomne, nakoľko budú slúžiť ako východisko pre ďalšie aktivity.

✓ **Čo: Analýza nedostatkov vo svetle novej legislatívy**

Kedy: október – december 2017

Ako: Prevádzkovateľ by mal vykonať dôkladnú analýzu existujúcich interných postupov všetkých zainteresovaných oddelení u prevádzkovateľa (napr. HR oddelenie, IT oddelenie znalé softvérových riešení vo firme, odd. styku so zákazníkmi, recepčných identifikujúcich návštevy, odd. vnútornej bezpečnosti, správcov kamerových systémov CCTV a iných monitorovacích zariadení a pod.) – ak majú kontakt s osobnými údajmi. Rovnako je potrebná analýza dokumentov upravujúcich tieto interné postupy, ak také prevádzkovateľ implementoval.

Zo zistení je potrebné vypracovať písomnú správu s uvedením identifikovaných nedostatkov a rizík a s uvedením návrhov na ich zmiernenie. So správou by sa malo oboznámiť najvyššie vedenie prevádzkovateľa.

✓ **Čo: Zodpovedná osoba a sprostredkovatelia**

Kedy: október 2017 – december 2017

Ako: Prevádzkovateľ je povinný ďalej preveriť, či bude potrebné k dátumu účinnosti Nariadenia poveriť zodpovednú osobu.

Je potrebné vykonať revíziu zmlúv so sprostredkovateľmi a prípadnými inými subjektmi za účelom zabezpečenia súladu zmluvných ustanovení s Nariadením. Odporúča sa zanalyzovať aj zodpovednostné vzťahy s týmito subjektmi týkajúce sa oblasti ochrany osobných údajov, a z nich vyplývajúce riziká vzniku nárokov na náhradu škody a prípadných sankcií.

✓ **Čo: Vytvorenie alebo aktualizovanie interných smerníc o ochrane osobných údajov**

Kedy: január 2018 – marec 2018

Ako: Je potrebné, aby ku dňu účinnosti Nariadenia mal prevádzkovateľ pripravenú zrevidovanú, prípadne novo vytvorenú internú dokumentáciu, ktorú požaduje Nariadenie. Uvedené bude zahŕňať napr. oznámenia o spracúvaní osobných údajov určené dotknutým osobám, registratúrne plány s uvedením doby uchovávania jednotlivých dokumentov obsahujúcich osobné údaje, súhlasy so spracúvaním osobných údajov, postupy určené pre prípad žiadostí o prístup k údajom, zásady ochrany osobných údajov, postupy pre výmaz či blokovanie údajov a pod.

✓ **Čo: Implementovanie vnútorných procesov**

Kedy: marec 2018 – máj 2018

Ako: Prevádzkovateľ je povinný implementovať vnútorné procesy záväzné pre zamestnancov narábajúcich s osobnými údajmi a riadne ich vyškoliť ohľadne úloh, ktoré sa od nich budú dňom účinnosti Nariadenia vyžadovať. Tieto postupy by sa mali týkať všetkých eventualít, ktoré sa v priebehu spracúvania môžu vyskytnúť, napr. pre prípad porušenia Nariadenia, v prípade žiadostí dotknutých osôb o prístup k údajom, o vymazanie údajov alebo ich blokovanie a pod.

Zamestnancov nakladajúcich s osobnými údajmi je potrebné detailne a preukázateľne oboznámiť s povinnosťou mlčanlivosti a s prijatými internými dokumentmi v oblasti spracúvania, a poučiť ich, ako sa ktorý dokument používa, poučiť ich o spôsobe komunikácie s dotknutými osobami a pod.

Samozrejmosťou je, že všetky potrebné spracovateľské operácie by mali byť technicky zrealizovateľné, k čomu je potrebné zabezpečiť služby IT špecialistu.

✓ **Čo: Školenie zamestnancov**

Kedy: február 2018 – máj 2018

Ako: Prevádzkovateľ je povinný za účelom zvýšenia povedomia o ochrane osobných údajov zabezpečiť potrebné školenia zamestnancov narábajúcich s osobnými údajmi. Od ich odbornosti bude priamo závisieť miera rizika a prípadných sankcií, ktoré za porušenie Nariadenia hrozia, a ktoré môžu byť v určitých prípadoch uložené prevádzkovateľovi až do výšky 20 mil. EUR alebo 4% celkového ročného obratu, podľa toho, ktorá suma je vyššia.

Kde začať

Tím odborníkov advokátskej kancelárie Balcar, Polanský & Spol. s.r.o. je pripravený Vám poskytnúť bližšie informácie ohľadne vyššie uvedených povinností alebo akýchkoľvek iných aspektov blížiacej sa účinnosti Nariadenia. Neváhajte sa preto obrátiť na niektorého z nižšie uvedených advokátov, alebo na Váš zvyčajný kontakt v našej advokátskej kancelárii.

Našu odbornosť, vrátane medzinárodnej certifikácie v oblasti ochrany osobných údajov, si môžete overiť tu:

http://www.balcarpolansky.cz/files/251/Focussed%20on%20DP_SK.pdf

Kontaktná osoba

Pre ďalšie informácie prosím kontaktujte:

Slovensko:



JUDr. Helga Madárová,
CIPP/E, CIPM
Advokátka | Certified Intl. Privacy
Professional/Europe | Certified
Intl. Privacy Manager
Tel.: +421 220 251 311
Mobil: +421 917 092 076
helga.madarova@bapol.sk

Česká republika:



JUDr. Jaroslav Srb
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz