

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

Vyrobena 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 obratu. 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 specifickou 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-

čení a záznamy o činnostech zpracování, ale například i zveřejňování informací, které obecné nařízení ukládá správci zveřejňovat, vyhotovením vnitřních předpisů až po řádnou spolupráci s příslušným dozorovým úřadem.

Kodexy a osvědčení

Kodexy budou moci vydávat sdružení či jiné subjekty zastupující různé kategorie správců nebo zpracovatelů přičemž návrh kodexu musí být předložen Úřadu pro ochranu osobních údajů, který vydá stanovisko, zdali je daný kodex či návrh na jeho změnu, v souladu s obecným nařízením a pokud shledá, že ano, schválí jej. Schváleným kodexem se pak můžou řídit správci v daném sektoru. Osvědčení o souladu zpracování bude moci vydávat k tomu akreditovaný subjekt.

Nové povinnosti vyplývající z obecného nařízení

Základní zásady, principy a klíčové instrumenty zůstaly de facto neměnné, resp. byly pouze detailněji rozpracovány a zpřesněny (např. nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.). Obecné nařízení na těchto základech přineslo nastavbu spočívající v dodatečných nových povinnostech, které jsou pro české správce nové.

Jde zejména o tyto nové povinnosti:

- povinnost vést záznamy o činnostech zpracování,
- posouzení vlivu na ochranu osobních údajů,

- předchozí konzultace,
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů,
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů,
- ustavení pověřence pro ochranu osobních údajů.

Kromě povinnosti vést záznamy o činnostech zpracování a ustanovit pověřence, jsou ostatní nové povinnosti založeny na přístupu založeném na riziku, tj. jejich uplatnění je vázáno na přítomnost rizika či vysokého rizika pro práva a svobody subjektu údajů. Avšak být u povinnosti ustanovit pověřence není přímo pracováno s pojmy riziko či vysoké riziko, odráží se v této povinnosti do určité míry též přístup založený na riziku, jelikož pro určitá zpracování, resp. určité subjekty, je povinností ustanovit pověřence pro ochranu osobních údajů.

Kdy musí správce posoudit vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před počtem předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek.

Posouzení vlivu na ochranu osobních údajů se vyžaduje především:

- u systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky,
- u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech,
- u rozsáhlého systematického monitorování veřejně přístupných prostorů.

Kdy musí správce konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů

Správce je povinen konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů, pokud z posouzení vlivu na ochranu osobních údajů vyplýne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika. Účelem předchozí konzultace je tak korigovat hrozící vysoké riziko.

Záznamy o činnostech

Záznamy o činnostech zpracování představují do jisté míry náhradu za oznamovací povinnost, která byla obecným nařízením zrušena. Správce a zpracovatel, pokud se na ně nevztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, jsou povinni vést záznamy s určitými informacemi. Tyto záznamy následně umožní správci prokázat soulad zpracování

osobních údajů s obecným nařízením.

Kdo nemusí vést záznamy o činnostech zpracování

Vést záznamy o činnostech zpracování nedoléhá na podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech.

■ Kapitola 3.

Zásady a právní důvody zpracování

Zásady, na kterých je postaveno obecné nařízení

Zásady lze ve stručnosti shrnout takto:

- zákonnost, korektnost, transparentnost
 - správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,
- omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
- minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
- přesnost – osobní údaje musí být přesné,
- omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpra-

covávány,

– integrita a důvěrnost – technické a organizační zabezpečení osobních údajů. Jednotlivé zásady jsou rozvinuty v článku 5 odst. 1 obecného nařízení. Vymezení, resp. dodržování těchto zásad, je pro správce zásadní, nejen z toho důvodu, že to jsou de facto zároveň povinnosti, ale i proto, že v článku 5 odst. 2 obecného nařízení je stanovena odpovědnost správce za jejich dodržování a zároveň povinnost správce být schopen dodržování těchto zásad (povinností) doložit. Jde o vyjádření tzv. principu odpovědnosti správce. K prokazování souladu s těmito zásadami slouží záznamy o činnostech zpracování a též kodexy a osvědčení.

Právní důvody zpracování osobních údajů

Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat. Právní důvody tak jsou nezbytným předpokladem, aby vůbec mohlo být hovořeno ze strany správce o legálním zpracování, jelikož pokud by správce nedisponoval řádným právním důvodem ke zpracování osobních údajů, bylo by dále nerozhodné, zdali plní ostatní povinnosti, jelikož by osobní údaje zpracovával nezákonně a musel by osobní údaje zlikvidovat. Je důležité vědět, že i osobní údaje může správce zpracovávat pro různé účely, přičemž pro každý účel potřebuje právní důvod zpracování osobních údajů. Zpracování osobních údajů se vždy váže k účelu, na základě kterého se určí právní důvod zpracování. Není vyloučeno, že „jed-

ny“ osobní údaje (nebo jejich určitý souhrn) bude správce zpracovávat pro různé účely, přičemž tyto účely mohou v čase vznikat či zanikat, aniž by to představovalo povinnost osobní údaje likvidovat. Povinnost likvidace osobních údajů nastane v případě, kdy správce pozbude poslední právní důvod ke zpracování osobních údajů.

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

- subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

Souhlas se zpracováním osobních údajů

Souhlas (viz článek 4 odst. 1 bod 11 obecného nařízení) je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Jde o aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen. Souhlas je jedním z právních důvodů, na základě kterého může správce osobní údaje zpracovávat. Souhlas se vždy poskytuje k určitému účelu zpracování, který musí subjekt údajů znát. Nikoli vždy odvolání souhlasu znamená povinnost správce osobní údaje zlikvidovat, jelikož odvolání souhlasu se děje k určitému účelu, pro který jsou osobní údaje zpracovávány, přičemž správce může osobní údaje zpracovávat pro jiné účely, pro které využije jiný právní důvod zpracování než souhlas subjektu údajů.

Podmínky udělení souhlasu se zpracováním osobních údajů

Aby bylo možné dosáhnout svobodnosti, konkrétnosti, informovanosti a jednoznačnosti projevu vůle subjektu údajů, stanovuje obecné nařízení v článku 7 podmínky vyjádření souhlasu. Zásadní je tzv. odlišitelnost souhlasu, což znamená, že souhlas musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje. Pro názornost, souhlas tak musí být oddělený např. od smlouvy či obchodních podmínek, resp. již není možné, aby byl jejich nedílnou součástí. Zároveň nesmí

být uzavření smlouvy (např. na službu) podmínováno poskytnutím souhlasu se zpracováním osobních údajů. Je však samozřejmé, že v závislosti na službě či výrobku bude správce muset zpracovávat (bez souhlasu) určité množství osobních údajů subjektu údajů právě pro účely plnění smlouvy či plnění zákonem stanovené povinnosti.

Je souhlas odvolatelný?

Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Je nutné si uvědomit, že souhlas byl dáván k určitým účelům a odvolání souhlasu nemusí vždy představovat pro správce povinnost osobní údaje zlikvidovat, ale bude představovat pro správce pouze povinnost přestat osobní údaje zpracovávat pro určitý účel, ke kterému byl souhlas udělen. Stejně tak i v případě, kdy správce použil souhlas pro případy, kdy mu svědčí jiný právní důvod zpracování osobních údajů, neznamená odvolání souhlasu (tedy úkonu, který nebyl nezbytný pro zpracování) povinnost osobní údaje zlikvidovat či je přestat zpracovávat, např. pokud osobní údaje musí mít pro zákonem stanovené účely.

Jak to bude se dřívějšími souhlasy za použitelnosti obecného nařízení?

Obecné nařízení v recitálu 171 předpokládá přechod souhlasu, avšak s podmínkou, že souhlas byl udělen způsobem a v sou-

ladu s podmínkami obecného nařízení. To bude pro mnoho správců problematické, jelikož jimi získávaný souhlas nebude splňovat podmínky stanovené v článku 7 obecného nařízení, například podmínku odlišitelnosti souhlasu (souhlas nesmí být neoddtělitelnou součástí obchodních podmínek) či podmínku nepodmínovat poskytnutí služby vyžadováním udělení souhlasu se zpracováním osobních údajů.

Zpracování osobních údajů zveřejněných na internetu

Osobní údaje patří subjektům údajů a ty musí v některých případech, zejména v zákonem stanovených případech, strpět jejich zveřejnění např. ve veřejném rejstříku. Osobní údaje ve veřejném rejstříku jsou zveřejněny na základě zákona, jelikož tak zákon stanoví (typicky např. živnostenský rejstřík). Skutečnost, že je stanovena veřejnost rejstříku, neznamená, že zveřejněné osobní údaje lze dále neomezeně přebírat a zpracovávat, např. jejich dalším zveřejňováním a tím na nich profitovat. Je nutné si uvědomit, že i další zveřejňování údajů z veřejných rejstříků je zpracováním osobních údajů a k tomu musí správci svědčit právní důvod, tj. zákonem předpokládané oprávnění. Další zveřejňování z veřejných rejstříků převzatých osobních údajů za použitelnosti obecného je nařízení problematické, jelikož správce bude muset využít některý z právních důvodů v článku 5 odst. 1 obecného nařízení. Obdobně je to u osobních údajů, které subjekty údajů dobrovolně zveřejňují na internetu za určitým účelem. Ani

tyto údaje, byť dobrovolně zveřejněné, nelze bez dalšího zpracovávat, jelikož i v tomto případě by správce měl absenci právního důvodu. Veřejnost údajů nikdy a priori neznamená možnost jejich dalšího bezmezného zpracovávání.

■ Kapitola 4.

Zvláštní kategorie osobních údajů (citlivé údaje)

Proč se rozlišují zvláštní kategorie osobních údajů

Některé osobní údaje jsou takového charakteru, že mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Z tohoto důvodu je taxativně (úplným výčtem) vymezena skupina údajů, které jsou považovány vůči subjektu údajů za citlivé a jimž je poskytnuta zvýšená ochrana při jejich zpracování. Zvýšená ochrana se projevuje zejména ve stanovených zvláštních právních důvodech, na základě kterých je lze zpracovávat, vázanost některých institutů na jejich zpracování, jako hlavní činnosti (např. posouzení vlivu, ustavení pověření), důraz na jejich zvýšené zabezpečení.

Jaké údaje spadají do zvláštní kategorie osobních údajů

Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za

zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. Jejich výčet je téměř totožný s výčtem citlivých údajů v zákoně č. 101/2000 Sb., o ochraně osobních údajů, až na údaj o odsouzení za trestný čin, který již nebude považován za zvláštní kategorii osobních údajů, ale podmínky pro zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů mají zvláštní režim v článku 10 obecného nařízení.

Lze zvláštní kategorie osobních údajů zpracovávat?

Zvláštní kategorie osobních údajů lze zpracovávat pouze pokud:

- subjekt údajů udělil výslovný souhlas,
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborné cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpří-

stupňovány mimo tento subjekt,

- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
 - zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
 - zpracování je nezbytné z důvodu významného veřejného zájmu,
 - zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.,
 - zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshrančními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
 - zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.
- Velmi často bude zmocnění pro zpracování zvláštní kategorie osobních údajů obsaženo v příslušném právním předpise, kterým se správce musí řídit nebo bude vyplývat z oprávněné činnosti správce.

■ Kapitola 5.

Práva subjektu údajů

Práva subjektu údajů jsou důležitým prvkem ochrany osobních údajů jako celku,

jelikož subjekt údajů je často ve slabším postavení než správce a tudíž vybalancovávají vztah mezi ním a správcem. Subjekt údajů má právo na to být informován o zpracování jeho osobních údajů. Tím se rozumí právo na určité informace o zpracování jeho osobních údajů. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. V tomto případě jde o pasivní právo, jelikož aktivitu musí vůči subjektu údajů vyvinout správce, aby požadované informace stanovené v obecném nařízení subjektu údajů poskytl, resp. zpřístupnil. Úplný výčet informací, které správce poskytuje při shromažďování osobních údajů, lze nalézt v článcích 13 a 14 obecného nařízení. Obecné nařízení formálně rozlišuje poskytování informací v případě, že osobní údaje jsou získány od subjektu údajů, resp. nejsou získány od subjektu údajů. Právo na informování je ekvivalentem práva na informace o zpracování stanoveném v § 11 zákona č. 101/2000 Sb., o ochraně osobních údajů. Mezi další práva subjektu údajů, která jsou mnohdy založena na aktivitě subjektu údajů, patří právo na přístup k osobním údajům, právo na opravu (resp. na doplnění), právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku a právo nebyť předmětem automatizovaného individuálního rozhodování, včetně profilování.

Přístup k osobním údajům

Přístupem k osobním údajům se rozumí právo subjektu údajů získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování,
 - kategorie dotčených osobních údajů,
 - příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
 - plánovaná doba, po kterou budou osobní údaje uloženy,
 - existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
 - právo podat stížnost u dozorového úřadu,
 - veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
 - skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.
- Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce. Jde o ekvivalent práva přístupu k osobním údajům, stanoveném v § 12 zákona č. 101/2000 Sb., o ochraně osobních údajů.

Nepřesné údaje

Subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají.

Neznamená to povinnost správce aktivně vyhledávat nepřesné údaje (avšak nic mu v tom ani nebrání), ani to neznamená povinnost správce např. každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že správce zpracovává jeho nepřesné údaje, upozorní jej na to. Je povinností správce, pokud mu subjekt údajů oznámí, že požaduje opravu jeho osobních údajů, zabývat se jeho žádostí.

Právo být zapomenut

Právo na výmaz (být zapomenut) představuje v obecném nařízení jinými slovy vyjádřenou povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení.

Většina vyjmenovaných případů byla součástí zákona č. 101/2000 Sb., o ochraně

osobních údajů, nebo vyplývají z jeho podstaty.

Právo na přenositelnost údajů

Právo na přenositelnost je zcela nové právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému správci, je-li to technicky proveditelné.

Společné podmínky k aplikaci práva na přenositelnost jsou tyto:

- musí jít o zpracování založené na právním důvodu souhlasu či smlouvě,
- zpracování se provádí automatizovaně. Výkonem práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob.

K právu na přenositelnost údajů byl ze strany skupiny WP29 vydán výkladový materiál dostupný zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28333.

Námítka proti zpracování osobních údajů

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na zákla-

dě právních důvodů:

- zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Do jisté míry jde o ekvivalent práva na vysvětlení dle § 21 zákona č. 101/2000 Sb., o ochraně osobních údajů. Námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud subjekt údajů vznesl námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

Právo subjektu údajů nebyť předmětem žádného rozhodnutí založeného výhradně na automatizovaném rozhodování

Toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, pokud je povoleno právem EU

nebo členským státem nebo pokud je založeno na výslovném souhlasu subjektu údajů. Nelze tak například automatizovaně pokutovat řidiče překračující rychlost, aniž by pokutu nepřezkoumal člověk. Nebo nelze automatizovaně odmítnout žádost o úvěr, aniž by žádost nepřezkoumal člověk.

Zákaz automatizovaného individuálního rozhodování byl stanoven i v § 11 odst. 6 zákona č. 101/2000 Sb., o ochraně osobních údajů.

Lhůta, do kdy musí správce reagovat na podanou žádost subjektu údajů

Pokud se jedná o žádost podle článků 15 až 22 obecného nařízení, musí být informace o přijatých opatřeních poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.

Může si správce účtovat náklady v souvislosti s výkonem nebo zneužitím práv subjektu údajů?

Zásadně platí, že informace podle článků 13 a 14 a veškerá sdělení a úkony podle článků 15 až 22 a 34 obecného nařízení se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené (zejména proto, že se opakují), může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce. Zde lze také

hovořit o zneužití výkonu práv subjektu údajů, kterým ale nelze a priori rozumět výkon práv subjektu údajů. O zneužití práva subjektem údajů jde zejména tehdy, pokud se žádosti opakují a jsou zjevně nedůvodné či nepřiměřené. V takovém případě může správce uložit přiměřený poplatek nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost v souvislosti se zneužitím opět dokládá správce.

■ Kapitola 6.

Správce, zpracovatel

Odpovědnost správce

Správce odpovídá za dodržování povinností kladených obecným nařízením. Zcela zásadní je dodržování zásad zpracování, jejichž dodržování zároveň musí být správce schopen doložit. Základním nezbytným předpokladem je existence řádného právního důvodu zpracování osobních údajů, kterým správce musí disponovat, aby vůbec mohl osobní údaje zpracovávat. Zároveň je nutné osobní údaje dostatečně zabezpečit. Samozřejmostí však musí být plnění i dalších povinností stanovených obecným nařízením.

Společní správci

Nové obecné nařízení výslovně počítá i s možností tzv. společných správců. Jde o případ, kdy účel a prostředky zpracování stanoví společně dva nebo více správců, kteří si mezi sebou transparentním ujed-

náním vymezí své podíly na odpovědnosti za plnění povinností.

Jak se různých správců dotýká obecné nařízení?

Každého správce se obecné nařízení dotýká jiným způsobem, a to v závislosti na aspektech zpracování, které provádí. Tomu musí odpovídat i přípravy správce na plnění požadavků obecného nařízení. Přístup založený na riziku váže některé povinnosti pouze na riziková či vysoce riziková zpracování, tudíž některé povinnosti mnoho správců nebude muset plnit, zatímco na jiné správce budou dopadat více méně všechny stanovené povinnosti. Každý správce by si měl udělat vlastní analýzu zpracování, které provádí, čímž zjistí, jaké eventuální povinnosti se na něj vztahují. Součástí analýzy může být i vytipování slabých míst správce, např. v zabezpečení, či provedení revize právních důvodů a jejich uvedení do souladu s podmínkami obecného nařízení (např. pokud správce využívá souhlas se zpracováním osobních údajů, provést zhodnocení, zdali udělené souhlasy budou použitelné i v době účinnosti obecného nařízení). Pokud správce řádně plnil povinnosti vyplývající ze zákona č. 101/2000 Sb., o ochraně osobních údajů, nemělo by obecné nařízení pro něj představovat výrazný problém, se kterým by si neporadil. Důležité též je nezapomenout na osvětu zaměstnanců.

Vztah správce – zpracovatel

Správce může ke zpracování osobních údajů přibrat jiný subjekt, který pro něj

bude osobní údaje zpracovávat. Správce by měl využít pouze takového zpracovatele, který s ohledem na povahu, kontext, kategorii osobních údajů a jejich možnosti, poskytuje dostatečné záruky vhodných technických a organizačních opatření, tak aby zpracování osobních údajů prostřednictvím zpracovatele splňovalo požadavky obecného nařízení a byla zajištěna ochrana práv subjektu údajů. Za tím účelem musí být mezi správcem a zpracovatelem uzavřena písemná smlouva, v níž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Smlouva dále musí zaručovat určité okolnosti zpracování – viz článek 28 odst. 3 obecného nařízení. Není nutné, aby se jednalo o samostatnou smlouvu, požadované náležitosti lze zakomponovat i do jiné smlouvy, kterou správce se zpracovatelem uzavírá v rámci například obchodního či jiného vztahu. Správce se prizváním zpracovatele nezbaňuje odpovědnosti za zpracování osobních údajů.

Může zpracovatel zapojit do zpracování jiného zpracovatele?

Jde o tzv. řetězení zpracovatelů, které není a priori zakázáno, nicméně je nutné, aby správce k tomuto dal písemné svolení zpracovateli. Svolení může být dáno k dalšímu konkrétnímu zpracovateli, nebo může být dáno obecné svolení, v takovém případě však zpracovatel musí správce informovat o veškerých přijatých dalších

zpracovatelů nebo jejich nahrazení. Účelem tak je, aby správce, který za zpracování osobních údajů primárně odpovídá, věděl, které subjekty pro něj osobní údaje zpracovávají.

■ Kapitola 7. Zabezpečení osobních údajů

Jak musí správce zabezpečit osobní údaje

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s obecným nařízením. Každý správce tak musí přijmout adekvátní bezpečnostní opatření a u každého správce takové opatření může být, právě s ohledem na povahu, rozsah a účely zpracování, odlišné. Jedním z prvků zabezpečení osobních údajů je jejich pseudonymizace nebo šifrování. Tyto prvky však nejsou povinné. Jejich dobrovolné nasazení však správci může přinést i zproštění např. povinnosti ohlásit případ porušení zabezpečení osobních údajů subjektu údajů.

Porušení zabezpečení osobních údajů

Za porušení zabezpečení osobních údajů se považuje porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Pokud dojde k po-

rušení zabezpečení osobních údajů, měl by správce zvážit, zdali nejde o okolnost, kterou je nutné ohlásit dozorovému úřadu, resp. oznámit subjektu údajů. Tyto povinnosti nastanou tehdy, pokud porušení zabezpečení představuje riziko, resp. vysoké riziko pro práva a svobody fyzických osob.

Kdy a co musí správce při bezpečnostním incidentu ohlásit Úřadu pro ochranu osobních údajů

Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu (Úřadu pro ochranu osobních údajů), ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Právě používání pseudonymizace či šifrování může případné riziko zcela eliminovat a tudíž i zbavit správce nutnosti případ ohlásit dozorovému úřadu. Vždy je však nutné míru rizika posoudit, a to i v případě, že byla použita pseudonymizace či šifrování. V oznámení správce subjektu údajů musí popsat povahu porušení zabezpečení, přijatá opatření, pravděpodobné důsledky a též musí sdělit kontaktní údaje na pověřence pro ochranu osobních údajů, byl-li ustaven. Pokud nastane porušení zabezpečení u zpracovatele, hlásí jej správci, pro kterého dotčené osobní údaje zpracovává.

Kdy a co musí správce při bezpečnostním incidentu oznámit subjektu údajů

V případě, že porušení zabezpečení představuje vysoké riziko pro práva a svobody subjektu údajů, vzniká správci povinnost zpravit o této události subjekt údajů. Správce tak nemusí činit, pokud použil předběžná opatření, která činí osobní údaje nečitelnými pro všechny neoprávněné osoby (např. šifrování nebo unikly pseudonymizované údaje bez vazby na subjekt údajů) či použil následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví. Povinnost oznámit bezpečnostní incident subjektu údajů správci nenastane ani tehdy, pokud by to vyžadovalo nepřiměřené úsilí. V takovém případě však musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení.

Určení rizika porušení zabezpečení

Při určování rizika porušení zabezpečení je nutné vycházet zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovníctví). Dalším rozhodným prvkem může být i okolnost, zdali došlo k porušení zabezpečení úmyslně či nedbalostně, přičemž úmyslný čin výrazně zvyšuje rizi-

ko takového činu, jelikož osobní údaje byly terčem útoku. Posouzení porušení zabezpečení se tak musí provést komplexně, nikoli izolovaně a vyšlé riziko následně určí eventuální povinnost oznámit porušení zabezpečení Úřadu pro ochranu osobních údajů nebo i oznámit subjektu údajů.

Musí být vždy osobní údaje u správce v šifrované nebo pseudonymizované podobě?

Šifrování ani pseudonymizace nejsou výslovnou podmínkou zpracování osobních údajů. Jsou bezpečnostním prvkem, který i v některých případech může správci zlepšit jeho postavení v případě úniků těchto údajů, jelikož v takovém případě se na něj nemusí (v závislosti na případě, neznamená to, že pokaždé) vztahovat povinnost ohlašovat případ porušení zabezpečení osobních údajů dozorovému úřadu, resp. jej oznamovat subjektu údajů. Vždy je však nutné míru rizika posoudit a to i v případě, že byla použita pseudonymizace či šifrování. Lze proto doporučit správcům, jejichž povaha zpracování osobních údajů jim to umožňuje, uchovávat (zpracovávat) údaje v šifrované či pseudonymizované podobě, k čemuž i obecné nařízení nabádá.

■ Kapitola 8.

Pověřenec pro ochranu osobních údajů

Kdo musí jmenovat pověřence pro ochranu osobních údajů
Pověřenec musí jmenovat správce a zpra-

covatel pokud:

- zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,
- hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
- hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech.

Skupina podniků může jmenovat jediného pověřence, avšak musí být pro každý podnik snadno dosažitelný.

Musí mít svého pověřence každá obec?

Vzhledem k tomu, že obec lze považovat za orgán veřejné moci, resp. veřejný subjekt ve smyslu článku 37 odst. 1 písm. a) obecného nařízení, formálně na ní dopadá povinnost jmenovat pověřence. Úřad však není toho názoru, že by každá obec musela mít svého vlastního samostatného pověřence, ale je možné, aby pro určitý počet obcí vykonával činnost pověřence např. pověřenec vyššího územně samosprávného celku či se několik obcí dohodlo a najaly si vlastního pověřence. S tímto ostatně počítá i obecné nařízení, které umožňuje pro více správců, kteří jsou orgánem veřejné moci či veřejným subjektem, jmenovat jednoho pověřence.

Musí být pověřenec organizačně podřízen přímo vedení organizace?

Pověřenec pro ochranu osobních údajů musí být přímo podřízen vrcholovým řídicím pracovníkům správce nebo zpracovatele. Nejde však o podmínku organizační, tj. že pověřence musí řídit přímo vedení organizace, ale jde o podmínku, aby pověřenec měl přímý přístup k vedení organizace, tj. aby při předávání informací vedení organizace nebyl mezi pověřencem a vedením další mezičlánek a pověřenec se tak na vedení organizace mohl kdykoli obrátit v záležitostech ochrany osobních údajů.

Úkoly pověřence pro ochranu osobních údajů

Mezi úkoly pověřence patří především poskytování informací a poradenství správci či zpracovateli, včetně zaměstnanců, kteří se na zpracování podílejí. Pověřenec dále monitoruje soulad zpracování s obecným nařízením a dalšími předpisy. Pověřenec poskytuje na vyžádání poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů. Nedílnou součástí výkonu funkce pověřence je dále spolupráce s Úřadem pro ochranu osobních údajů a působení jako kontaktní místo.

Jaké vzdělání má mít pověřenec pro ochranu osobních údajů

Obecné nařízení nestanovuje přesné požadavky na vzdělání pověřence ve smyslu akademických titulů. Pověřenec musí být osoba disponující profesními kvalitami a odbornou znalostí práva a praxe v oblasti ochrany osobních údajů a musí dostateč-