

www.
gdpr365.info

DonauMedia

PRAKTICKÝ MANUÁL GDPR PRO KAŽDÉHO

Vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů v praktickém kompletu s webem a aktualizacím servisem

Exkluzivně a **ZDARMA** k této příručce:

**ON-LINE
předpisy**

**365
servis**



E-book, bezplatná aktualizace:

Načtěte QR a odešlete SMS na +420 739 866 871

Podrobnosti na www.gdpr365.info

STORMWARE
POHODA
Ekonomický software

Připraveno
na **GDPR**



Volejte zdarma:

800 178 278

www.pohoda.cz



9788081830501

INFORMACE K BONUSŮM

Nedílnou součástí této publikace v pdf v právním stavu k 1. dubnu 2018 je aktualizací servis s novými právními výklady, stanovisky a legislativou, e-booky s platnými zněními vždy po změnách a další služby na servisní webové stránce www.gdpr365.info. Aktualizace obdržíte mailem po jednoduché registraci, která je zdarma a nezavazuje k odběru žádných dalších produktů nebo služeb.

POSTUP REGISTRACE: 1. registrujete se pomocí QR kódu na obálce **NEBO** 2. odešlete SMS *ManualGDPR_18_CR_Aktualizace* na číslo +420 739 866 871 **NEBO** 3. odešlete e-mail s předmětem nebo textem *ManualGDPR_18_CR_Aktualizace* na adresu newsletter@newsletter.cz **NEBO** 4. vyplňte formulář na www.gdpr365.info

IMPRESSUM

Praktický manuál GDPR pro každého (e-book v pdf)

ISBN 978-80-8183-050-1

DonauMedia, s. r. o., Bratislava, Slovenská republika © 2018. Všechna práva vyhrazena.

Informace: newsletter@newsletter.cz

Vyrobeno v EU.

Úvodní text Zvládněte základy GDPR za 30 minut a texty Malý slovník pojmů, Desatero zpracování pro správce, Desatero omylů o GDPR, Mýty o veřejných WiFi v souvislosti s obecným nařízením GDPR a Udělit souhlas se zpracováním osobních údajů je možnost, nikoliv povinnost byly publikovány s laskavým svolením Úřadu pro ochranu osobních údajů (www.uoou.cz, *titulky a mezititulky doplnila redakce vydavatelství*). Text Desatero pro živnostníky a malé firmy připravili JUDr. Ing. Jaroslav Švamberk a Bc. Jaromír Kuba ze společnosti Kuba a partneři s. r. o. (www.poverenec.info). Další prameny: webové stránky eur-lex.europa.eu, dataprotection.gov.sk, publikace 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

Účetnictví a GDPR
pod jednou střechou



www.pohoda.cz

Praktický manuál GDPR pro každého

PĚT MINUT TEORIE NA ÚVOD	4
ZVLÁDNĚTE ZÁKLADY OBECNÉHO NAŘÍZENÍ GDPR ZA 30 MINUT	10
MALÝ SLOVNÍK POJMŮ	23
DESATERO ZPRACOVÁNÍ PRO SPRÁVCE	26
DESATERO PRO ŽIVNOSTNÍKY A MALÉ FIRMY	27
UDĚLIT SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ JE MOŽNOST, NIKOLIV POVINNOST	29
MÝTY O VEŘEJNÝCH SÍTÍCH WiFi V SOUVISLOSTI S OBECNÝM NAŘÍZENÍM GDPR	29
DESATERO OMYLŮ O GDPR	30
OPAKOVÁNÍ	33
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679	36



PĚT MINUT TEORIE NA ÚVOD

GDPR:

BEZPROSTŘEDNÍ PLATNOST
VNITROSTÁTNÍ ÚPRAVY
TRANSPARENTNOST
PRÁVNÍ ODŮVODNĚNOST

Na rozdíl od předchozí směrnice 95/46/EU (Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů), kterou musely státy EU prosadit do národních předpisů, platí **Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ve všech členských státech od 25. května 2018 přímo** (je z kategorie obecných nařízení, v tuzemském právu má váhu zákona publikovaného ve Sbírce zákonů). Jednotlivé členské státy pouze musí s pomocí vlastních právních předpisů uvést právo na ochranu osobních údajů podle nového nařízení do souladu s právem na svobodu projevu a informace (viz

článek 88 obecného nařízení) a upravit některé další dílčí otázky, neboť obecné nařízení obsahuje otevřená ustanovení, která umožňují jednotlivým členským státům určovat si některé aspekty ochrany osobních údajů na vnitrostátní úrovni. Členským státům ale v zásadě není dovoleno oslabovat nebo zpřísnovat předepsanou ochranu osobních údajů vlastní domácí legislativou. Otevřená ustanovení je třeba v České republice upravit novým zákonem o zpracování osobních údajů,

který byl v době uzávěrky této publikace v meziresortním připomínkovém řízení (obecné nařízení předpokládá, že vnitros-

Kuba a partneři s.r.o.

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

Upozornění: *Znění textů v této publikaci bylo prověřeno s veškerou dostupnou péčí, vydavatel ani prodejce však nepřebírají žádné záruky za eventuální škody vzniklé jejím použitím a neodpovídají tedy za to, pokud by na základě textů zveřejněných v této publikaci kdokoliiv konal nebo se zdržel konání a v souvislosti s tím mu vznikla jakákoliv škoda materiální nebo nemateriální povahy. Jediným rozhodujícím zněním zákonů v případě pochybností a sporů jsou texty ve Sbírce zákonů. Autorská práva k této publikaci jsou předmětem ochrany podle zákonů ČR a SR a vykonává je výhradně vydavatel. Rozmnožování a šíření jakýmkoliv způsobem celku nebo části této publikace bez výslovného písemného svolení vydavatele je zakázáno. Nerespektování práv vydavatele může vést k soudnímu postihu včetně povinnosti náhrady škody.*

tátní legislativní úpravy měly být hotové již k 25. květnu 2018). Zákon č. 101/2000 Sb., o ochraně osobních údajů bude zrušen.

Obsah a struktura

Nariadení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), zkráceně též *General Data Protection Regulation*, *GDPR* nebo dále také pouze *obecné nařízení* je součástí reformy ochrany osobních údajů v rámci celé EU. Obecné nařízení tvoří 99 článků rozčleněných do jedenácti kapitol:

■ **Kapitola 1** (Články 1 až 4): Obecná ustanovení (předmět a cíle, věcná a místní působnost, definice)

■ **Kapitola 2** (Články 5 až 11): Zásady (zásady zpracování osobních údajů, zákonnost zpracování, podmínky vyjádření souhlasu, podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti, zpracování zvláštních kategorií osobních údajů, zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů, zpracování, které nevyžaduje identifikaci)

■ **Kapitola 3** (Články 12 až 23): Práva subjektu údajů (transparentní informace, sdělení a postupy pro výkon práv subjektu údajů, informace a přístup k osobním údajům, právo na opravu, právo na výmaz, právo na omezení zpracování, oznamovací povin-

nost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování, právo na přenositelnost údajů, právo vznést námitku a automatizované individuální rozhodování)

■ **Kapitola 4** (Články 24 až 43): Správce a zpracovatel (obecné povinnosti, odpovědnost správce, záměrná a standardní ochrana osobních údajů, společní správci, zástupci správců nebo zpracovatelů, kteří nejsou usazeni v Unii, zpracovatel, zpracování z pověření správce nebo zpracovatele, záznamy o činnostech zpracování, spolupráce s dozorovým úřadem, zabezpečení osobních údajů, zabezpečení zpracování, ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu, oznamování případů porušení zabezpečení osobních údajů subjektu údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace, pověřenec pro ochranu osobních údajů, kodexy chování a vydávání osvědčení)

■ **Kapitola 5** (Články 44 až 50): Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (obecná zásada pro předávání, předání založené na rozhodnutí o odpovídající ochraně, předávání založené na vhodných zárukách, závazná podniková pravidla, předání či zveřejnění údajů nepovolená právem Unie, výjimky pro specifické situace, mezinárodní spolupráce v zájmu ochrany osobních údajů)

■ **Kapitola 6** (Články 51 až 59): Nezávislé dozorové úřady (obecné podmínky pro členy dozorového úřadu, pravidla pro zřízení dozorového úřadu, příslušnost, úkoly a pra-

vomoci)

■ **Kapitola 7** (Články 60 až 76): Spolupráce a jednotnost (spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady, vzájemná pomoc, společné postupy dozorových úřadů, mechanismus jednotnosti, stanovisko sboru, řešení sporů sborem, postup pro naléhavé případy, výměna informací, evropský sbor pro ochranu osobních údajů)

■ **Kapitola 8** (Články 77 až 84): Právní ochrana, odpovědnost a sankce (právo podat stížnost u dozorového úřadu, právo na účinnou soudní ochranu vůči dozorovému úřadu, správci nebo zpracovateli, právo na náhradu újmy a odpovědnost, obecné podmínky pro ukládání správních pokut, sankce)

■ **Kapitola 9** (Články 85 až 91): Ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování (zpracování a svoboda projevu a informací, zpracování a přístup veřejnosti k úředním dokumentům, zpracování národních identifikačních čísel, zpracování v souvislosti se zaměstnáním, záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, povinnost mlčenlivosti, zavedená pravidla pro ochranu údajů uplatňovaná církvemi a náboženskými sdruženími)

■ **Kapitola 10** (Články 92 až 93): Akty v přenesené pravomoci a prováděcí akty (výkon přenesené pravomoci)

■ **Kapitola 11** (Články 94 až 99): Závěrečná ustanovení (zrušení směrnice 95/46/ES, vztah

ke směrnici 2002/58/ES, vztah k dříve uzavřeným dohodám, vstup v platnost a použitelnost)

99 článků je uvozeno 173 body tzv. recitálů, které představují odůvodnění, resp. výklad jednotlivých zásad.

Oblasti nové úpravy

Mnoho principů ochrany osobních údajů přešlo z původní směrnice do nového obecného nařízení. Především pojem *osobní údaje* v článku 4 byl v zásadě zachován: *osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.* Dále platí stejně jako dosud, že zpracování osobních údajů bez souhlasu dotčené osoby je přípustné jen na základě existence zákonných důvodů. Ty jsou uvedeny v článku 6:

- zpracování je potřebné pro naplnění smlouvy nebo pro uskutečnění předsmulvních opatření;
- zpracování je potřebné pro naplnění právních závazků;
- zpracování je potřebné pro ochranu životně důležitých zájmů subjektu údajů;
- zpracování je potřebné pro splnění úkolu, který je ve veřejném zájmu;

– zpracování je potřebné pro ochranu oprávněných zájmů správce nebo třetí osoby.

Je však nutné zvážení těchto zájmů oproti zájmům dotčené osoby.

Principy zpracování osobních údajů

Obecné nařízení uvádí v článku 5 explicitně šest principů pro zpracování osobních údajů:

- zákonnost, korektnost a transparentnost;
- účelovost (zpracování jen pro jasné dané, jednoznačné a legitimní účely);
- minimalizaci (přiměřenost, omezenost na nezbytný rozsah ve vztahu k účelu zpracování);
- přesnost;
- omezenost (uložení po dobu ne delší, než je nezbytné pro účely zpracování);
- integritu a důvěrnost (zpracování způsobem, který zajistí náležité zabezpečení).

Nerušená výměna osobních údajů v rámci EU

Výměna osobních údajů v rámci EU nesmí být odmítnutá s argumentem, že se v různých zemích v rámci EU s ochranou údajů zachází jinak. Článek 1 odstavec 3 stanoví: *Volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán.*

Oblast platnosti

Obecné nařízení nerozlišuje mezi zpracováním osobních údajů veřejnými institucemi a soukromými firmami – pro všech-

ny zpracovatele platí stejná práva a povinnosti. Přesto určité druhy zpracování osobních údajů nespádají podle článku 2 obecného nařízení pod tuto úpravu. Recitály 16 a 18 to blíže objasňují:

(16) Toto nařízení se nevztahuje na otázky ochrany základních práv a svobod nebo volného pohybu osobních údajů v souvislosti s činnostmi, které nespádají do působnosti práva Unie, jako jsou činnosti týkající se národní bezpečnosti. Toto nařízení se rovněž nevztahuje na zpracování osobních údajů členskými státy při výkonu činnosti v rámci společné zahraniční a bezpečnostní politiky Unie.

(18) Toto nařízení se nevztahuje na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností. Činnosti osobní povahy nebo činnosti v domácnosti by mohly zahrnovat korespondenci a vedení adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi. Toto nařízení se však vztahuje na správce nebo zpracovatele, kteří pro tyto činnosti osobní povahy či činnosti v domácnosti poskytují prostředky pro zpracování osobních údajů.

Princip místního trhu

Evropské právo na ochranu osobních údajů platí také pro mimounijní firmy, pokud nabízejí svoje výrobky nebo služby v rámci jednotného evropského trhu. Princip místního trhu je jedním z mnoha principi-

pů, které upravují právní postavení firem nabízejících výrobky a služby na společném trhu. Místní trh je místo, na kterém se střetávají zájmy prodávajících a nakupujících a s ohledem na konkurenci je to také místo výrazného křížení konkurenčních zájmů. Proto se uplatňují pravidla konkrétního trhu, na který je nabídka zaměřena. Díky tomu se pak na cílovém trhu vyrovnávají rozdíly mezi podmínkami pro domácí a zahraniční firmy.

Požadavek na souhlas

V principu jsou požadavky na účinný souhlas se zpracováním osobních údajů definovány tak, že písemná forma není nutná, je přípustný souhlas udělený technickým nastavením (např. prohlížeče při prohlížení webové stránky), prohlášením či jednáním, ale musí jít o jasnou signalizaci souhlasu v daných souvislostech, což musí být zpracovatel schopen prokázat. Mlčení, předem zaškrtnutá políčka nebo nečinnost nelze za souhlas považovat (viz recitál 32). Písemná forma je nutná pro souhlas se zpracováním zvláštních osobních údajů.

Omezení zpracovávaných údajů

Obecné nařízení spočívá na zásadě minimalizace zpracovávaných údajů podmíněné účelem. K určitému účelu (například zaslání objednaného zboží a vystavení faktury) tak může být zpracovááno třeba jméno, adresa, e-mailová adresa a telefon, ale k dosažení tohoto účelu už nejsou

třeba žádné jiné údaje.

Transparentnost

Recitál 39 vyzdvihuje princip transparentnosti každého zpracování údajů pro dotčené osoby. Na různých místech vyžaduje obecné nařízení odpovídající opatření:

- podle článku 15 má každá osoba právo na informace o všech údajích, které se jí týkají,

- tyto informace musí být poskytnuty podle článku 12 v precizní, transparentní, srozumitelné, lehce dostupné a jednoduše pochopitelné podobě,

- podle článků 13 a 14 musí každá dotčená osoba dostat při získávání údajů úplné informace, mimo jiné o účelu, příjemci a osobě zodpovědné za zpracování údajů, době uchování údajů, právu na úpravu, zabezpečení uložení a výmazu a použití údajů pro účely profilování. Pokud se účel změní, musí být dotčená osoba aktivně informovaná,

- podle článku 16 má dotčená osoba právo na opravu nesprávných údajů, stejně jako má podle článku 18 právo na omezení (blokování) zpracování údajů, pokud je sporná správnost nebo důvod pro zpracování údajů.

Efektivita těchto práv ale závisí na nevysloveném předpokladu, že se dotčená osoba musí sama aktivně starat o to, kdo a jak o ní zpracovává údaje a sama se těchto práv dožadovat (přestože právě toto kritici obecného nařízení nevnímají jako příliš reálné). Vedle toho má obecné nařízení podle recitálu 13 ovlivnit také trans-

parentnost a právní bezpečnost pro **7** nejmenší firmy, malé a střední podniky (do 250 zaměstnanců), jejichž potřeby jsou specifické.

Právo být zapomenut

Právo být zapomenut, které je přímo vyjádřené v nadpisu článku 17, je jedno ze základních práv vyplývajících z obecného nařízení. Zahrnuje na jedné straně právo dotčené osoby požadovat výmaz všech údajů, které se jí týkají, pokud pominou důvody pro uchování těchto údajů. Dále musí správce sám aktivně mazat údaje, u kterých už neexistuje žádný důvod pro jejich uchování a zpracování.

Právo na přenositelnost údajů

Stejně jako předcházející úprava, požaduje obecné nařízení v článku 20, aby dotčená osoba (subjekt údajů) měla právo získat údaje, které se jí týkají, ve strukturované, standardní, běžně používané a strojově čitelné podobě a mohla tak předat tuto údaje bez omezení jinému správci, aniž by tomu původní správce bránil. Při výkonu práva na přenositelnost údajů má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

Sankce

Pro efektivní prosazení pravidel na ochranu osobních údajů je nově možné ukládat vyšší pokuty než dosud. Mimo to mohou místní dozorové úřady do budoucna poža-

dovat sankce nejen po privátních správcích údajů, ale také po veřejných institucích, pokud to ovšem umožňují národní předpisy. Výše pokut za přestupky proti obecnému nařízení je stanovena podle článku 83 až do dvaceti miliónů euro nebo do čtyř procent mezinárodního ročního obrátu. Členské státy mimo to mohou stanovit další možnosti sankcí. Například podle recitálu 149 je možné do pokuty zahrnout (odebrat) i zisky dosažené v souvislosti s přestupkem. Vždy však platí zásada přiměřenosti sankce. Náležitě by se tedy měla zohlednit povaha, závažnost a doba trvání porušení, úmyslný charakter porušení, kroky, které byly učiněny s cílem zmírnit způsobenou škodu, míra odpovědnosti nebo jakékoli relevantní předchozí porušení, způsob, jakým se dozorový úřad o daném porušení dozvěděl, dodržování opatření, která byla vůči správci nebo zpracovateli nařízena, dodržování kodexu chování nebo jakýkoli jiný přitěžující nebo polehčující faktor. Je tedy možné místo peněžité sankce uložit také pouhé napomenutí. Uložení sankcí včetně správních pokut by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami právních předpisů Unie a Listiny základních práv a svobod, včetně účinné právní ochrany a spravedlivého procesu.

Privacy by design, privacy by default

Recitál 78 zahrnuje pojmy *data protection by design* a *data protection by default* (běžněji používané jako *privacy by design*

a *privacy by default*). Tyto pojmy znamenají, že technika (*design*) zpracování údajů by měla být navrhovaná a tak zaměřená a nastavení organizačních opatření (*defaults*) by mělo být takové, aby bylo učiněno zadost potřebám ochrany osobních údajů a bylo zajištěno splnění požadavků vyplývajících z obecného nařízení. Takto dokumentovaný postup může pomoci správcům a zpracovatelům při dodržování obecného nařízení. Výklad těchto principů může být poměrně široký. Zjednodušeně řečeno zahrnuje například to, že počítače, počítačové sítě, datová úložiště, aplikace apod. by měly být navrhovány a konstruovány tak, aby umožňovaly zabezpečení a přístup k nim by měly mít pouze oprávněné osoby.

Požadavky na jmenování pověřenců

Obecné nařízení předpokládá jmenování osob pověřených dohledem nad ochranou osobních údajů (pověřenců) u jednotlivých správců, minimálně u všech orgánů veřejné moci a veřejných subjektů (s výjimkou soudů) a v těch soukromých společnostech, u nichž vznikají rizika při zpracování osobních údajů. Článek 37 obecného nařízení zavádí minimální standard pro zřízení těchto pozic. Malí podnikatelé a malé společnosti nemusí mít žádného pověřence, pokud jejich hlavní činnosti nespočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo nespočívají v rozsáhlém zpra-

cování zvláštních kategorií údajů. Pojem *rozsáhlé zpracování* a předpoklady pro posouzení vlivu na ochranu údajů jsou přesněji popsány v recitálu 91. Některé profese jako například právníci, lékaři nebo lékárníci (*příslušníci zdravotnických povolání*) nemusejí ustanovit pověřence (posouzení vlivu na ochranu osobních údajů u nich není povinné).

Ustanovení o výjimkách (otevřené klauzule)

Obecné nařízení předpokládá, že vnitrostátní předpisy upřesní v mnohých oblastech právo na ochranu osobních údajů detailními úpravami. Obecné nařízení obsahuje takových otevřených klauzulí několik desítek. Některá ustanovení o výjimkách přímo vyžadují právní úkony po členských státech (přijetí speciální právní úpravy), některá jen dávají pro vnitrostátní úpravu prostor. Ten je ovšem v zásadě omezený tak, aby nebyla snížena hranice ochrany osobních údajů s hranicemi danými obecným nařízením. Příkladem otevřené klauzule může být ochrana údajů zaměstnanců: článek 88 odstavec 1 umožňuje, aby si členské státy stanovily specifické předpisy pro zajištění práv a svobod při zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním. Formulace tohoto pravidla sice neumožňuje zpřísnění ani úlevy v ochraně osobních údajů, ale předpokládá konkrétní úpravy v národních předpisech. Další ustanovení o výjimkách můžeme nalézt:

– v článku 9 odstavcích 2 a 4 pro stanove-

ní zvláštních podmínek pro zpracování zvláštních druhů osobních údajů, jako jsou zdravotní záznamy nebo údaje o sexuální orientaci;

– v článku 10 pro povolení ke zpracování údajů o rozsudcích v trestních věcech a trestných činech;

– v článku 28 o právních základech zpra-

cování údajů zpracovatelem pro správce na smluvním základě;

– v článku 37 o požadavcích na pověřené osoby (rozdílných od podmínek stanovených v tomto článku);

– v článku 85 pro vyrovnání rozdílů mezi ochranou údajů a svobodou projevu nebo pro pravidla svobody tisku;

– v článku 87 pro pravidla zpracování národních identifikačních čísel nebo údajů všeobecného významu;

– v článku 89 pro pravidla výjimek v právech dotčených osob při zpracování údajů pro vědecké, historické, statistické nebo archivní potřeby.

9

STORMWARE
POHODA
Ekonomický software

Účetnictví a GDPR
pod jednou střechou



www.pohoda.cz

ZVLÁDNĚTE ZÁKLADY OBECNÉHO NAŘÍZENÍ GDPR ZA 30 MINUT

To, co se obecně rozumí pod zkratkou GDPR (General Data Protection Regulation) je v přesné terminologii Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Jde o dosud nejobsáhlejší jednotný legislativní rámec, který byl přijat s cílem zajistit základní práva občanů EU na ochranu v souvislosti se zpracováním osobních údajů. Jelikož obecné nařízení stanovilo práva a povinnosti při zpracování osobních údajů, v tomto rozsahu zákon č. 101/2000 Sb., o ochraně osobních údajů nahradilo. Práva a povinnosti stanovená zákonem o ochraně osobních údajů byla tedy nahrazena právy a povinnostmi vyplývajících z obecného nařízení o ochraně osobních údajů. Zákon o ochraně osobních údajů bude v blízké budoucnosti zrušen a nahrazen připravovaným zákonem o zpracování osobních údajů, který bude upravovat pouze některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci, působnost, činnost apod.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které obecné nařízení neupravuje nebo je umožňuje upravit na vnitrostátní úrovni (v některých otázkách dokonce obecné nařízení vnitrostátní úpravu předpokládá: zpracování osobních údajů pro účely výkonu svobody projevu, právo na informace, novinářská činnost, svoboda vědeckého bádání, literární tvorba, umělecký projev, veřejný zájem, ochrana zdroje informací). Nový zákon také vymenuje další konkrétní přestupky a možné sankce za ně. Výše případných pokut je vždy specifikována jako „do částky“ a pro jednotlivé přestupky je v návrhu zákona stanovena do 5 000 korun až do 1 000 000 korun, v jednom z případů obzvláště závažných až do 10 000 000 korun. Obecné nařízení je univerzálně použitelné ve všech státech Evropského hospodářského prostoru, tedy ve státech Evropské unie, na Islandu, v Norsku a Lichtenštejnsku).

■ Kapitola 1. Obecné nařízení

Revize právního rámce ochrany osobních údajů

K revizi bylo přikročeno z toho důvodu, že právní rámec založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současné době, zejména pokud jde o prostředky, které jsou ke zpracování vy-

užívány a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami let (např. v oblasti profilování, automatizace zpracování osobních údajů atd.). Zároveň v jednotlivých zemích Evropské unie nebyla Směrnicí 95/46/ES dosažena požadovaná míra sjednocení právní úpravy, což správcům působícím ve více zemích činilo problémy. Cílem obecného nařízení je přizpůsobení právního rámce ochrany osobních

údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektu údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady.

Kdo se bude muset obecným nařízením řídit

Obecným nařízením se bude především, pokud jde o povinnosti, řídit subjekt, který zpracovává osobní údaje. Takový sub-

jekt je nazýván správcem osobních údajů. Obecným nařízením se řídí i zpracovatel, což je subjekt, který pro správce osobní údaje zpracovává. Pokud jde o práva vyplývající z obecného nařízení, ta plynou fyzické osobě, což je subjekt údajů. Dále se obecným nařízením budou řídit i dozorové úřady, tj. i Úřad pro ochranu osobních údajů, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů.

Na jaké činnosti obecné nařízení nedopadá

Z působnosti obecného nařízení jsou vyloučeny činnosti fyzické osoby [viz článek 2 odst. 2 písm. c) obecného nařízení], při kterých jsou zpracovávány osobní údaje výlučně pro osobní či domácí činnost. Dále je z působnosti obecného nařízení vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. To je předmětem úpravy Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Jelikož jde o směrnici, je nutné její provedení (promítnutí do tuzemské legislativy), které bude vesměs v zákoně č. 273/2008 Sb., o Policii České

republiky a též i v novém zákoně o zpracování osobních údajů.

■ Kapitola 2.

Nové přístupy a povinnosti

Nové přístupy, na kterých je obecné nařízení založeno

Lze hovořit o dvou nových přístupech, na kterých je obecné nařízení založeno. Novými přístupy jsou princip odpovědnosti správce a přístup založený na riziku. Princip odpovědnosti znamená odpovědnost správce za dodržení zásad zpracování, které jsou uvedeny v článku 5 odst. 1 obecného nařízení a zároveň musí správce být schopen tento soulad doložit. K dokládání souladu budou mimo jiné sloužit kodexy, osvědčení či certifikace, případně záznamy o činnostech zpracování (viz dále). Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. V užším slova smyslu můžeme hovořit o přístupu založeném na riziku jako o aplikaci některých povinností pouze v případě, kdy zpracování osobních údajů či porušení zabezpečení (bezpečnostní incident) představuje riziko či vysoké riziko pro práva a svobody fyzické osoby. V tomto rozsahu princip založený na riziku se uplatňuje zejména u nových povinností: ohlašování, resp. oznamování případu porušení

zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, resp. subjektu údajů, posuzování vlivu zpracování na ochranu osobních údajů a povinné konzultace s Úřadem pro ochranu osobních údajů, jejichž aplikace je vázána na přítomnost rizika či vysokého rizika pro práva a svobody fyzických osob.

Jak správce dokládá soulad zpracování

Ke splnění stanovené odpovědnosti správce za soulad zpracování se zásadami zpracování a schopnost tento soulad prokázat, mají správci, jak výslovně zmiňuje obecné nařízení, napomáhat mimo jiné i kodexy, osvědčení (pečetě, známky) a záznamy o činnostech zpracování. Kodexy mají správci, zejména na sektorové úrovni, sloužit jako vodítko správné praxe při zpracování osobních údajů právě s ohledem na specifčnost daného sektoru (např. bankovníctví, telekomunikace, internetové obchody, zdravotnictví). Osvědčení má sloužit k prokázání souladu zpracování s obecným nařízením. Záznamy o činnostech zpracování obsahují informace o prováděném zpracování, což správci umožní lehčí orientaci ohledně zpracování, která provádí. Tato povinnost je stanovena v článku 30 obecného nařízení, přičemž někteří správci jsou vyňati z nutnosti vést záznamy o činnostech zpracování. Dokládání souladu zpracování však nelze omezit pouze na shora uvedené možnosti, ale dokládání souladu je komplexní činnost, zahrnující dílčí činnosti, mezi které lze zařadit nejen shora uvedené kodexy, osvěd-