Barbora Lániková

GDPR v praxi

PRAKTICKÁ PRÍRUČKA S KOMPLETNÝMI VZORMI PRE JEDNODUCHÉ ZAVEDENIE GDPR DO PRAXE

2. aktualizované vydanie

Lanikova Group, s.r.o.

JUDr. Barbora Lániková

GDPR v praxi, 2., aktualizované vydanie
Praktická príručka pre zavedenie GDPR do praxe

Vydala Advokátska kancelária Lanikova Group, s.r.o.
Grösslingová 8, Bratislava
Tel.č.: 0948/264 244
Web: lanikovagroup.sk
Email: info@lanikovagroup.sk

Počet strán : 224
Druhé vydanie, Bratislava 2019
Tlač: Projects, s.r.o.
ISBN: 978-80-973028-1-8

O autorovi

JUDr. Barbora Lániková je advokátka v advokátskej kancelárii Lanikova Group, s.r.o. a odborníčka na oblasť ochrany osobných údajov. Publikovala celú radu odborných článkov na tému ochrany osobných údajov a IT práva v denníkoch, časopisoch a na internetovej stránke lanikovagroup.sk. Je lektorkou na in-house školeniach, prednáškach a konferenciách.

Pri zostavovaní tejto knihy vychádzala z bohatých skúseností v oblasti ochrany osobných údajov a IT práva. Zaviedla pravidlá ochrany osobných údajov do praxe a vypracovala kompletnú dokumentáciu k ochrane osobných údajov pre viac ako 500 firiem a orgánov verejnej správy. Pre svojich klientom vykonáva aj funkciu externej zodpovednej osoby.

Má iný pohľad na právo. Verí, že právo má byť prístupné pre všetkých, a preto vytvorila unikátny online právny softvér virtualnypravnik.sk, kde si môžu podnikatelia riešiť svoje právne veci rýchlo a jednoducho.

Predslov

GDPR bol pre mnohých strašiakom. Podnikatelia sa obracali na našu advokátsku kanceláriu a žiadali nás o pomoc. Zmenám v oblasti ochrany osobných údajov nerozumeli, nemali k dispozícii žiadne návody či vzory. Nemohli sme pomôcť každému, a preto sme sa rozhodli napísať zrozumiteľnú príručku pre rýchle a jednoduché zavedenie GDPR do praxe. Jej súčaťou boli kompletné vzory, podľa ktorých zvládol GDPR takmer každý.

Množstvo pozitívnych recenzií a poďakovaní čitateľov mojej prvej knihy, ma viedlo k jej aktualizácii. Od účinnosti GDPR v máji 2018 sa toho veľa zmenilo. Prax zodpovedala niektoré otázky a rozhodnutia súdov dotvorili právny rámec ochrany osobných údajov. Kompetentné orgány vydali množstvo usmernení a stanovísk, ktoré spresňujú a vysvetľujú niektoré aplikačné problémy, prípadne dopĺňajú zákon.

Aktualizovanú knihu GDPR V PRAXI musí mať každý, kto chce mať GDPR v poriadku aj po zohľadnení všetkých zmien, ktoré nastali v priebehu uplynulého roka. Kniha je omnoho rozsiahlejšia. Je rozdelená na všeobecnú a osobitnú časť. Všeobecná časť zhrňuje všetko podstatné o spracúvaní osobých údajov. Osobitná časť podrobne vysvetľuje osobitosti spracúvania osobných údajov v najbežnejších agendách, ktoré bežný podnikateľ prevádzkuje. Podrobne sa zaoberá personálnou agendou, e-shopom, marketingom, či kamerovým systémom.
V neposlednom rade aktualizované znenie poukazuje na hrozbu pokuty pri nesprávnom riešení GDPR a popisuje výsledky kontrol na Slovensku, ale aj v iných štátoch EÚ.

Verím, že aktualizovaná verzia knihy bude motivovať čitateľov k tomu, aby problematike ochrany osobných údajov venovali väčšiu pozornosť, nakoľko ide o závažný zásah do osobných práv človeka.

Záverom sa chcem poďakovať Nine Nagyovej, ktorá mi pomáhala pri zostavovaní aktualizácie tejto knihy a prispeva svojimi vedomosťami v oblasti ochrany osobných údajov.

Prajem príjemné čítanie.

Barbora Lániková
autor

virtualnypravnik.sk

ONLINE PRÁVNY SOFTVÉR PRE FIRMY NA JEDNODUCHÉ A RÝCHLE VYTVÁRANIE PRÁVNYCH DOKUMENTOV A SPRÁVU PRÁVNEJ AGENDY

Ušetrite až 95% nákladov na právnika. Virtuálny právnik vyrieši váš právny problém za pár eur. Odpoviete na jednoduché otázky a virtuálny právnik vygeneruje všetky právne dokumenty a spracuje vám konkrétny postup.

Lanikova Group advokátska kancelária

Obsah

VŠEOBECNÁ ČASŤ

Úvod

Pojmy ako osobné údaje, ochrana osobných údajov či porušenie ochrany osobných údajov sú v posledných rokoch veľmi skloňované. Ľudia si čoraz viac uvedomujú, akú majú ich osobné údaje hodnotu, ako môžu byť informácie o ich osobe, taktiež o ich správaní (napr. na internete) zneužité.

Všeobecné nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb v súvislosti so spracúvaním osobných údajov a o voľnom pohybe týchto údajov (pozn.: po angl. General Data Protection Regulation, skr.: GDPR) je v platnosti od 25. mája 2018. Od tohto dátumu sa ním riadia všetky firmy, orgány verejnej správy a iné organizácie. Na základe tohto nariadenia sa prijal zákon č. 18/2018 Z. z. o ochrane osobných údajov, ktorý nadobudol účinnosť v ten istý deň.
Nové predpisy nahradili dovtedajšiu právnu úpravu, ktorú predstavovala smernica Európskeho parlamentu a Rady (EÚ) 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov a zákona č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších právnych predpisov.
Každý, kto spracúva osobné údaje, musí v praxi už implementovať nové pravidlá o ochrane osobných údajov. Avšak ako treba správne postupovať? Jasne a jednoducho vás prevedieme celým procesom prechodu na nové podmienky spracúvania osobných údajov a na desiatkach príkladov vám vysvetlíme, ako treba jednotlivé povinnosti zaviesť do praxe. Táto kniha sa skladá z dvoch častí:

- všeobecná časť,
- osobitná časť.

Vo všeobecnej časti si podrobne vysvetlíme najmä:
- základne pojmy,
- základné zásady,
- právne základy, na akých môžete spracúvať osobné údaje,
- povinnosti, ktoré vám vyplývajú z GDPR,
- aké práva majú dotknuté osoby,
- čo robiť v prípade kontroly kompetentnými orgánmi.

V osobitnej časti sa zameriame aj na osobitné oblasti práva a podnikania, ktorých sa taktiež týka GDPR. Vysvetlíme vám predovšetkým, akým spôsobom sa GDPR vzťahuje na personálnu agendu, účtovníctvo, marketing a na mnohé iné oblasti. Poukážeme aj ročný vývoj problematiky ochrany osobných údajov od účinnosti nového nariadenia, na sankcie, ktoré sa vzťahujú na nedodržanie nariadenia, ako aj na najčastejšie chyby prevádzkovateľov.
Ku knihe si môžete kúpiť balík kompletných vzorových dokumentov, podľa ktorých si GDPR spracujete sami za pár hodín. Ak máte obavy, či budete vedieť zaviesť GDPR do praxe správne, pomôžeme vám s tým. Objednajte si balík GDPR, ktorý sa hodí presne na váš typ podnikania a GDPR vám vyriešime my. Problematiku ochrany osobných údajov sme za posledných 10 rokov riešili komplexne pre stovky klientov, ktorí boli spokojní, a preto veríme, že spoluprácu s nami oceníte i vy.

Čo sa môže stať, ak nebudete GDPR brať vážne? Brať nové pravidlá o ochrane osobných údajov na ľahkú váhu sa vám skutočne nevyplatí. Sankcie sú likvidačné. Pokiaľ si povinnosti vyplývajúce z GDPR a zákona č. 18/2018 Z. z. o ochrane osobných údajov nesplníte, môžete dostať pokutu až do výšky 20 mil. eur alebo vo výške 4 % z celosvetového obratu.

Nepodceňujte to a začnite sa s nami pripravovať už dnes. Poradíme vám, ako vykonať audit spracúvania osobných údajov a na základe zistených nedostatkov prijať potrebné organizačné a technické zmeny. Následne vám poskytneme v elektronickej forme všetky dokumenty, ktoré podľa GDPR musíte mať. S našou pomocou budete na GDPR riadne pripravení.

Kapitola 1
Aké právne predpisy musíte poznať?

1.1 Čo predchádzalo prijatiu GDPR?

Ochrana osobných údajov nie je nová oblasť práva. V právnom poriadku Slovenskej republiky spracúvanie osobných údajov najprv upravoval zákon č. 428/2002 Z. z. o ochrane osobných údajov. V roku 2013 ho vystriedal nový zákon o ochrane osobných údajov č. 122/2013 Z. z. a v súčasnosti je to zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Prijatie tohto zákona sa viaže na GDPR čiže všeobecné nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.

Do účinnosti nariadenia GDPR národná právna úprava ochrany osobných údajov na Slovensku vychádzala z európskej právnej úpravy, a to zo Smernice Európskeho parlamentu a Rady (EÚ) 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Smernica na rozdiel od nariadenia nebola priamo aplikovateľná na naše právne vzťahy bez toho, aby sa zaviedla do nášho právneho poriadku. Fyzické a právnické osoby v jednotlivých členských štátoch EÚ sa nemohli priamo dovolávať svojich práv vyplývajúcich zo smernice na súdoch či orgánoch verejnej správy. Aby sa mohli odvolať na ustanovenia smernice, bolo potrebné, aby členské štáty smernicu implementovali do svojho právneho poriadku.

Keďže každý členský štát si mohol zaviesť pravidlá smernice do svojho právneho poriadku po svojom, právna úprava ochrany osobných údajov bola v jednotlivých členských štátoch EÚ rozdielna. Tento nepriaznivý

stav vo veľkej miere odstraňuje GDPR. Aby sa fyzické a právnické osoby mohli priamo dovolávať svojich práv vyplývajúcich z ustanovení GDPR, bola zvolená práve forma nariadenia. Preto už nie je potrebná implementácia GDPR do právneho poriadku jednotlivých krajín. Členské štáty síce mali povinnosť dať národné právne predpisy o ochrane osobných údajov do súladu s GDPR, avšak ak by tak aj neurobili, ich občanov by sa to nedotklo. Nariadenie, ktoré má prednosť pred zákonom, sa na nich priamo vzťahuje.

Potreba zmeny právnej úpravy ochrany osobných údajov vyplynula zo zmeny spoločnosti a jej postupnej elektronizácie. Pôvodné právne predpisy už nezodpovedali potrebám súčasnej doby. GDPR odzrkadľuje inovatívne technické prostriedky spracúvania údajov, nutnosť posilnenia práv dotknutých osôb a potrebu zjednotenia právnej úpravy v celej EÚ.

Vo všeobecnosti možno povedať, že GDPR je založená na dvoch hlavných princípoch. Ide o princíp zodpovednosti prevádzkovateľa a o princíp založený na riziku. Prvý spomínaný princíp vyjadruje zodpovednosť prevádzkovateľa za dodržiavanie základných zásad spracúvania osobných údajov a za preukázanie ich dodržiavania. Princíp založený na riziku znamená, že prevádzkovateľ už pri samotnom vymedzení účelu, prostriedkov spracúvania osobných údajov a bezpečnostných opatrení musí vychádzať z rizika, ktoré spracúvanie osobných údajov predstavuje pre dotknuté osoby. V závislosti od miery rizika vyplýva pre prevádzkovateľa viac či menej povinností.[1]

1.2 Nariadenie o ochrane údajov

Potreba harmonizácie oblasti ochrany osobných údajov v celej EÚ, ako aj nutnosť posilnenia práv dotknutých osôb a zvýšenia bezpečnosti spracúvaných údajov viedli k prijatiu nového Všeobecného nariadenia o ochrane údajov – GDPR.
Všeobecné nariadenie o ochrane údajov predstavuje právny rámec oblasti ochrany osobných údajov, ktorý platí v celej EÚ. Jeho hlavným cieľom je prehĺbiť práva osôb, ktorých osobné údaje sa spracúvajú,

1 Nezmar, L. (2017). GDPR: Praktický průvodce implementací. Grada Publishing.

a zabezpečiť ochranu ich údajov pred neoprávneným zásahom. GDPR stavia na predchádzajúcich pravidlách ochrany osobných údajov zakotvených v spomínanej smernici. Základné zásady a princípy spracúvania osobných údajov zostali bez podstatných zmien, nariadenie ich len ďalej rozpracúva a spresňuje.
GDPR od 25. mája 2018 priamo stanovuje povinnosti pre subjekty, ktoré spracúvajú osobné údaje a práva pre tie fyzické osoby, ktorým dané subjekty osobné údaje spracúvajú. Mnohé z povinností sú od účinnosti nariadenia v rámci Slovenskej republiky úplne nové. Ide najmä o tieto povinnosti:

- vedenie záznamov o spracovateľských činnostiach,
- posúdenie vplyvov na ochranu osobných údajov,
- absolvovanie konzultácie na Úrade na ochranu osobných údajov SR,
- poverenie zodpovednej osoby,
- oznámenie porušenia bezpečnosti osobných údajov.

Rozsah povinností prevádzkovateľa závisí od podmienok spracúvania osobných údajov v organizácii a od miery rizika, ktoré toto spracúvanie predstavuje v súvise s právami a slobodou dotknutých osôb. Niektoré z uvedených povinností sa totiž vzťahujú len na prípady, keď spracúvanie osobných údajov predstavuje pre dotknutú osobu riziko alebo vysoké riziko v súvise s jej právami a slobodou.

1.3 Usmernenia pracovnej skupiny WP29

Výklad k jednotlivým problematickým oblastiam aplikácie GDPR poskytujú usmernenia pracovnej skupiny WP29. Medzi významné usmernenia patria napríklad:

- Usmernenia ohľadom práva na prenosnosť údajov;
- Usmernenia na určenie vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa;
- Usmernenia týkajúce sa zodpovedných osôb;
- Usmernenia na automatizované spracúvanie osobných údajov a profilovanie;
- Usmernenia ohľadom oznámenia o porušení ochrany osobných

údajov;
- Usmernenia týkajúce sa posúdenia vplyvu na ochranu osobných údajov.

Usmernenia pracovnej skupiny WP29 sú vypracované v anglickom jazyku a zverejnené na oficiálnej internetovej stránke <http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360>. Jednotlivé usmernenia dal Úrad na ochranu osobných údajov SR (ÚOOÚ SR) preložiť do slovenského jazyka a zverejnil ich na svojich internetových stránkach www.dataprotection.gov.sk.

1.4 Zákon o ochrane osobných údajov

Zmena pravidiel ochrany osobných údajov sa odzrkadľuje aj v právnom poriadku Slovenskej republiky. Hoci je nariadenie priamo aplikovateľné na právne vzťahy v rámci členských štátov EÚ, a teda aj na území Slovenskej republiky, právne predpisy SR bolo potrebné dať do súladu s GDPR.

Do úvahy prichádzali dva spôsoby, ako dať doterajšiu právnu úpravu Slovenskej republiky v oblasti ochrany osobných údajov do súlady s GDPR, a to novelizáciou doterajšieho zákona č. 122/2013 Z. z. o ochrane osobných údajov s odkazmi na nariadenie alebo prijatím úplne nového zákona.

Zákonodarný orgán zvolil druhú možnosť, a tak s účinnosťou od 25. mája 2018 nahradil pôvodný zákon nový – a to zákon č. 18/2018 Z. z. o ochrane osobných údajov.

Zákon č. 18/2018 Z. z. bol ku dňu vydania tejto publikácie zmenený len raz, a to novelou č. 221/2019 Z. z., ktorou sa mení a dopĺňa zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii) a ktorou sa menia a dopĺňajú niektoré zákony. Táto zmena však vôbec nebola rozsiahla a netýkala sa ani prevádzkovateľa ani dotknutej osoby. Vzťahuje sa len na predsedu a podpredsedu Úradu na ochranu osobných údajov SR pri preukazovaní bezúhonnosti.

1.5 Kedy zákon a kedy nariadenie?

Zákon č. 18/2018 Z. z. je vo veľkej miere zhodný s GDPR. Neobsahuje veľké odlišnosti, ale ak áno, týkajú sa napríklad Úradu na ochranu osobných údajov SR či iných právnych inštitútov, ktorých úpravu aj samotné GDPR prenecháva na úpravu v jednotlivých členských štátoch.
Aký je vzťah GDPR a zákona č. 18/2018 Z. z. o ochrane osobných údajov? Zákon nariadenie nenahrádza, platí popri ňom. V niektorých častiach, napríklad v súvislosti so zákonnou úpravou týkajúcou sa Úradu na ochranu osobných údajov SR, zákon nariadenie dopĺňa. Ak by došlo k nezrovnalostiam medzi zákonom a nariadením, nariadenie má pred naším vnútroštátnym zákonom prednosť.
Väčšina prevádzkovateľov rieši otázku – kedy použiť nariadenie a kedy zákon? Úrad na ochranu osobných údajov SR k tomu zaujal jednoznačné stanovisko. Väčšina spracovateľských operácií má spadať pod režim nariadenia. Na ostatné oblasti, ktoré nie sú upravené právom únie, sa má vzťahovať zákon. Zjednodušene možno vysvetliť prípady, keď sa aplikuje nariadenia a keď zákon, nasledovne:

- ☞ Ak pôjde o také spracúvanie osobných údajov, ktoré spadá pod právo únie, použije sa nariadenie, niektoré časti zákona (1. časť, 4. až 6. časť) a osobitné právne predpisy.
- ☞ Ak pôjde o spracúvanie osobných údajov, ktoré nespadá pod právo únie, použije sa zákon s výnimkou 3. časti a osobitné právne predpisy.
- ☞ Ak pôjde o spracúvanie osobných údajov príslušnými orgánmi na plnenie úloh na účely trestného konania, použijú sa len niektoré časti zákona.[2]

1.6 Vykonávacie predpisy a metodiky

Pri riešení ochrany osobných údajov je potrebné sa riadiť nielen naria-

2 Stanovisko ÚOOÚ. Kedy nariadenie a kedy zákon o ochrane osobných údajov. Zdroj: <https://dataprotection.gov.sk/uoou/sites/default/files/kedy_zakon_kedy_nariadeniepdff.pdf)>.