

www.
gdpr365.info

DonauMedia

PRAKTICKÝ MANUÁL GDPR PRE KAŽDÉHO

Všetko, čo potrebujete vedieť o novom nariadení
Európskeho parlamentu a Rady (EÚ) 2016/679
o ochrane osobných údajov v kompletu s webovou
stránkou, e-bookom a aktualizácnym servisom

ZADARMO k tejto príručke:

**ON-LINE
předpisy**

**365
servis**

ZÍSKAJTE e-book, aktualizácie, prístup
do uzavretej zóny webu:

Naskenujte QR a odošlite SMS na +420 603 282 990

Detaily na www.gdpr365.info



STORMWARE
POHODA
Ekonomický software

Pripravené
na **GDPR**



Volajte zadarmo:

0800 116 117

www.pohoda.sk



978081830525

INFORMÁCIE K BONUSOM

Neoddeliteľnou súčasťou tejto publikácie je aktualizčný servis, v ktorom priebežne nájdete ďalšie výklady jednotlivých ustanovení všeobecného nariadenia, príklady z praxe a podrobnosti o novej legislatíve. Aktualizačný servis zdarma získate podľa návodu na prvej strane. Ďalšie informácie na www.GDPR365.info.

POSTUP REGISTRÁCIE: 1. registrujte sa pomocou QR kódu na obálke **ALEBO** 2. odošlite SMS *ManualGDPR_18_SR_Aktualizacia* na číslo +420 603 282 990 **ALEBO** 3. odošlite e-mail s predmetom alebo textom *ManualGDPR_18_SR_Aktualizacia* na adresu newsletter@newsletter.cz **ALEBO** 4. vyplňte formulár na www.gdpr365.info

IMPRESSUM

Praktický manuál GDPR pre každého

ISBN 978-80-8183-052-5

DonauMedia, s. r. o., Bratislava, Slovenská republika © 2018. Všetky práva vyhradené.

Informácie: newsletter@newsletter.cz

Vyrobené v EÚ.

Texty Zvládnite základy GDPR za 30 minút, Malý slovník pojmov, Desatoro spracovania pre prevádzkovateľov boli publikované s láskavým súhlasom Úradu na ochranu osobných údajov ČR (www.uoou.cz, *titulky, medzititulky a odkazy do slovenskej legislatívy doplnila redakcia vydavateľstva*). Text Praktické otázky a odpovede k všeobecnému nariadeniu a zákonu č. 18/2018 Z. z. bol pripravený podľa zdrojov Úradu pre ochranu osobných údajov SR (dataprotection.gov.sk, *titulky a medzititulky doplnila redakcia vydavateľstva*). Text Desatoro pre živnostníkov a malé firmy pripravili JUDr. Ing. Jaroslav Švamberg a Bc. Jaromír Kuba zo spoločnosti Kuba a partneri s. r. o. (www.poverenec.info). Ďalšie pramene: webové stránky eur-lex.europa.eu, dataprotection.gov.sk, slov-lex.sk, publikácie Kühling J., Klar M., Sackmann F.: *Datenschutzrecht*, 4. vyd., C. F. Müller Verlag, Heidelberg 2018; Sydow G.: *Europäische Datenschutzgrundverordnung*, 2. vyd. Nomos, Baden-Baden 2018.

STORMWARE
POHODA
Ekonomický software

Účtovníctvo a GDPR
pod jednou strechou



www.pohoda.sk

Praktický manuál GDPR pre každého

3

PÄŤ MINÚT TEÓRIE NA ÚVOD	4
ZVLÁDNITE ZÁKLADY VŠEOBECNÉHO NARIADENIA GDPR ZA 30 MINÚT	10
MALÝ SLOVNÍK POJMOV	24
DESATORO SPRACOVANIA PRE PREVÁDZKOVATEĽOV	27
DESATORO PRE ŽIVNOSTNÍKOV A MALÉ FIRMY	28
PRAKTICKÉ OTÁZKY A ODPOVEDE K VŠEOBECNÉMU NARIADENIU A ZÁKONU Č. 18/2018 Z. z.	30
NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679	41
ZÁKON Č. 18/2018 Z. z. O OCHRANE OSOBNÝCH ÚDAJOV	124

PÄŤ MINÚT TEÓRIE NA ÚVOD

GDPR:

**PRIAMA PLATNOSŤ
VNÚTROŠTÁTNE ÚPRAVY
TRANSPARENTNOSŤ
PRÁVNA ODÔVODNENOSŤ**

Na rozdiel od predchádzajúcej smernice 95/46/EU, ktorú museli štáty EÚ presadiť do národných predpisov, platí **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 (všeobecné nariadenie o ochrane údajov)** vo všetkých členských štátoch od 25. mája 2018 priamo (je z kategórie všeobecných nariadení, v tuzemskom práve má váhu zákona publikovaného v Zbierke). Jednotlivé členské štáty musia iba pomocou vlastných právnych predpisov uviesť právo na ochranu osobných údajov podľa nového všeobecného nariadenia do súladu s právom na slobodu prejavu a informácie (pozrite článok 88 všeobecného nariadenia a upraviť niektoré ďalšie čiastkové otázky, lebo všeobecného nariadenia obsahuje otvorené ustanovenia, ktoré umožňujú jednotlivým

členským štátom určovať si niektoré aspekty ochrany osobných údajov na vnútroštátnej úrovni. Členským štátom však v zásade nie je dovolené oslabovať alebo sprísňovať predpísanú ochranu osobných údajov vlastnou domácou legislatívou. Otvorené ustanovenia bolo treba na Slovensku upraviť novým zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov bol zrušený.

Obsah a štruktúra

Všeobecné nariadenie (alebo ďalej taktiež iba *GDPR*) je súčasťou reformy ochrany osobných údajov v rámci celej EÚ. Vše-

Kuba a partneri s.r.o.

GDPR poradenství, školení,
služby pověřence (DPO)
www.gdpr-pardubice.cz

Právne upozornenie: Znenie textov v tejto publikácii bolo preverené so všetkou dostupnou starostlivosťou, vydavateľ ani predajca však nepreberajú žiadne záruky za eventuálne škody vzniknuté jej použitím a nezodpovedajú teda za to, ak by na základe textov zverejnených v tejto publikácii ktokoľvek konal alebo sa zdržal konania a v súvislosti s tým mu vznikla akákoľvek škoda materiálnej alebo nemateriálnej povahy. Autorské práva k tejto publikácii sú predmetom ochrany podľa zákonov ČR a SR a ich nositeľom je výhradne vydavateľ. Rozmnožovanie a šírenie celku alebo častí tejto publikácie akýmkoľvek spôsobom bez výslovného písomného dovolenia vydavateľa je zakázané.

becné nariadenie tvorí 99 článkov rozčlenených do jedenástich kapitol.

■ **Kapitola 1** (Články 1 až 4): Všeobecné ustanovenia (predmet úpravy a ciele, vecná a územná pôsobnosť, vymedzenie pojmov)

■ **Kapitola 2** (Články 5 až 11): Zásady (zásady spracúvania osobných údajov, zákonnosť spracúvania, podmienky vyjadrenia súhlasu, podmienky uplatniteľné na súhlas dieťaťa v súvislosti so službami informačnej spoločnosti, spracúvanie osobitných kategórií osobných údajov, spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, spracúvanie bez potreby identifikácie)

■ **Kapitola 3** (Články 12 až 23): Práva dotknutej osoby (transparentnosť informácií, oznámenia a postupy výkonu práv dotknutej osoby, informácie a prístup k osobným údajom, právo dotknutej osoby na prístup k údajom, právo na opravu, právo na vymazanie, právo na obmedzenie spracúvania, oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania, právo na prenosnosť údajov, právo namietat a automatizované individuálne rozhodovanie)

■ **Kapitola 4** (Články 24 až 43): Prevádzkovateľ a sprostredkovateľ (všeobecné povinnosti, zodpovednosť prevádzkovateľa, špecificky navrhnutá a štandardná ochrana údajov, spoloční prevádzkovatelia, zástupcovia prevádzkovateľov alebo sprostredkovateľov, ktorí nie sú usadení v Únii, sprostredkovateľ, spracúvanie na základe poverenia prevádzkovateľa alebo

sprostredkovateľa, záznamy o spracovateľských činnostiach, spolupráca s dozorným orgánom, bezpečnosť osobných údajov, bezpečnosť spracúvania, oznámenie porušenia ochrany osobných údajov dozornému orgánu, oznámenie porušenia ochrany osobných údajov dotknutej osobe, posúdenie vplyvu na ochranu údajov a predchádzajúca konzultácia, zodpovedná osoba a jej určenie, postavenie a úlohy, kódexy správania a certifikácia)

■ **Kapitola 5** (Články 44 až 50): Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám (všeobecná zásada prenosov, prenosy na základe rozhodnutia o primeranosti, prenosy vyžadujúce primerané záruky, záväzné vnútropodnikové pravidlá, prenosy alebo poskytovanie údajov, ktoré právo Únie nepovoľuje, výnimky pre osobitné situácie, medzinárodná spolupráca na účely ochrany osobných údajov)

■ **Kapitola 6** (Články 51 až 59): Nezávislé dozorné orgány (dozorný orgán, nezávislosť, všeobecné podmienky týkajúce sa členov dozorného orgánu, pravidlá zriadenia dozorného orgánu, príslušnosť, úlohy a právomoci)

■ **Kapitola 7** (Články 60 až 76): Spolupráca a konzistentnosť (spolupráca medzi vedúcim dozorným orgánom a inými dotknutými dozornými orgánmi, vzájomná pomoc, spoločné operácie dozorných orgánov, mechanizmus konzistentnosti, stanovisko výboru, riešenie sporov výborom, postup pre naliehavé prípady, výmena informácií, európsky výbor pre ochranu údajov a jeho

nezávislosť, úlohy, správy a postupy)

■ **Kapitola 8** (Články 77 až 84): Prostriedky nápravy, zodpovednosť a sankcie (právo podať sťažnosť dozornému orgánu, právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu a voči voči prevádzkovateľovi alebo sprostredkovateľovi, právo na náhradu škody a zodpovednosť, všeobecné podmienky ukladania správnych pokút, sankcie)

■ **Kapitola 9** (Články 85 až 91): Ustanovenia o osobitných situáciách spracúvania (spracúvanie a sloboda prejavu a právo na informácie, spracúvanie a prístup verejnosti k úradným dokumentom, spracúvanie národného identifikačného čísla, spracúvanie v súvislosti so zamestnaním, záruky a odchýlky týkajúce sa spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely, povinnosť zachovávať mlčanlivosť, existujúce pravidlá ochrany údajov cirkví a náboženských združení)

■ **Kapitola 10** (Články 92 až 93): Delegované akty a vykonávacie akty (vykonávanie delegovania právomocí)

■ **Kapitola 11** (Články 94 až 99): Záverečné ustanovenia (zrušenie smernice 95/46/ES, vzťah k smernici 2002/58/ES, vzťah k dohodám uzavretým v minulosti, nadobudnutie účinnosti a uplatňovanie)

99 článkom predchádza 173 bodov tzv. recitálov, ktoré predstavujú odôvodnenie, resp. výklad jednotlivých zásad.

Oblasti novej úpravy

Mnoho princípov ochrany osobných údajov prešlo z pôvodnej smernice do nového všeobecného nariadenia. Predovšetkým pojem osobné údaje v článku 4 bol v zásade zachovaný: *osobnými údajmi sú všetky informácie o identifikovanej alebo identifikovateľnej fyzickej osobe; identifikovateľnou fyzickou osobou je fyzická osoba, ktorú je možné priamo či nepriamo identifikovať, najmä odkazom na určitý identifikátor, napríklad meno, identifikačné číslo, lokalizačné údaje, sieťový identifikátor alebo na jeden či viac zvláštnych prvkov fyzickej, fyziologickej, genetickej, psychickej, ekonomickej, kultúrnej alebo spoločenskej identity tejto fyzickej osoby.* Ďalej platí rovnako ako doteraz, že spracovanie osobných údajov bez súhlasu dotknutej osoby je prípustné len na základe existencie zákonných dôvodov. Tie sú uvedené v článku 6:

- *spracovanie je potrebné z dôvodu naplnenia zmluvy alebo z dôvodu uskutočnenia predzmluvných opatrení;*
- *spracovanie je potrebné z dôvodu naplnenia právnych záväzkov;*
- *spracovanie je potrebné z dôvodu ochrany životne dôležitých záujmov subjektu údajov;*
- *spracovanie je potrebné z dôvodu splnenia úlohy, ktorá je vo verejnom záujme;*
- *spracovanie je potrebné z dôvodu ochrany oprávnených záujmov prevádzkovateľa alebo tretej osoby.*

Je však nutné zvážiť tieto záujmy oproti záujmom dotknutej osoby.

Princípy spracovania osobných údajov

Všeobecné nariadenie uvádza v článku 5 explicitne šesť princípov pre spracovanie osobných údajov:

- *zákonnosť, korektnosť a transparentnosť;*
- *účelovosť (spracovanie len na jasne dané, jednoznačné a legitímne účely);*
- *minimalizáciu (primeranosť, obmedzenosť na nutný rozsah vo vzťahu k účelu spracovania);*
- *presnosť;*
- *obmedzenosť (uloženie na čas nie dlhší, než je nutné na účely spracovania);*
- *integritu a dôvernú (spracovanie spôsobom, ktorý zaistí náležité zabezpečenie).*

Nerušená výmena osobných údajov v rámci EÚ

Výmenu osobných údajov v rámci EÚ nie je možné odmietnuť s argumentom, že sa v rôznych krajinách v rámci EÚ s ochranou údajov zaobchádza inak. Článok 1 odsek 3 všeobecného nariadenia stanovuje: „3. Voľný pohyb osobných údajov v rámci Únie sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov“.

Oblasť platnosti

Všeobecné nariadenie nerozlišuje medzi spracovaním osobných údajov verejnými inštitúciami a súkromnými firmami – pre všetkých sprostredkovateľov platia rovnaké práva a povinnosti. Napriek tomu určité druhy spracovania osobných údajov nespádajú podľa článku 2 všeobecného nariadenia pod túto úpravu. Recitály 16 a 18 to bližšie objasňujú:

(16) *Toto nariadenie sa nevzťahuje na otázky ochrany základných práv a slobôd ani na voľný tok osobných údajov týkajúcich sa činností, ktoré nepatria do pôsobnosti práva Únie, ako sú činnosti týkajúce sa národnej bezpečnosti. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov členskými štátmi pri vykonávaní činností v súvislosti so spoločnou zahraničnou a bezpečnostnou politikou Únie.*

(18) *Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v priebehu výlučne osobnej alebo domácej činnosti, a teda bez spojenia s profesijnou alebo komerčnou činnosťou. Osobné alebo domáce činnosti by mohli zahŕňať korešpondenciu a uchovávanie adresy či využívanie sociálnych sietí a online činnosti vykonávané v kontexte takýchto činností. Toto nariadenie sa však vzťahuje na prevádzkovateľov alebo sprostredkovateľov, ktorí poskytujú prostriedky na spracúvanie osobných údajov na takéto osobné alebo domáce činnosti.*

Princíp miestneho trhu

Európske právo na ochranu osobných údajov platí taktiež pre firmy so sídlom mimo EÚ, ak ponúkajú svoje výrobky alebo služby v rámci jednotného európskeho trhu. Princíp miestneho trhu je jedným z mnohých princípov, ktoré upravujú právne postavenie firiem ponúkajúcich výrobky a služby na spoločnom trhu. Miestny trh je miesto, na ktorom sa stretávajú záujmy predávajúcich a nakupujúcich a s ohľadom na konkurenciu je to taktiež miesto vý-

razného kríženia konkurenčných záujmov. Preto sa uplatňujú pravidlá konkrétneho trhu, na ktorý je ponuka zameraná. Vďaka tomu sa potom na cieľovom trhu vyrovnávajú rozdiely medzi podmienkami pre domáce a zahraničné firmy.

Požiadavka na súhlas

V princípe sú požiadavky na účinný súhlas so spracovaním osobných údajov definované tak, že písomná forma nie je nutná, je prípustný súhlas udelený technickým nastavením (napr. prehľadávača pri prezeraní webovej stránky), vyhlásením či rokováním, ale musí ísť o jasnú signalizáciu súhlasu v daných súvislostiach, čo musí byť sprostredkovateľ schopný preukázať. Mlčanie, dopredu začiarknuté políčka alebo nečinnosť nie je možné za súhlas považovať (pozrite recitál 32). Písomná forma je nutná pre súhlas so spracovaním osobitných osobných údajov.

Obmedzenia spracovávaných údajov

Všeobecné nariadenie spočíva na zásade minimalizácie spracovávaných údajov podmienených účelom. Na určitý účel (napríklad zaslanie objednaného tovaru a vystavenie faktúry) sa tak môže spracovávať napríklad meno, adresa, e-mailová adresa a telefón, ale na dosiahnutie tohto účelu už netreba žiadne iné údaje.

Transparentnosť

Recitál 39 vyzdvihuje princíp transparentnosti každého spracovania údajov pre dotknutú osobu. Na rôznych miestach vyža-

duje všeobecné nariadenie zodpovedajúce opatrenia:

- podľa článku 15 má každá osoba právo na informácie o všetkých údajoch, ktoré sa jej týkajú,
 - tieto informácie musia byť poskytnuté podľa článku 12 v precíznej, transparentnej, zrozumiteľnej, ľahko dostupnej a jednoducho pochopiteľnej podobe,
 - podľa článkov 13 a 14 musí každá dotknutá osoba dostať pri získavaní údajov úplné informácie, okrem iného o účele, príjemcovi a osobe zodpovednej za spracovanie údajov, čase uchovania údajov, práve na úpravu, zabezpečení uloženia a vymazaní a použití údajov na účely profilovania. Ak sa účel zmení, je nutné dotknutú osobu aktívne informovať,
 - podľa článku 16 má dotknutá osoba právo na opravu nesprávnych údajov, rovnako ako má podľa článku 18 právo na obmedzenie (blokovanie) spracovania údajov, ak je sporná správnosť alebo dôvod na spracovanie údajov.
- Efektivita týchto práv však závisí od nevysloveného predpokladu, že sa dotknutá osoba musí sama aktívne starať o to, kto a ako o nej spracováva údaje, a sama sa týchto práv dožadovať (hoci práve toto kritici všeobecného nariadenia nevnímajú ako príliš reálne). Okrem toho má všeobecné nariadenie podľa recitálu 13 ovplyvniť taktiež transparentnosť a právnu bezpečnosť pre najmenšie firmy, malé a stredné podniky (do 250 zamestnancov), ktorých potreby sú špecifické.

Právo byť zabudnutý

Právo byť zabudnutý, ktoré je priamo vyjadrené v nadpise článku 17, je jedno zo základných práv vyplývajúcich z všeobecného nariadenia. Zahŕňa na jednej strane právo dotknutej osoby požadovať vymazanie všetkých údajov, ktoré sa jej týkajú, ak pominú dôvody na uchovanie týchto údajov. Ďalej musí prevádzkovateľ sám aktívne mazať údaje, pre ktoré už neexistuje žiadny dôvod na ich uchovanie a spracovanie.

Právo na prenositeľnosť údajov

Rovnako ako predchádzajúca úprava, požaduje všeobecné nariadenie v článku 20, aby dotknutá osoba (subjekt údajov) mala právo získať údaje, ktoré sa jej týkajú, v štruktúrovanej, štandardnej, bežne používanej a strojovo čitateľnej podobe, a mohla tak poskytnúť tieto údaje bez obmedzenia inému prevádzkovateľovi bez toho, aby tomu pôvodný prevádzkovateľ bránil. Pri výkone práva na prenositeľnosť údajov má subjekt údajov právo na to, aby osobné údaje boli poskytnuté priamo jedným prevádzkovateľom prevádzkovateľovi druhému, ak je to technicky vykonateľné.

Sankcie

Z dôvodu efektívneho presadenia pravidiel na ochranu osobných údajov je po novom možné ukladať vyššie pokuty než doteraz. Okrem toho môžu miestne dozorné úrady do budúcnosti požadovať sankcie nielen od súkromných prevádzkovateľov

údajov, ale taktiež od verejných inštitúcií, ak to však umožňujú národné predpisy. Výška pokút za priestupky proti všeobecnému nariadeniu je stanovená podľa článku 83 až do dvadsiatich miliónov eur alebo do štyroch percent medzinárodného ročného obratu. Členské štáty okrem toho môžu stanoviť ďalšie možnosti sankcií. Napríklad podľa recitálu 149 je možné do pokuty zahrnúť (odobrať) aj zisky dosiahnuté v súvislosti s priestupkom. Vždy však platí zásada primeranosti sankcie. Náležite by sa teda mala zohľadniť povaha, závažnosť a čas trvania porušenia, úmyselný charakter porušenia, kroky, ktoré boli uskutočnené s cieľom zmierniť spôsobenú škodu, miera zodpovednosti alebo akékoľvek relevantné predchádzajúce porušenie, spôsob, akým sa dozorný úrad o danom porušení dozvedel, dodržiavanie opatrení, ktoré boli voči prevádzkovateľovi alebo sprostredkovateľovi nariadené, dodržiavanie kódexu správania alebo akýkoľvek iný pridaťujúci alebo poľahčujúci faktor. Je teda možné miesto peňazitej sankcie uložiť taktiež iba napomenutie. Uloženie sankcií vrátane správnych pokút by malo podliehať vhodným procesným zárukám v súlade so všeobecnými zásadami právnych predpisov Únie a Listiny základných práv a slobôd vrátane účinnej právnej ochrany a spravodlivého procesu.

Privacy by design, privacy by default

Recitál 78 zahŕňa pojmy *data protection by design* a *data protection by default* (bežnejšie používané ako *privacy by design*

a *privacy by default*). Tieto pojmy znamenajú, že technika (*dizajn*) spracovania údajov by mala byť navrhovaná a tak zameraná a nastavenie organizačných opatrení (*defaults*) by malo byť také, aby bolo učené zadost' potrebám ochrany osobných údajov a bolo zaistené splnenie požiadaviek vyplývajúcich z všeobecného nariadenia. Takto dokumentovaný postup môže pomôcť prevádzkovateľom a sprostredkovateľom pri dodržiavaní všeobecného nariadenia. Výklad týchto princípov môže byť pomerne široký. Zjednodušene povedané zahŕňa napríklad to, že počítače, počítačové siete, dátové úložiská, aplikácie a pod. by sa mali navrhovať a byť konštruované tak, aby umožňovali zabezpečenie a prístup k nim by mali mať iba oprávnené osoby.

Požiadavky na menovanie zodpovedných osôb

Všeobecné nariadenie predpokladá menovanie osôb poverených dohľadom nad ochranou osobných údajov (zodpovedných osôb) u jednotlivých prevádzkovateľov, minimálne u všetkých orgánov verejnej moci a verejných subjektov (s výnimkou súdov) a v tých súkromných spoločnostiach, v ktorých vznikajú riziká pri spracovaní osobných údajov. Článok 37 všeobecného nariadenia zavádza minimálny štandard pre zriadenie týchto pozícií. Malí podnikatelia a malé spoločnosti nemusia mať žiadnu zodpovednú osobu, ak ich hlavné činnosti nespočívajú v operáciách spracovania, ktoré kvôli svojej povahe, svojmu rozsahu alebo svojím účelom vyžadujú

rozsiahle pravidelné a systematické monitorovanie subjektov údajov alebo nespochívajú v rozsiahlom spracovaní osobitných kategórií údajov. Pojem rozsiahle spracovanie a predpoklady pre posúdenie vplyvu na ochranu údajov sú presnejšie popísané v recitáli 91. Niektoré profesie ako napríklad právnici, lekári alebo lekárnici (príslušníci zdravotníckych povolání) nemusia ustanoviť zodpovednú osobu (posúdenie vplyvu na ochranu osobných údajov u nich nie je povinné).

Ustanovenie o výnimkách (otvorené klauzuly)

Všeobecné nariadenie predpokladá, že vnútroštátne predpisy spresnia v mnohých oblastiach právo na ochranu osobných údajov detailnými úpravami. Všeobecné nariadenie obsahuje takých otvorených klauzúl niekoľko desiatok. Niektoré ustanovenia o výnimkách priamo vyžadujú právne úkony od členských štátov (prijatie špeciálnej právnej úpravy), niektoré len dávajú na vnútroštátnu úpravu priestor. Ten je však v zásade obmedzený tak, aby nebola znížená hranica ochrany osobných údajov s hranicami danými všeobecným nariadením. Príkladom otvorenej klauzuly môže byť ochrana údajov zamestnancov: článok 88 odsek 1 umožňuje, aby si členské štáty stanovili špecifické predpisy pre zaistenie práv a slobôd pri spracovaní osobných údajov zamestnancov v súvislosti so zamestnaním. Formulácia tohto pravidla síce neumožňuje sprísnenia ani úľavy v ochrane osobných údajov, ale predpokladá konkrétne úpravy v národných predpi-

soch. Ďalšie ustanovenia o výnimkách môžeme nájsť:

- v článku 9 odsekoch 2 a 4 pre stanovenie zvláštnych podmienok pre spracovanie osobitných druhov osobných údajov, ako sú zdravotné záznamy alebo údaje o sexuálnej orientácii;
- v článku 10 pre povolenie na spracovanie údajov o rozsudkoch v trestných veci-

ach a trestných činoch;

- v článku 28 o právnych základoch spracovania údajov sprostredkovateľom pre prevádzkovateľa na zmluvnom základe;
- v článku 37 o požiadavkách na zodpovedné osoby (rozdielných od podmienok stanovených v tomto článku);
- v článku 85 pre vyrovnanie rozdielov medzi ochranou údajov a slobodou preja-

vu alebo pre pravidlá slobody tlače;

- v článku 87 pre pravidlá spracovania národných identifikačných čísel alebo údajov všeobecného významu;
- v článku 89 pre pravidlá výnimiek v prácach dotknutých osôb pri spracovaní údajov na vedecké, historické, štatistické alebo archívne potreby.

9

STORMWARE
POHODA
Ekonomický software

Účtovníctvo a GDPR
pod jednou strechou



www.pohoda.sk

ZVLÁDNITE ZÁKLADY VŠEOBECNÉHO NARIADENIA GDPR ZA 30 MINÚT

To, čo sa všeobecne rozumie pod skratkou GDPR, je v presnej terminológii 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 (všeobecné nariadenie o ochrane údajov). Ide o doteraz najobsiahlejší jednotný legislatívny rámec, ktorý bol prijatý s cieľom zaistiť základné práva občanov EÚ na ochranu v súvislosti so spracovaním osobných údajov. Zákon č. 122/2013 Z. z. bol zrušený a nahradený zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorý podrobne rekapituluje základné pojmy a pravidlá ochrany osobných údajov a upravuje činnosť Úradu na ochranu osobných údajov SR (napr. jeho ustanovenia, organizáciu, pôsobnosť, kontroly a pod.) a niektoré čiastkové záležitosti nutné na dotvorenie celého rámca ochrany osobných údajov, ktoré všeobecné nariadenie o ochrane údajov neupravuje alebo ich umožňuje upraviť na vnútroštátnej úrovni (v niektorých otázkach dokonca všeobecné nariadenie vnútroštátnu úpravu predpokladá: zvláštne situácie pri spracovaní osobných údajov na účely výkonu slobody prejavu, právo na informácie, novinárska činnosť, sloboda vedeckého bádania, literárna tvorba, umelecký prejav, verejný záujem, ochrana zdroja informácií). Nový zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov taktiež vymenuje konkrétne správne delikty a možné sankcie za ne. Výška prípadných pokút je vždy špecifikovaná ako „do sumy“ a pre jednotlivé správne delikty je v zákone stanovená do 2 000 eur až do 10 000 000 eur (2 % obratu), v prípadoch obzvlášť závažných až do 20 000 000 eur (4 % obratu). Všeobecné nariadenie je univerzálne použiteľné vo všetkých štátoch Európskeho hospodárskeho priestoru, teda v štátoch Európskej únie, na Islande, v Nórsku a Lichtenštajnsku).

■ Kapitola 1.

Všeobecné nariadenie o ochrane údajov

Revízia právneho rámca ochrany osobných údajov

K revízii sa prišlo z toho dôvodu, že právny rámec založený smernicou 95/46/ES už prestal zodpovedať súčasnosti, najmä pokiaľ ide o prostriedky, ktoré sa na spracovanie využívajú, a tiež aj pokiaľ ide o spracovanie ako také, ktoré je oveľa komplexnejšie, než bolo pred niekoľkými desiatkami rokov (napr. v oblasti profilo-

vania, automatizácie spracovania osobných údajov atď.). Zároveň v jednotlivých krajinách EÚ nebola smernicou 95/46/ES dosiahnutá požadovaná miera zjednotenia právnej úpravy, čo prevádzkovateľom pôsobiacim vo viacerých krajinách robilo problémy. Cieľom všeobecného nariadenia je prispôbiť právny rámec ochrany osobných údajov dnešnej dobe, dosiahnuť väčšiu jednotu právneho rámca vo všetkých krajinách, na ktoré dopadá, posilniť práva subjektu údajov a v neposlednom rade

je snahou dosiahnuť zjednotený výklad všeobecného nariadenia a dozor jednotlivými dozornými úradmi.

Kto sa bude musieť všeobecným nariadením riadiť

Všeobecným nariadením sa bude predovšetkým, pokiaľ ide o povinnosti, riadiť subjekt, ktorý spracováva osobné údaje. Taký subjekt sa nazýva prevádzkovateľom osobných údajov. Všeobecným nariadením sa riadi aj sprostredkovateľ, čo je subjekt, ktorý pre prevádzkovateľa osobné údaje

spracováva. Pokiaľ ide o práva vyplývajúce z všeobecného nariadenia, tie plnú fyzickej osobe, čo je subjekt údajov. Ďalej sa všeobecným nariadením budú riadiť aj dozorné úrady, t. j. aj Úrad na ochranu osobných údajov SR, ktorý bude uplatňovať zverené právomoci s cieľom plniť stanovené úlohy.

Na aké činnosti GDPR nedopadá

Z pôsobnosti všeobecného nariadenia sú vylúčené činnosti fyzickej osoby [pozrite článok 2 ods. 2 písm. c) všeobecného nariadenia], pri ktorých sa spracovávajú osobné údaje výlučne na osobnú či domácu činnosť. Ďalej je z pôsobnosti všeobecného nariadenia o ochrane údajov vylúčené spracovanie vykonávané príslušnými orgánmi na účel prevencie, vyšetrovania, odhaľovania či stíhania trestných činov alebo výkonu trestov vrátane ochrany pred hrozbami pre verejnú bezpečnosť a ich predchádzanie. To je predmetom úpravy smernice Európskeho parlamentu a Rady (EÚ) 2016/680. Keďže ide o smernicu, bolo nutné jej vykonanie (premietnutie do tuzemskej legislatívy), ktoré bolo vykonané čl. II – XV nového zákona o ochrane osobných údajov.

■ Kapitola 2. Nové prístupy a povinnosti

Nové prístupy, na ktorých je GDPR založené

Je možné hovoriť o dvoch nových prístupoch, na ktorých je všeobecné nariadenie

založené. Novými prístupmi sú princíp zodpovednosti prevádzkovateľa a prístup založený na riziku. Princíp zodpovednosti znamená zodpovednosť prevádzkovateľa za dodržanie zásad spracovania, ktoré sú uvedené v článku 5 ods. 1 všeobecného nariadenia, a zároveň musí prevádzkovateľ byť schopný tento súlad doložiť. Na dokladanie súladu budú okrem iného slúžiť kódexy, osvedčenia či certifikácie, prípadne záznamy o činnostiach spracovania (pozrite ďalej). Prístup založený na riziku v širšom slova zmysle znamená, že prevádzkovateľ už od počiatku koncipovania spracovania osobných údajov musí brať do úvahy povahu, rozsah, kontext a účel spracovania a prihliadnuť na pravdepodobné riziká pre práva a slobody fyzických osôb a tomu musí prispôbiť aj zabezpečenie osobných údajov. V užšom slova zmysle môžeme hovoriť o prístupe založenom na riziku ako o aplikácii niektorých povinností iba v prípade, keď spracovanie osobných údajov či porušenie zabezpečenia (bezpečnostný incident) predstavuje riziko či vysoké riziko pre práva a slobody fyzickej osoby. V tomto rozsahu sa princíp založený na riziku uplatňuje najmä v prípade nových povinností: ohlasovanie, resp. oznamovanie prípadu porušenia zabezpečenia osobných údajov Úradu na ochranu osobných údajov SR, resp. subjektu údajov, posudzovanie vplyvu spracovania na ochranu osobných údajov a povinné konzultácie s Úradom na ochranu osobných údajov SR, ktorých aplikácia je viazaná na prítomnosť rizika či vysokého rizika pre

práva a slobody fyzických osôb.

Ako prevádzkovateľ dokladá súlad spracovania

Splniť stanovenú zodpovednosť prevádzkovateľa za súlad spracovania so zásadami spracovania a schopnosť tento súlad preukázať, majú prevádzkovateľovi, ako výslovne zmieňuje všeobecné nariadenie, napomáhať okrem iného aj kódexy, osvedčenia (pečate, známky) a záznamy o činnostiach spracovania. Kódexy majú prevádzkovateľom, najmä na sektorovej úrovni, slúžiť ako vodidlo správnej praxe pri spracovaní osobných údajov práve s ohľadom na špecifickosť daného sektora (napr. bankovníctvo, telekomunikácie, internetové obchody, zdravotníctvo). Osvedčenie má slúžiť na preukázanie súladu spracovania so všeobecným nariadením. Záznamy o činnostiach spracovania obsahujú informácie o vykonávanom spracovaní, čo prevádzkovateľovi umožní ľahšiu orientáciu vo veci spracovania, ktoré vykonáva. Táto povinnosť je stanovená v článku 30 všeobecného nariadenia, pričom niektorí prevádzkovatelia sú vyňatí z nutnosti viesť záznamy o činnostiach spracovania. Dokladanie súladu spracovania však nie je možné obmedziť iba na hore uvedené možnosti, ale dokladanie súladu je komplexná činnosť zahŕňajúca čiastkové činnosti, medzi ktoré je možné zaradiť nielen hore uvedené kódexy, osvedčenia a záznamy o činnostiach spracovania, ale napríklad aj zverejňovanie informácií, ktoré všeobecné nariadenie ukladá prevádzkovateľovi zverejňovať, vyhotovením vnútorných predpisov až po

riadnu spoluprácu s príslušným dozorným úradom.

Kódexy a osvedčenia

Kódexy budú môcť vydávať združenia či iné subjekty zastupujúce rôzne kategórie prevádzkovateľov alebo sprostredkovateľov, pričom návrh kódexu musí byť predložený Úradu na ochranu osobných údajov SR, ktorý vydá stanovisko, či je daný kódex či návrh na jeho zmenu v súlade so všeobecným nariadením, a ak zistí, že áno, schváli ho. Schváleným kódexom sa potom môžu riadiť prevádzkovatelia v danom sektore. Osvedčenie o súlade spracovania bude môcť vydávať na to akreditovaný subjekt.

Nové povinnosti vyplývajúce z GDPR

Základné zásady, princípy a kľúčové instrumenty zostali de facto nemenné, resp. boli iba detailnejšie rozpracované a spresnené (napr. nutnosť disponovať právnym dôvodom na spracovanie, zabezpečenie osobných údajov, transparentnosť voči subjektu údajov atď.). Všeobecné nariadenie na týchto základoch prinieslo nadstavbu spochybňujúcu v dodatočných nových povinnostiach, ktoré sú pre slovenských prevádzkovateľov nové.

Ide najmä o tieto nové povinnosti:

- povinnosť viesť záznamy o činnostiach spracovania,
- posúdenie vplyvu na ochranu osobných údajov,
- predchádzajúca konzultácia,
- ohlasovanie prípadu porušenia zabezpe-

čenia osobných údajov Úradu na ochranu osobných údajov,

- oznamovanie prípadu porušenia zabezpečenia osobných údajov subjektu údajov,
- ustanovenie zodpovednej osoby na ochranu osobných údajov.

Okrem povinnosti viesť záznamy o činnostiach spracovania a ustanoviť zodpovednú osobu sú ostatné nové povinnosti založené na prístupe založenom na riziku, t. j. ich uplatnenie je viazané na prítomnosť rizika či vysokého rizika pre práva a slobody subjektu údajov. Hoci sa však pri povinnosti ustanoviť zodpovednú osobu priamo nepracuje s pojmami riziko či vysoké riziko, odráža sa v tejto povinnosti do určitej miery tiež prístup založený na riziku, keďže pre určité spracovanie, resp. určité subjekty, je povinnosťou ustanoviť zodpovednú osobu na ochranu osobných údajov.

Kedy musí prevádzkovateľ posúdiť vplyv na ochranu osobných údajov

Posúdiť vplyv na ochranu osobných údajov musí prevádzkovateľ, ak je pravdepodobné, že určitý druh spracovania, najmä pri využití nových technológií, s prihliadnutím na povahu, rozsah, kontext a účely spracovania bude predstavovať vysoké riziko pre práva a slobody fyzických osôb. Posúdenie musí prebehnúť pred začatím predmetného spracovania. Ak bola ustanovená zodpovedná osoba na ochranu osobných údajov, vyžiada si prevádzkovateľ jej posudok.

Posúdenie vplyvu na ochranu osobných

údajov sa vyžaduje predovšetkým v prípade:

- systematického a rozsiahleho vyhodnocovania osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracovaní vrátane profilovania a na ktorom sa zakladajú rozhodnutia, ktoré vyvolávajú vo vzťahu k fyzickým osobám právne účinky,
- rozsiahleho spracovania osobitných kategórií údajov alebo rozsudkov v trestných veciach,
- rozsiahleho systematického monitorovania verejne prístupných priestorov.

Kedy musí prevádzkovateľ konzultovať spracovanie

osobných údajov s Úradom na ochranu osobných údajov
Prevádzkovateľ je povinný konzultovať spracovanie osobných údajov s Úradom na ochranu osobných údajov SR, ak z posúdenia vplyvu na ochranu osobných údajov vyplynie, že by dané spracovanie malo za následok vysoké riziko v prípade, že by prevádzkovateľ neprijal opatrenia na zmierenie tohto rizika. Cieľom predchádzajúcej konzultácie je tak korigovať hroziace vysoké riziko.

Záznamy o činnostiach

Záznamy o činnostiach spracovania predstavujú do istej miery náhradu za oznamovaciu povinnosť, ktorá bola všeobecným nariadením zrušená. Prevádzkovateľ a sprostredkovateľ, ak sa na nich nevzťahuje výnimka z povinnosti viesť záznamy o činnostiach spracovania, sú povinní viesť záznamy s určitými informáciami. Tieto

záznamy následne umožnia prevádzkovateľovi preukázať súlad spracovania osobných údajov so všeobecným nariadením.

Kto nemusí viesť záznamy o činnostiach spracovania

Viesť záznamy o činnostiach spracovania nedolieha na podnik alebo organizáciu zamestnávajúcu menej než 250 osôb, iba ak spracovanie, ktoré vykonáva, pravdepodobne predstavuje riziko pre práva a slobody subjektov údajov, spracovanie nie je príležitostné alebo zahŕňa spracovanie osobitných kategórií údajov alebo osobných údajov týkajúcich sa rozsudkov v trestných veciach.

■ Kapitola 3.

Zásady a právne dôvody spracovania

Zásady, na ktorých je postavené všeobecné nariadenie

Zásady je možné v stručnosti zhrnúť takto:

- zákonnosť, korektnosť, transparentnosť
- prevádzkovateľ musí spracovávať osobné údaje na základe najmenej jedného právneho dôvodu a voči subjektu údajov transparentne,
- obmedzenie účelu – osobné údaje sa musia zhromažďovať na určité a legitímne účely a nesmú sa spracovávať nezlučiteľným spôsobom s týmito účelmi,
- minimalizácia údajov – osobné údaje musia byť primerané a relevantné vo vzťahu k účelu, na ktorý sa spracovávajú,
- presnosť – osobné údaje musia byť presné,

- obmedzenie uloženia – osobné údaje by mali byť uložené vo forme umožňujúcej identifikáciu subjektu údajov len po nutný čas na dané účely, na ktoré sa spracovávajú,
- integrita a dôvernosť – technické a organizačné zabezpečenie osobných údajov. Jednotlivé zásady sú rozvinuté v článku 5 ods. 1 všeobecného nariadenia. Vymedzenie, resp. dodržiavanie týchto zásad, je pre prevádzkovateľa zásadné, nielen z toho dôvodu, že to sú de facto zároveň povinnosti, ale aj preto, že v článku 5 ods. 2 všeobecného nariadenia je stanovená zodpovednosť prevádzkovateľa za ich dodržiavanie a zároveň povinnosť prevádzkovateľa byť schopný dodržiavanie týchto zásad (povinností) doložiť. Ide o vyjadrenie tzv. princípu zodpovednosti prevádzkovateľa. Na preukazovanie súladu s týmito zásadami slúžia záznamy o činnostiach spracovania a tiež kódexy a osvedčenia.

Právne dôvody spracovania osobných údajov

Právne dôvody spracovania osobných údajov znamenajú oprávnenie prevádzkovateľa osobné údaje spracovávať. Právne dôvody sú tak nutným predpokladom, aby sa vôbec mohlo hovoriť zo strany prevádzkovateľa o legálnom spracovaní, keďže ak by prevádzkovateľ nedisponoval riadnym právnym dôvodom na spracovanie osobných údajov, bolo by ďalej nerozhodné, či plní ostatné povinnosti, keďže by osobné údaje spracovával nezákonne a musel by osobné údaje zlikvidovať. Je dôležité vedieť, že aj osobné údaje môže pre-

vádzkovateľ spracovávať na rôzne účely, pričom na každý účel potrebuje právny dôvod spracovania osobných údajov. Spracovanie osobných údajov sa vždy viaže na účel, na základe ktorého sa určí právny dôvod spracovania. Nie je vylúčené, že „jeden“ osobné údaje (alebo ich určitý súhrn) bude prevádzkovateľ spracovávať na rôzne účely, pričom tieto účely môžu v čase vznikáť či zanikať bez toho, aby to predstavovalo povinnosť osobné údaje likvidovať. Povinnosť likvidácie osobných údajov nastane v prípade, keď prevádzkovateľ stratí posledný právny dôvod na spracovanie osobných údajov. Osobné údaje je možné spracovávať, ak je prítomný aspoň jeden z týchto právnych dôvodov:

- subjekt údajov udelil súhlas pre jeden či viac konkrétnych účelov,
- spracovanie je nutné z dôvodu splnenia zmluvy, ktorej zmluvnou stranou je subjekt údajov, alebo na vykonanie opatrení prijatých pred uzavretím zmluvy na žiadosť tohto subjektu údajov,
- spracovanie je nutné z dôvodu splnenia právnej povinnosti, ktorá sa na prevádzkovateľa vzťahuje,
- spracovanie je nutné z dôvodu ochrany životne dôležitých záujmov subjektu údajov alebo inej fyzickej osoby,
- spracovanie je nutné z dôvodu splnenia úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci, ktorým je poverený prevádzkovateľ,
- spracovanie je nutné na účely oprávnených záujmov príslušného prevádzkova-

teľa či tretej strany, okrem prípadov, keď pred týmito záujmami majú prednosť záujmy alebo základné práva a slobody subjektu údajov vyžadujúce ochranu osobných údajov.

Súhlas so spracovaním osobných údajov

Súhlas (pozrite článok 4 ods. 1 bod 11 všeobecného nariadenia) je slobodný, konkrétny, informovaný a jednoznačný prejav vôle, ktorým subjekt údajov dáva vyhlásením či iným zjavným potvrdením svoj súhlas na spracovanie svojich osobných údajov. Ide o aktívny a dobrovoľný prejav vôle subjektu údajov, do ktorého nesmie byť nútený. Súhlas je jedným z právnych dôvodov, na základe ktorého môže prevádzkovateľ osobné údaje spracovávať. Súhlas sa vždy poskytuje na určitý účel spracovania, ktorý musí subjekt údajov poznať. Nie vždy odvolanie súhlasu znamená povinnosť prevádzkovateľa osobné údaje zlikvidovať, keďže odvolanie súhlasu sa deje na určitý účel, na ktorý sa osobné údaje spracovávajú, pričom prevádzkovateľ môže osobné údaje spracovávať na iné účely, na ktoré využije iný právny dôvod spracovania než súhlas subjektu údajov.

Podmienky udelenia súhlasu so spracovaním osobných údajov

Aby bolo možné dosiahnuť slobodu, konkrétnosť, informovanosť a jednoznačnosť prejavu vôle subjektu údajov, stanovuje všeobecné nariadenie v článku 7 podmienky vyjadrenia súhlasu. Zásadná je tzv. odlišiteľnosť súhlasu, čo znamená, že sú-

hlas musí byť odlišený od iných skutočností, ku ktorým sa subjekt údajov vyjadruje. Pre názornosť, súhlas tak musí byť oddelený napr. od zmluvy či obchodných podmienok, resp. už nie je možné, aby bol ich neoddeliteľnou súčasťou. Zároveň nesmie byť uzavretie zmluvy (napr. na službu) podmienené poskytnutím súhlasu so spracovaním osobných údajov. Je však samozrejmé, že v závislosti od služby či výrobku bude prevádzkovateľ musieť spracovávať (bez súhlasu) určité množstvo osobných údajov subjektu údajov práve na účely plnenia zmluvy či plnenia zákonom stanovenej povinnosti.

Je súhlas odvolateľný?

Subjekt údajov má právo svoj súhlas kedykoľvek odvolať. Odvolaním nie je dotknutá zákonnosť spracovania vychádzajúceho zo súhlasu, ktorý bol daný pred jeho odvolaním. Je nutné si uvedomiť, že súhlas bol dávaný na určité účely a odvolanie súhlasu nemusí vždy predstavovať pre prevádzkovateľa povinnosť osobné údaje zlikvidovať, ale bude predstavovať pre prevádzkovateľa iba povinnosť prestať osobné údaje spracovávať na určitý účel, na ktorý bol súhlas udelený. Takisto aj v prípade, keď prevádzkovateľ použil súhlas pre prípady, keď mu náleží iný právny dôvod spracovania osobných údajov, neznamená odvolanie súhlasu (teda úkonu, ktorý nebol nutný na spracovanie) povinnosť osobné údaje zlikvidovať či ich prestať spracovávať, napr. ak osobné údaje musia byť na zákonom stanovené účely.

Ako to bude so skoršími súhlasmi počas použiteľnosti všeobecného nariadenia?

Všeobecné nariadenie v recitáli 171 predpokladá prechod súhlasu, avšak s podmienkou, že súhlas bol udelený spôsobom a v súlade s podmienkami všeobecného nariadenia. To bude pre veľa prevádzkovateľov problematické, keďže nimi získavaný súhlas nebude spĺňať podmienky stanovené v článku 7 všeobecného nariadenia, napríklad podmienku odlišiteľnosti súhlasu (súhlas nesmie byť neoddeliteľnou súčasťou obchodných podmienok) či podmienku nepodmieňovať poskytnutie služby vyžadovaním udelenia súhlasu so spracovaním osobných údajov.

Spracovanie osobných údajov zverejnených na internete

Osobné údaje patria subjektom údajov a tie musia v niektorých prípadoch, najmä v zákonom stanovených prípadoch, strpieť ich zverejnenie napr. vo verejnom registri. Osobné údaje vo verejnom registri sú zverejnené na základe zákona, keďže tak zákon stanovuje (typicky napr. živnostenský register). Skutočnosť, že je stanovená verejný register, neznamená, že zverejnené osobné údaje je možné ďalej neobmedzene preberať a spracovávať, napr. ich ďalším zverejňovaním, a tým na nich profitovať. Je nutné si uvedomiť, že aj ďalšie zverejňovanie údajov z verejných registrov je spracovaním osobných údajov a na to musí prevádzkovateľovi náležať právny dôvod, t. j. všeobecným nariadením predpokladané oprávnenie. Ďalšie zverejňovanie z verejných registrov prevza-

tých osobných údajov za použiteľnosti všeobecného nariadenia je problematické, keďže prevádzkovateľ bude musieť využiť niektorý z právnych dôvodov v článku 5 ods. 1 všeobecného nariadenia. Obdobne je to v prípade osobných údajov, ktoré subjekty údajov dobrovoľne zverejňujú na internete s určitým cieľom. Ani tieto údaje, hoci dobrovoľne zverejnené, nie je možné bez ďalšieho spracovávať, keďže aj v tomto prípade by mal prevádzkovateľ absenciu právneho dôvodu. Verejnosť údajov nikdy a priori neznamená možnosť ich ďalšieho bezmedzného spracovávanía.

■ Kapitola 4.

Osobitné kategórie osobných údajov (citlivé údaje)

Prečo sa rozlišujú osobitné kategórie osobných údajov

Niektoré osobné údaje sú takého charakteru, že môžu subjekt údajov samy o sebe poškodiť v spoločnosti, v zamestnaní, v škole či môžu zapríčiniť jeho diskrimináciu. Z tohto dôvodu je taxatívne (úplným vymenovaním) vymedzená skupina údajov, ktoré sa považujú voči subjektu údajov za citlivé a ktorým je poskytnutá zvýšená ochrana pri ich spracovaní. Zvýšená ochrana sa prejavuje najmä v stanovených zvláštnych právnych dôvodoch, na základe ktorých ich možno spracovávať, viazanosti niektorých inštitútov na ich spracovanie ako hlavné činnosti (napr. posúdenie vplyvu, ustanovenie zodpovednej osoby), dôraze na ich zvýšené zabezpečenie.

Aké údaje spadajú do osobitnej kategórie osobných údajov

Osobitné kategórie osobných údajov sú také osobné údaje, ktoré vypovedajú o rasovom či etnickom pôvode, politických názoroch, náboženskom vyznaní či filozofickým presvedčení, členstve v odboroch, zdravotnom stave či o sexuálnom živote alebo sexuálnej orientácii fyzickej osoby. Za osobitnú kategóriu údajov sa považujú aj genetické a biometrické údaje, ktoré sú spracovávané na účel jedinečnej identifikácie fyzickej osoby. Podmienky pre spracovanie osobných údajov týkajúcich sa rozsudkov v trestných veciach a trestných činov majú zvláštny režim podľa článku 10 všeobecného nariadenia.

Je možné osobitné kategórie osobných údajov spracovávať?

Osobitné kategórie osobných údajov je možné spracovávať, iba ak:

- subjekt údajov udelil výslovný súhlas,
- spracovanie je nutné na plnenie povinností v oblasti pracovného práva, práva sociálneho zabezpečenia a sociálnej ochrany,
- spracovanie je nutné z dôvodu ochrany životne dôležitých záujmov subjektu údajov alebo inej fyzickej osoby v prípade, že subjekt údajov nie je fyzicky alebo právne spôsobilý udeliť súhlas,
- spracovanie vykonáva v rámci svojich oprávnených činností nadácia, združenie či iný neziskový subjekt, ktorý sleduje politické, filozofické, náboženské alebo odborové ciele, za podmienky, že sa spracovanie vzťahuje iba na súčasných alebo bývalých členov alebo na osoby, ktoré

s týmto subjektom udržiavajú pravidelné styky súvisiace s jeho cieľmi, a že tieto osobné údaje nie sú bez súhlasu subjektu údajov sprístupňované mimo tohto subjektu,

- spracovanie sa týka osobných údajov zjavne zverejnených subjektom údajov,
- spracovanie je nutné z dôvodu určenia, výkonu alebo obhajoby právnych nárokov alebo pri konaní súdov,
- spracovanie je nutné z dôvodu významného verejného záujmu,
- spracovanie je nutné na účely preventívneho alebo pracovného lekárstva, na posúdenie pracovných schopností zamestnancov, lekárskej diagnostiky, poskytovania zdravotnej alebo sociálnej starostlivosti atď.,

- spracovanie je nutné z dôvodu verejného záujmu v oblasti verejného zdravia, ako je ochrana pred vážnymi cezhraničnými zdravotnými hrozbami alebo zaistenie bezpečnosti zdravotnej starostlivosti, liečivých prípravkov alebo zdravotníckych prostriedkov,
- spracovanie je nutné na účely archivácie vo verejnom záujme, na účely vedeckého či historického výskumu alebo na štatistické účely.

Veľmi často bude splnomocnenie na spracovanie osobitnej kategórie osobných údajov obsiahnuté v príslušnom právnom predpise, ktorým sa prevádzkovateľ musí riadiť alebo bude vyplývať z oprávnenej činnosti prevádzkovateľa.

■ Kapitola 5.

Práva subjektu údajov (dotknutej osoby)

Práva subjektu údajov sú dôležitým prvkom ochrany osobných údajov ako celku, keďže subjekt údajov je často v slabšom postavení než prevádzkovateľ a teda vyrovňávajú vzťah medzi ním a prevádzkovateľom. Subjekt údajov má právo na to byť informovaný o spracovaní jeho osobných údajov. Tým sa rozumie právo na určité informácie o spracovaní jeho osobných údajov. Ide najmä o informácie o účele spracovania, totožnosti prevádzkovateľa, o jeho oprávnených záujmoch, o príjemcoch osobných údajov. V tomto prípade ide o pasívne právo, keďže aktivitu musí voči subjektu údajov vyvinúť prevádzkovateľ, aby požadované informácie stanovené vo všeobecnom nariadení subjektu údajov poskytol, resp. sprístupnil. Úplný výpočet informácií, ktoré prevádzkovateľ poskytuje pri zhromažďovaní osobných údajov, je možné nájsť v článkoch 13 a 14 všeobecného nariadenia. Všeobecné nariadenie formálne rozlišuje poskytovanie informácií v prípade, že osobné údaje sú získané od subjektu údajov, resp. nie sú získané od subjektu údajov. Medzi ďalšie práva subjektu údajov, ktoré sú často založené na aktivite subjektu údajov, patrí právo na prístup k osobným údajom, právo na opravu (resp. na doplnenie), právo na výmaz, právo na obmedzenie spracovania, právo na prenositeľnosť údajov, právo vzniesť námietku a právo nebyť predmetom automatizovaného individuálneho

rozhodovania vrátane profilovania.

Prístup k osobným údajom

Prístupom k osobným údajom sa rozumie právo subjektu údajov získať od prevádzkovateľa informáciu (potvrdenie), či sa jeho osobné údaje spracovávajú, alebo nespracovávajú, a ak sa spracovávajú, má subjekt údajov právo tieto osobné údaje získať a zároveň má právo získať nasledujúce informácie:

- účely spracovania,
- kategórie dotknutých osobných údajov,
- príjemcovia alebo kategórie príjemcov, ktorým osobné údaje boli alebo budú sprístupnené,
- plánované obdobie, počas ktorého budú osobné údaje uložené,
- existencia práva požadovať od prevádzkovateľa opravu alebo výmaz osobných údajov, právo vzniesť námietku,
- právo podať sťažnosť na dozornom úrade,
- všetky dostupné informácie o zdroji osobných údajov, ak nie sú získané od subjektu údajov,
- skutočnosť, že dochádza k automatizovanému rozhodovaniu vrátane profilovania.

Ak prevádzkovateľ o fyzickej osobe žiadne údaje nespracováva, poskytuje sa informácia, že osobné údaje pýtajúceho sa nie sú predmetom spracovania osobných údajov zo strany prevádzkovateľa.

Nepresné údaje

Subjekt údajov má právo na opravu ne-

presných osobných údajov, ktoré sa ho týkajú. Neznamená to povinnosť prevádzkovateľa aktívne vyhľadávať nepresné údaje (avšak nič mu v tom ani nebráni) ani to neznamená povinnosť prevádzkovateľa napr. každoročne požadovať od subjektu údajov aktualizáciu jeho údajov. Ak sa subjekt údajov domnieva, že prevádzkovateľ spracováva jeho nepresné údaje, upozorní ho na to. Je povinnosťou prevádzkovateľa, ak mu subjekt údajov oznámi, že požaduje opravu jeho osobných údajov, zaoberať sa jeho žiadosťou.

Právo byť zabudnutý

Právo na výmaz (byť zabudnutý) predstavuje v GDPR inými slovami vyjadrenú povinnosť prevádzkovateľa zlikvidovať osobné údaje, ak je splnená aspoň jedna podmienka:

- osobné údaje už nie sú potrebné na účely, na ktoré boli zhromaždené alebo inak spracované,
- subjekt údajov odvolá súhlas a neexistuje žiadny ďalší právny dôvod na spracovanie,
- subjekt údajov vznesie námietku proti spracovaniu a neexistujú žiadne prevažujúce oprávnené dôvody na spracovanie,
- osobné údaje boli spracované protiprávne,
- osobné údaje je nutné vymazať kvôli splneniu právnej povinnosti,
- osobné údaje boli zhromaždené v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 všeobecného nariadenia.

Právo na prenositeľnosť údajov

Právo na prenositeľnosť je úplne nové právo subjektu údajov, ktorého podstatou je možnosť za určitých podmienok získať osobné údaje, ktoré sa ho týkajú a ktoré prevádzkovateľovi poskytol, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, a právo poskytnúť tieto údaje inému prevádzkovateľovi bez toho, aby tomu pôvodný prevádzkovateľ bránil. Zároveň má subjekt údajov, ak požiada, aj právo na to, aby prevádzkovateľ poskytol jeho osobné údaje v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte inému prevádzkovateľovi, ak je to technicky vykonateľné. Spoločné podmienky pre aplikáciu práva na prenositeľnosť sú tieto:

- musí ísť o spracovanie založené na právnom dôvode súhlasu či zmluve,
- spracovanie sa vykonáva automatizovane.

Výkonom práva na prenositeľnosť nesmú byť nepriaznivo dotknuté práva a slobody iných osôb.

K právu na prenositeľnosť údajov bol zo strany skupiny WP29 vydaný výkladový materiál dostupný tu: <https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k-pravu-na-prenosnost-udajov>.

Námietka proti spracovaniu osobných údajov

Subjekt údajov má z dôvodov týkajúcich sa jeho konkrétnej situácie právo kedykoľvek vzniesť námietku proti spracovaniu osobných údajov, ktoré sa spracovávajú na základe právnych dôvodov:

- spracovanie je nutné z dôvodu plnenia úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci, ktorou je prevádzkovateľ poverený,
- spracovanie je nutné na účely oprávnených záujmov príslušného prevádzkovateľa či tretej strany.

Prevádzkovateľ osobné údaje ďalej nespracováva, ak nepreukáže závažné oprávnené dôvody na spracovanie, ktoré prevažujú nad záujmami alebo právami a slobodami subjektu údajov, alebo na určenie, výkon alebo obhajobu právnych nárokov. Námietku je možné vzniesť aj proti spracovaniu osobných údajov na účely priameho marketingu alebo profilovania. Ak subjekt údajov vznesie námietku proti spracovaniu na účely priameho marketingu, nebudú sa už osobné údaje na tieto účely spracovávať.

Právo subjektu údajov byť predmetom žiadneho rozhodnutia založeného výhradne na automatizovanom rozhodovaní

Toto právo zaistuje subjektu údajov, že nebude predmetom rozhodnutia založeného výhradne na automatizovanom spracovaní vrátane profilovania, ktoré má preňho právne účinky alebo sa ho obdobným spôsobom významne dotýka. Automatizované rozhodovanie je prípustné v prípade, keď je nutné na uzavretie alebo plnenie zmluvy medzi subjektom údajov a prevádzkovateľom, ak je povolené právom Európskej únie alebo členským štátom alebo ak je založené na výslovnom súhlase subjektu údajov. Nie je možné tak

napríklad automatizovane pokutovať vodiča prekračujúceho rýchlosť bez toho, aby pokutu preskúmal človek. Alebo nie je možné automatizovane odmietnuť žiadosť o úver bez toho, aby žiadosť preskúmal človek.

Lehota, dokiaľ musí prevádzkovateľ reagovať na podanú žiadosť subjektu údajov

Pokiaľ ide o žiadosť podľa článkov 15 až 22 všeobecného nariadenia, musí byť informácia o prijatých opatreniach poskytnutá bez zbytočného odkladu a v každom prípade do jedného mesiaca od prijatia žiadosti. Lehotu je možné vo výnimočných prípadoch predĺžiť o dva mesiace, o čom musí byť subjekt údajov zo strany prevádzkovateľa informovaný vrátane dôvodov predĺženia.

Môže si prevádzkovateľ účtovať náklady v súvislosti s výkonom alebo zneužitím práv subjektu údajov?

Zásadne platí, že informácie podľa článkov 13 a 14 a všetky oznámenia a úkony podľa článku 15 až 22 a 34 všeobecného nariadenia sa poskytujú a robia bezplatne. Iba v prípade, keď sú žiadosti podané subjektom údajov zjavne nedôvodné alebo neprimerané (najmä preto, že sa opakujú), môže prevádzkovateľ buď uložiť primeraný poplatok, alebo odmietnuť žiadosť vyhovieť. Zjavnú nedôvodnosť dokladá prevádzkovateľ. Tu je možné taktiež hovoriť o zneužití výkonu práv subjektu údajov, ktorým však nie je možné a priori rozumieť výkon práv subjektu údajov. O zneužití práva subjektom údajov ide na-

jmä vtedy, ak sa žiadosti opakujú a sú zjavne nedôvodné či neprimerané. V takom prípade môže prevádzkovateľ uložiť primeraný poplatok alebo odmietnuť žiadosť vyhovieť. Zjavnú nedôvodnosť alebo neprimeranosť v súvislosti so zneužitím opäť dokladá prevádzkovateľ.

■ Kapitola 6.

Prevádzkovateľ, sprostredkovateľ

Zodpovednosť prevádzkovateľa

Prevádzkovateľ zodpovedá za dodržiavanie povinností kladených všeobecným nariadením. Úplne zásadné je dodržiavanie zásad spracovania, ktorých dodržiavanie zároveň musí byť prevádzkovateľ schopný doložiť. Základným nutným predpokladom je existencia riadneho právneho dôvodu spracovania osobných údajov, ktorým prevádzkovateľ musí disponovať, aby vôbec mohol osobné údaje spracovávať. Zároveň je nutné osobné údaje dostatočne zabezpečiť. Samozrejmosťou však musí byť plnenie aj ďalších povinností stanovených všeobecným nariadením.

Spoloční prevádzkovatelia

Nové všeobecné nariadenie výslovne počíta aj s možnosťou tzv. spoločných prevádzkovateľov. Ide o prípad, keď účel a prostriedok spracovania stanovujú spoločne dvaja alebo viacerí prevádzkovatelia, ktorí si medzi sebou transparentnou dohodou vymedzia svoje podiely na zodpovednosti za plnenie povinností.

Ako sa rôznych prevádzkovateľov dotýka všeobecné nariadenie?

Každého prevádzkovateľa sa všeobecné nariadenie dotýka iným spôsobom, a to v závislosti od aspektov spracovania, ktoré vykonáva. Tomu musia zodpovedať aj prípravy prevádzkovateľa na plnenie požiadaviek všeobecného nariadenia. Prístup založený na riziku viaže niektoré povinnosti iba na rizikové či veľmi rizikové spracovanie, teda niektoré povinnosti mnoho prevádzkovateľov nebude musieť plniť, zatiaľ čo na iných prevádzkovateľov budú dopadať viac-menej všetky stanovené povinnosti. Každý prevádzkovateľ by si mal urobiť vlastnú analýzu spracovania, ktorú vykonáva, čím zistí, aké eventuálne povinnosti sa naň vzťahujú. Súčasťou analýzy môže byť aj vytipovanie slabých miest prevádzkovateľa, napr. v zabezpečení, či revízia právnych dôvodov a ich uvedenie do súladu s podmienkami GDPR (napr. ak prevádzkovateľ využíva súhlas so spracovaním osobných údajov, zhodnotiť, či udelené súhlasy budú použiteľné aj v čase účinnosti všeobecného nariadenia). Ak prevádzkovateľ riadne plnil povinnosti vyplývajúce zo zákona č. 122/2013 Z. z., nemalo by všeobecné nariadenie preňho predstavovať výrazný problém, s ktorým by si neporadil. Dôležité je tiež nezabudnúť na osvetu zamestnancov.

Vzťah prevádzkovateľ – sprostredkovateľ

Prevádzkovateľ môže na spracovanie osobných údajov pribrať iný subjekt, ktorý preňho bude osobné údaje spracovávať.

Prevádzkovateľ by mal využiť iba takého sprostredkovateľa, ktorý s ohľadom na povahu, kontext, kategóriu osobných údajov a ich možnosti poskytuje dostatočné záruky vhodných technických a organizačných opatrení, tak aby spracovanie osobných údajov prostredníctvom sprostredkovateľa splňalo požiadavky všeobecného nariadenia a bola zaistená ochrana práv subjektu údajov. Na tento účel musí byť medzi prevádzkovateľom a sprostredkovateľom uzatvorená písomná zmluva, v ktorej je stanovený predmet a obdobie trvania spracovania, povaha a účel spracovania, typ osobných údajov a kategória subjektov údajov, povinnosti a práva prevádzkovateľa. Zmluva ďalej musí zaručovať určité okolnosti spracovania – pozrite článok 28 ods. 3 všeobecného nariadenia. Nie je nutné, aby išlo o samostatnú zmluvu, požadované náležitosti je možné zakomponovať aj do inej zmluvy, ktorú prevádzkovateľ so sprostredkovateľom uzatvára v rámci napríklad obchodného či iného vzťahu. Prevádzkovateľ sa prizvaním sprostredkovateľa nezbavuje zodpovednosti za spracovanie osobných údajov.

Môže sprostredkovateľ zapojiť do spracovania iného sprostredkovateľa?

Ide o tzv. reťazenie sprostredkovateľov, ktoré nie je a priori zakázané, avšak je nutné, aby prevádzkovateľ na toto dal písomný súhlas sprostredkovateľovi. Súhlas môže byť daný pre ďalšieho konkrétného sprostredkovateľa, alebo môže byť daný všeobecný súhlas, v takom prípade však

sprostredkovateľ musí prevádzkovateľa informovať o všetkých prijatých ďalších sprostredkovateľoch alebo ich nahradení. Účelom tak je, aby prevádzkovateľ, ktorý za spracovanie osobných údajov primárne zodpovedá, vedel, ktoré subjekty preňho osobné údaje spracovávajú.

■ Kapitola 7. Zabezpečenie osobných údajov

Ako musí prevádzkovateľ zabezpečiť osobné údaje
Prevádzkovateľ musí prijať s ohľadom na povahu, rozsah a účel spracovania technické a organizačné opatrenia, aby zaistil a bol schopný doložiť, že spracovanie prebieha v súlade so všeobecným nariadením. Každý prevádzkovateľ tak musí prijať adekvátne bezpečnostné opatrenia a u každého prevádzkovateľa také opatrenie môže byť, práve s ohľadom na povahu, rozsah a účel spracovania, odlišné. Jedným z prvkov zabezpečenia osobných údajov je ich pseudonymizácia alebo šifrovanie. Tieto prvky však nie sú povinné. Ich dobrovoľné nasadenie však prevádzkovateľovi môže priniesť aj zbavenie napr. povinnosti ohlásiť prípad porušenia zabezpečenia osobných údajov subjektu údajov.

Porušenie zabezpečenia osobných údajov

Za porušenie zabezpečenia osobných údajov sa považuje porušenie zabezpečenia, ktoré vedie k náhodnému alebo protiprávnemu zničeniu, strate, zmene alebo neoprávnenému poskytnutiu alebo sprístup-

neniu prenášaných, uložených alebo inak spracovávaných osobných údajov. Ak dôjde k porušeniu zabezpečenia osobných údajov, mal by prevádzkovateľ zvážiť, či nejde o okolnosť, ktorú je nutné ohlásiť dozornému úradu, resp. oznámiť subjektu údajov. Tieto povinnosti nastanú vtedy, ak porušenie zabezpečenia predstavuje riziko, resp. vysoké riziko pre práva a slobody fyzických osôb.

Kedy a čo musí prevádzkovateľ pri bezpečnostnom incidente ohlásiť Úradu na ochranu osobných údajov SR

Ak dôjde k porušeniu zabezpečenia osobných údajov, musí prevádzkovateľ toto porušenie bez zbytočného odkladu a ak to je možné do 72 hodín od okamihu, keď sa o ňom dozvedel, ohlásiť dozornému úradu, iba ak je nepravdepodobné, že by toto porušenie malo za následok riziko pre práva a slobody fyzických osôb. Práve používanie pseudonymizácie či šifrovania môže prípadné riziko úplne eliminovať, a teda aj zbaviť prevádzkovateľa nutnosti prípad ohlásiť dozornému úradu. Vždy je však nutné mieru rizika posúdiť, a to aj v prípade, že bola použitá pseudonymizácia či šifrovanie. V oznámení prevádzkovateľ subjektu údajov musí popísať povahu porušenia zabezpečenia, prijaté opatrenia, pravdepodobné dôsledky a tiež musí oznámiť kontaktné údaje na zodpovednú osobu na ochranu osobných údajov, ak bola ustanovená. Ak nastane porušenie zabezpečenia u sprostredkovateľa, hlási ho prevádzkovateľovi, pre ktorého dotknuté osobné údaje spracováva.

Kedy a čo musí prevádzkovateľ pri bezpečnostnom incidente oznámiť subjektu údajov

V prípade, že porušenie zabezpečenia predstavuje vysoké riziko pre práva a slobody subjektu údajov, vzniká prevádzkovateľovi povinnosť upovedomiť o tejto udalosti subjekt údajov. Prevádzkovateľ tak nemusí urobiť, ak použil predbežné opatrenia, ktoré robia osobné údaje nečitateľnými pre všetky neoprávnené osoby (napr. šifrovanie alebo unikli pseudonymizované údaje bez väzby na subjekt údajov) či použil následné opatrenia, ktoré zaistia, že vysoké riziko sa už pravdepodobne neprejaví. Povinnosť oznámiť bezpečnostný incident subjektu údajov prevádzkovateľovi nenastane ani vtedy, ak by to vyžadovalo neprimerané úsilie. V takom prípade však musia byť subjekty údajov informované rovnako účinným spôsobom pomocou verejného oznámenia.

Určenie rizika porušenia zabezpečenia

Pri určovaní rizika porušenia zabezpečenia je nutné vychádzať najmä z kategórie osobných údajov, ktoré boli porušením zabezpečenia dotknuté, charakteru porušenia zabezpečenia a počtu dotknutých subjektov údajov. Vyššie riziko budú vždy predstavovať zvlášť kategórie osobných údajov (napr. údaje o zdravotnom stave), prípadne údaje, ktorými je možné spôsobiť subjektu údajov ujmu či zásah do jeho práv (napr. únik prihlasovacích údajov do elektronického bankovníctva). Ďalším rozhodným prvkom môže byť aj okolnosť, či došlo k porušeniu zabezpečenia úmyselne,

či nedbalostne, pričom úmyselný čin výrazne zvyšuje riziko takého činu, keďže osobné údaje boli terčom útoku. Posúdiť porušenie zabezpečenia je tak nutné komplexne, nie izolovane, a prekonané riziko následne určí eventuálnu povinnosť oznámiť porušenie zabezpečenia Úradu na ochranu osobných údajov alebo aj oznámiť subjektu údajov.

Musia byť vždy osobné údaje u prevádzkovateľa v šifrovanej alebo pseudonymizovanej podobe?

Šifrovanie ani pseudonymizácia nie sú výslovnou podmienkou spracovania osobných údajov. Sú bezpečnostným prvkom, ktorý aj v niektorých prípadoch môže prevádzkovateľovi zlepšiť jeho postavenie v prípade únikov týchto údajov, keďže v takom prípade sa naň nemusí (v závislosti od prípadu, neznamená to, že zakaždým) vzťahovať povinnosť ohlasovať prípad porušenia zabezpečenia osobných údajov dozornému úradu, resp. ho oznamovať subjektu údajov. Vždy je však nutné mieru rizika posúdiť, a to aj v prípade, že bola použitá pseudonymizácia či šifrovanie. Je možné preto odporučiť prevádzkovateľom, ktorých povaha spracovania osobných údajov im to umožňuje, uchovávať (spracovávať) údaje v šifrovanej či pseudonymizovanej podobe, na čo aj všeobecné nariadenie nabáda.

■ Kapitola 8.

Zodpovedná osoba na ochranu osobných údajov

Kto musí menovať zodpovednú osobu na ochranu osobných údajov

Zodpovednú osobu musí menovať prevádzkovateľ a sprostredkovateľ, ak:

- spracovanie vykonáva orgán verejnej moci či verejný subjekt s výnimkou súdov konajúcich v rámci svojich súdnych právomocí,
 - hlavné činnosti spočívajú v operáciách spracovania, ktoré kvôli svojej povahe, svojmu rozsahu alebo svojim účelom vyžadujú rozsiahle pravidelné a systematické monitorovanie subjektov údajov,
 - hlavné činnosti spočívajú v rozsiahlom spracovaní zvláštnych kategórií osobných údajov a osobných údajov týkajúcich sa rozsudkov v trestných veciach.
- Skupina podnikov môže menovať jedinú zodpovednú osobu, avšak musí byť pre každý podnik ľahko dosiahnuteľná.

Musí mať svoju zodpovednú osobu každá obec?

Vzhľadom na to, že obec je možné považovať za orgán verejnej moci, resp. verejný subjekt v zmysle článku 37 ods. 1 písm. a) všeobecného nariadenia, formálne na ňu dopadá povinnosť menovať zodpovednú osobu. Nie je však nutné, aby každá obec musela mať svoju vlastnú samostatnú zodpovednú osobu, ale je možné, aby pre určitý počet obcí vykonávala činnosť zodpovednej osoby napr. zodpovedná osoba vyššieho územného samosprávneho celku či sa niekoľko obcí dohodlo a najali

si vlastnú zodpovednú osobu. S týmto ostatne počíta aj všeobecné nariadenie, ktoré umožňuje pre viac prevádzkovateľov, ktorí sú orgánom verejnej moci či verejným subjektom, menovať jednu zodpovednú osobu.

Musí byť zodpovedná osoba organizačne podriadená priamo vedeniu organizácie?

Zodpovedná osoba na ochranu osobných údajov musí byť priamo podriadená vrcholovým riadiacim pracovníkom prevádzkovateľa alebo sprostredkovateľa. Nejde však o podmienku organizačnú, t. j. že zodpovednú osobu musí riadiť priamo vedená organizácia, ale ide o podmienku, aby zodpovedná osoba mala priamy prístup k vedeniu organizácie, t. j. aby pri poskytovaní informácií vedeniu organizácie nebol medzi zodpovednou osobou a vedením ďalší medzičlánok a zodpovedná osoba sa tak na vedenie organizácie mohla kedykoľvek obrátiť v záležitostiach ochrany osobných údajov.

Úlohy zodpovednej osoby na ochranu osobných údajov

Medzi úlohy zodpovednej osoby patrí predovšetkým poskytovanie informácií a poradenstvo prevádzkovateľovi či sprostredkovateľovi vrátane zamestnancov, ktorí sa na spracovaní podieľajú. Zodpovedná osoba ďalej monitoruje súlad spracovania so všeobecným nariadením a ďalšími predpismi. Zodpovedná osoba poskytuje na vyžiadanie poradenstvo, pokiaľ ide o posúdenie vplyvu na ochranu osobných údajov. Neoddeliteľnou súčasťou výkonu funk-