

Vážení přátelé,

dnem 25. května 2018 vstoupí v platnost Obecné nařízení EU o ochraně osobních údajů (zkráceně GDPR, podle anglického General Data Protection Regulation) na celém území EU, Islandu, Norska a Lichtenštejnska. Vzhledem k tomu, že bylo vydáno jako evropské nařízení, bude platit jednotně ve všech státech a národní vlády nemají možnost jej jakkoli upravovat. V tomto čísle našeho (Vašeho) DISu Vám proto přinášíme základní náměty pro realizaci GDPR. Závěrem tohoto DISu pak uvádíme aktuální informace k DPH.

GDPR

Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“ příp. „Nařízení“) přináší všem, kteří shromažďují nebo zpracovávají osobní údaje množství nových povinností a mnohdy až likvidační sankce za jejich nedodržení. Nezáleží na tom, zda se jedná o jednotlivce, malou firmu nebo nadnárodní společnost.

Postupně uvádíme:

- Právní norma (**A**)
- Zásady ochrany osobních údajů (**B**)
- Koncept směrnice a smlouvy se zpracovatelem (**C**)

Právní návaznosti

Berte prosím jakékoliv návaznosti na právní ujednání, například návrhy textů do obecných obchodních podmínek nebo texty do smluv jako pracovní verze, které nebyly autorizovány, resp. posouzeny právníky.

Odkazy na zdroje

Základní informace jsou k dispozici na stránkách Úřadu pro ochranu osobních údajů (dále „Úřad“), viz

<https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938>

V některých případech uvádíme odkaz na konkrétní ustanovení Nařízení, resp. příslušný článek, a to formou: (čl. xy). Naopak neuvádíme odkazy na další výklady, odborné rozborů zpracované tzv. pracovními skupinami.

A) Právní norma

Postupně se krátce seznámíme:

- s právními zdroji (**A1**),
- co je změněno (**A2**),
- kdo se novými pravidly řídí (**A3**) a
- s doplňujícími informacemi o povinnostech (**A4**).

A1) Právní zdroje

Jedná se o účinnost nové právní normy – **Nařízení** platné od 25. května 2018, které nahradí stávající tuzemský zákon č. 101/2000 Sb., o ochraně osobních

údajů a o povinnostech souvisejících se zpracováním osobních údajů („původní zákon“).

Promítá se tak realizace 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).

Poznámka

Po schválení Nařízení probíhala dvouletá lhůta, v jejímž průběhu měli správci a zpracovatelé uvést svá zpracování osobních údajů do souladu s obecným nařízením. Tato lhůta končí dnem **25. 5. 2018**.

Další zdroje

K dispozici je vedle Nařízení i jeho Preambule, která obsahuje tzv. **recitály**, což jsou výklady (resp. důvodová zpráva) k vlastnímu textu Nařízení.

V současné době probíhají v tuzemsku „dodatečně“ legislativní procesy související s prováděcími předpisy, které ale nemají měnit podstatu práv a povinností založených GDPR. Jde o tzv. **adaptační zákon** („AdZ“), který bude obsahovat drobné odchylky a zvláštní úpravy. Například v oblasti zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby se výslovně předpokládá zvláštní vnitrostátní úprava AdZ.

A2) Co se změnilo?

Podle výkladů Úřadu:

- Nemění se základní zásady zpracování osobních údajů či základní pojmy – například: osobní údaj, subjekt údajů, správce, zpracovatel či zpracování.
- Nerozšiřuje se působnost oproti současné právní úpravě.

Jedná se tedy podle Nařízení o evidenci osobních údajů, podle čl. 2 konkrétně jejich zpracování, klasifikaci jako strukturované soubory. Jde o údaje, které identifikují konkrétní znaky, vlastnosti fyzické osoby.

Doporučujeme spíše širší přístup při posuzování této problematiky, včetně navazující etapy jejich zpracování, jak je dále rozebráno: nakládání s osobními údaji různou formou, například jejich sběr, analýza, použití pro výstupy, archivace a též skartace (výmaz).

Zpracování osobních údajů

Pro některé subjekty, však klade vyšší nároky při zpracování osobních údajů:

- Typicky jde o velké správce osobních údajů typu bank, telekomunikačních operátorů, ústředních orgánů, atd., tj. pro správce, kteří zpracovávají rozsáhlé množství osobních údajů, a které je současně ze své podstaty rizikové pro práva a svobody subjektů údajů, tedy fyzických osob, o nichž jsou osobní údaje zpracovávány.

Pro malé firmy (též drobné živnostníky), které zpracovávají:

- Osobní údaje svých zákazníků pouze pro účely poskytnutí služby či výrobku, nepřináší obecné nařízení zásadní změny oproti stávající úpravě.

V takových případech je nutné zejména sledovat dodržování základních zásad zpracování.

A3) KDO se řídí Nařízením

Jedná se o následující subjekty.

Správce

Nařízení je povinen dodržovat každý subjekt, který provádí zpracování osobních údajů. Takový subjekt je nazýván správcem osobních údajů.

Zpracovatel

Dalším subjektem je zpracovatel, který pro správce osobní údaje zpracovává.

Subjekt údajů

Pokud jde o práva vyplývající z obecného nařízení, přísluší fyzické osobě, což je subjekt údajů.

Jiné úřady

Jedná se například o dozorové úřady, tj. o Úřad, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů.

Poznámka

Definice jsou popsány v čl. 4 Nařízení.

A3) CO je obsahem povinností

Předchozí text doplňujeme o přehled některých povinností se zohledněním pozice běžného podnikatelského subjektu, ať už Fyzické nebo Právnícké osoby (dále jen „SRO“).

Kritérium

Nařízení se týká zpracování osobních údajů, ať už jsou zpracovány tzv. automatizovaně nebo neautomatizovaně (čl. 2). Mimo oblast personální a mzdovou (údaje zaměstnanců) se setkáme s osobními údaji:

- zákazníků – fyzických osob, a
- obchodních partnerů.

„Běžná činnost“

Při běžné podnikatelské činnosti se více a podrobněji s „osobními údaji“ zákazníků a obchodních partnerů nepracuje, neshromažďují se.

Příklad 1)

Informace o zákaznících, ať už se jedná o fyzické osoby („FO“) nebo právnícké osoby („PO“), potřebuje SRO v minimálním rozsahu, prakticky se žádné citlivé údaje nezjišťují (viz kategorie údajů).

Přesto se setkáme například u:

- FO mimo adresy bývá k dispozici DIČ nebo rodné číslo,
- PO pouze standardně dostupné údaje v souladu s obchodním rejstříkem,
- u obou skupin telefonní a mailové spojení.

Příklad 2)

Informace o obchodních partnerech obsahují též obdobné údaje jako v předchozím příkladu s tím, že k dispozici jsou navíc např. čísla bankovních účtů.

„Jiná činnost“

Pokud by společnost SRO třeba prováděla různé marketingové akce, průzkumy trhu apod., mohla by získat skutečně citlivé osobní údaje (např. rodinné poměry aj.).

Příklad 3)

Například při zpracování dotazníků, kterým SRO zjišťuje osobní situaci svých současných nebo potencionálních zákazníků, musí být striktně dodržena ochrana takových údajů a je nutné mít souhlas respondentů.

Taková činnost může mít totiž znaky tzv. profilování, což je již vlastně analýza citlivých údajů fyzické osoby.

Konkrétní povinnosti – rekapitulace realizace

Pro běžnou činnost bude dostačující, neboť skutečně nedochází k žádným významným rozdílům ve srovnání s původním zákonem, aby SRO:

- Zpracovalo směrnici pro zajištění ochrany osobních údajů podle stanovených zásad (viz **třetí** kapitola).

Záznamy o činnostech zpracování

Ze směrnice by mělo také vyplývat, jak jsou zachyceny tzv. záznamy o činnostech zpracování (čl. 30 a násl.). V podstatě jde o zmapování:

- KDO je správcem a případně zástupcem,
- účely zpracování,
- popis dotčených subjektů,
- kategorie osobních údajů,
- KOMU mohou být údaje poskytnuty,
- archivační lhůty,
- adekvátní bezpečnostní opatření (čl. 32).

Poznámka

Obecné zásady jsou definovány v čl. 5 Nařízení. Viz následující kapitola.

B) Zásady ochrany údajů

Dále uvádíme přehled základních principů ochrany osobních údajů z pohledu SRO, které jsou základem pro návrh pracovní verze směrnice – viz kapitola **třetí**.

Rozebereme si atributy ochrany údajů (**B1**), povinnosti správce a zpracovatele (**B2**), součinnost s dotčenými subjekty (**B3**) a teorii zabezpečení osobních údajů (**B4**).

B1) Atributy pro ochranu osobních údajů

Je nutné zdůraznit povinnost doložit účel a ochranu údajů.

Účel

SRO musí definovat případy, kdy tyto údaje shromažďuje – v zásadě se jedná - mimo oblast zaměstnanců o obchodní kontrakty, ať už nákup zboží/služby a následný prodej. Nařízení považuje tuto příčinu za tzv. legitimní účel.

Zabezpečení údajů

Povinností SRO je samozřejmě osobní údaje zákazníků a obchodních partnerů zabezpečit.

B2) Povinnosti správce a zpracovatele

Správce

KDO je správcem

Obecně jde o subjekt, který zpracovává osobní údaje. Odpovídá mimo jiné za dodržení zásad jejich zpracování a oprávněnost jejich získání, musí existovat relevantní právní důvody.

Musíme zdůraznit, že v případě právnické osoby je správcem tato právnická osoba, která má odpovědnost za zpracování osobních údajů. Není jím konkrétní zaměstnanec, společník nebo jednatel. (Samozřejmě za SRO koná jednatel, prokurista atd.).

Správcem může být fyzická osoba, která zpracovává osobní údaje svých zaměstnanců a obchodních partnerů.

Existuje podle Nařízení také varianta tzv. společných správců (čl. 26).

Povinnosti správce

V této části rozebíráme povinnosti správce a následně též zpracovatele. Jedná se zejména o:

- záznamy o činnostech zpracování (**B2.1**),
- jmenování zpracovatele (**B2.2**),
- posouzení vlivu na ochranu osobních údajů (**B2.3**),
- zabezpečení údajů a práv subjektů údajů (**B2.4**).

Hlášení Úřadu

Povinností existuje více, ale některé se skutečně SRO týkat nebudou, například ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů (jde-li o závažné „rizikové“ případy) atd., je nepravděpodobné. Přesto je vhodné tuto skutečnost zakotvit do směrnice (viz třetí kapitola – povinnost zaměstnanců sdělit své připomínky).

Zpracovatel

Správce **může** (nemusí) těmito činnostmi pověřit zpracovatele, v takovém případě je nutné uzavřít **písemnou smlouvu** (čl. 28). Není zakázáno tzv. řetězení zpracovatelů – tzv. zpracovatel zpracovatele (vždy je základní právní vztah mezi správcem a zaměstnavatelem).

Lze též sjednat, že zpracovatel má svého subdodavatele – opět se souhlasem správce, ale nemusí být v pozici „dalšího“ zpracovatele, neboť plní jiné úkoly, které nesouvisí přímo se zpracováním a ochranou osobních údajů.

Vzor smlouvy

Ve smlouvě se zpracovatelem samozřejmě nesmí scházet standardní ustanovení popisující období, na které je sjednána, dohoda o mlčenlivosti atd.

U stávajících smluv na vedení účetní, mzdové a jiné agendy je rozumné zpracovat dodatek ke smlouvě. Je třeba zdůraznit, že odpovědnost za dodržování GDPR má stále správce, nelze je na zpracovatele přenést.

Příklad 4)

Doplňme si, jaké postavení mají jednotlivé subjekty například při dodavatelském zpracování mezd:

- *Správce je Klient subdodavatele, který obecně v plné míře odpovídá za GDPR.*
- *Dotčeným subjektem („subjektem údajů“) jsou fyzické osoby, zaměstnanci správce.*
- *Zpracovatelem je tato externí firma, která poskytuje záruky zabezpečení procesu GDPR podle sjednaného rozsahu.*
- *Více viz část C2.*

KDO je zpracovatelem

Stručně rekapitulujeme výše uvedený výklad, aby nedošlo k omylu, třeba záměně mezi pověřencem a zpracovatelem.

Je jím správcem pověřená osoba, která zpracovává osobní údaje pro správce, provádí tzv. zpracovatelské operace. Zpracovatelem je takový subjekt pouze ve vztahu k osobním údajům poskytnutým správcem.

Může jít také o externí firmu. Zpracovatelem není zaměstnanec správce, finanční nebo mzdový účetní, ani konkrétní útvar. Subdodavatele pro zpracovatele musí vždy odsouhlasit správce.

Povinnosti zpracovatele

Tyto povinnosti budou vycházet z realizace Nařízení, konkrétně popsanych ve Směrnici a dále též specifikovaných v našem teoretickém výkladu v části **B4**.

B2.1 Záznamy o činnostech zpracování

Správce dokládá splnění svých povinností záznamy o činnostech zpracování podle čl. 30 Nařízení.

Poznámka

Doplňme si, že postup se u SRO uvede ve Směrnici, není nutné u takových subjektů vytvářet speciální „Kodexy“ nebo získávat „Osvědčení“ od akreditovaných subjektů.

„Záznamy“ v pojetí Nařízení totiž povinně musí vést subjekty zaměstnávající více než 250 osob (pokud se nejedná o rizika pro práva a svobody subjektů údajů).

B2.2 Jmenování zpracovatele aj.

Správce jmenuje konkrétní subjekt, který bude vyřizovat agendu ochrany osobních údajů.

Pověřenec

U běžných SRO by neměla vzniknout povinnost jmenovat tzv. Pověřence (jde spíše o obce, státní organizace, apod.). Viz čl. 27.

Doplňme si, že u běžných vztahů mezi správcem a pověřencem by neměla nastat situace, že by zpracovatel měl mít statut pověřence („DPO“ – Data Protection Officer) - viz mimo jiné čl. 9. Standardní účetní nebo daňová kancelář například nemá jako hlavní činnost rozsáhlé a pravidelné monitorování zvláštních kategorií osobních údajů (uvádí se třeba „...v trestních věcech a trestních činech...“). Zjišťované citlivé údaje o zdravotním stavu nebo účasti v odborech jsou z tohoto pohledu „běžné“, protože jsou nutné pro daňové úlevy apod.

B2.3 Posouzení vlivu ochrany osobních údajů

Vedení SRO musí vyhodnotit, jestli některé zjišťované osobní údaje nejsou velmi citlivé a rizikové.

Proto u SRO by měla být dostačující forma analýzy, resp. její závěr vyjádřený ve Směrnici.

Příklad 5)

Navážeme na třetí příklad. Pro marketingové akce, resp. údaje při nich zjištěných, by měl být zaveden „zprísněný“ režim ochrany dat.

B3) Součinnost s dotčenými subjekty

Je třeba mít souhlas pro získání osobních údajů (**B3.1**) a následně je nutné zvolit vhodnou formu (**B3.2**).

B3.1 Souhlas

Nařízení je v tomto bodě poměrně striktní a vyžaduje se tzv. odlišitelnost souhlasu. To znamená, že musí být zcela zřejmý a musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje.

V Nařízení je „souhlas“ definován v čl. 4 bodu 11, musí být skutečně svobodný, jde o jednoznačný projev vůle.

Viz zamezení teoretické zaměnitelnosti v našem dalším příkladu.

B3.2 Forma souhlasu

Ve Směrnici je nutné upravit pravidla pro součinnost se zákazníky a obchodními partnery. Ideální formou je zakotvení příslušných odkazů na práva a povinnosti související s realizací Nařízení do obecných obchodních podmínek.

Příklad 6)

SRO má zpracovány obecné obchodní podmínky, které jsou k dispozici například v prodejnách jednotkách a na webových stránkách. Jakékoliv obchodní kontrakty obsahují odkaz na tyto zdroje.

Jednou ze součástí těchto podmínek je například:

- *SRO potvrzuje, že se při ochraně osobních údajů obchodních partnerů řídí platným nařízením GDPR.*
- *Obchodní partner při uzavření obchodního kontraktu souhlasí s tím, že SRO má právo na získání nezbytných osobních údajů pro zajištění kontraktu.*
- *Současně tento souhlas výslovně potvrzuje, že se jedná o agendu GDPR, aby nebyl zaměnitelný.*

Doporučujeme učinit samostatné úkony (zpracovat dodatky) a nespolehat se na dříve používané texty obchodních podmínek.

B4) Zabezpečení údajů a práv „subjektů údajů“

Pro další výklad je nezbytné doplnit si základní definice (**B4.1**) a dále si stručně vysvětlíme konkrétní formy zabezpečení osobních údajů (**B4.2**).

B4.1 Základní pojmy

Ve Směrnici se SRO odvolává na několik klíčových pojmů.

Osobní údaje

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů).

Například jde o údaje: jméno, rodné číslo, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Zpracování osobních údajů

Zpracováním je jakákoli operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů.

Formy skutečně mohou být různé, jde o shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Subjekt údajů

Subjektem údajů je fyzická osoba, již se osobní údaje týkají. Jak vyplývá z výkladu, v zásadě jsou jimi zaměstnanci správce.

Subjekt údajů není právnická osoba, přesto ji v předchozím výkladu zmiňujeme, neboť předpokládáme, že za obchodní partnery – právnické osoby – vystupují konkrétní fyzické osoby, viz následující příklad.

Příklad 7)

SRO projednává obchodní kontrakt se společností AS, za kterou jedná referent pan Nováček. E-mailová adresa pana Nováčka je osobním údajem.

Přenos údajů

Dotčené subjekty mají právo na tzv. portabilitu, tj. přenos osobních údajů ve strukturované podobě. To by neměl být problém, neboť logicky by měl být prvním úkonem požadavek zaměstnance – třeba doložení skutečností pro nárok na sociální dávky apod.

Poznámka

Doplňme si, že subjekty údajů mají mimo jiné právo na informace – výpisy o evidovaných údajích, mohou data omezovat, požadovat jejich výmaz atd. Viz čl. 17 aj.

B4.2 Zajištění osobních údajů a jejich teoretické principy

V praxi bude tato povinnost zabezpečena skutečně různou formou.

V našem případě se jedná o SRO s běžnými obchodními aktivitami, vlastní drobnou výrobou a podnikovou prodejnou. SRO má několik desítek zaměstnanců.

Principy

Stručně uvádíme některé principy požadované Nařízením:

- zákonnost, korektnost, transparentnost a pro jejich zpracování mít právní důvody,
- omezení pro konkrétní účely a jejich minimalizace,
- omezení uložení jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
- integrita a důvěrnost - technické a organizační zabezpečení osobních údajů.

Opatření

Zajištění výše uvedených principů se v praxi realizuje běžně, přesto je vhodné (nutné) postupy zakotvit do Směrnice.

Ve výkladech Úřadu se počítá s opatřeními, která stanoví rozsah a účely zpracování technická a organizační.

Zabezpečení

S nimiž souvisí odpovídající bezpečnostní opatření.

Doporučeno je zabezpečení osobních údajů formou jejich pseudonymizace nebo šifrování (což není povinné), viz čl. 32. Pseudonymizací se přitom rozumí *"zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací"*. Dodatečné informace musí být zároveň *"uchovávány odděleně"* a musí se na ně vztahovat *"technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě"*.

Externí úložiště

Pečlivě je třeba sjednávat podmínky v případech, kdy jsou využívány služby externích firem, například různá úložiště nebo zpracovatelé.

Hlášení Úřadu

Doplňme si, že když 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, nahlásit Úřadu.

To není nutné, jestliže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob (hlásí se pouze rizikové incidenty).

Sankce

V tomto dokumentu neřešíme sankce, které však mohou být astronomické.

Pro posuzování sankcí vydal Úřad „Pokyny“.

C) Koncept směrnice

Navazujeme na předchozí výklad a uvádíme koncept směrnice pro běžný subjekt, v našem pojetí SRO (C1) a námět na smlouvu mezi správcem a zpracovatelem (C2).

Směrnice obsahuje obecné principy promítnuté do praxe, ale není podle nás nutné, aby u takové společnosti byly uváděny například jednotlivé položky osobních údajů (u zaměstnanců), neboť jejich rozsah je zřejmý z obecně závazných předpisů.

C1) Aktualizace směrnice

Jedná se skutečně o vzorový návrh, který je možné aktualizovat podle konkrétních podmínek daného subjektu (správce).

Uvádíme níže několik tipů:

- Interní pravidla mohou být dostupná například též formou „Intranetu“. V takovém případě je možné se ve směrnici odvolat na tento způsob komunikace a také jako zdroj závazných informací pro zaměstnance.
 - Máme na mysli „interní“ Intranet.
 - Ve směrnici je zatím varianta: je k dispozici v písemné podobě u asistentky jednatele.
- Ideální je pro obchodní partnery mít vše zakotveno v obecných obchodních podmínkách, které budou k dispozici na externí části Intranetu (nebo webových stránkách).
- Souhlas zaměstnanců: doporučujeme v této oblasti „přísnější postup“, a to vzhledem k hysterii, která kolem zavedení GDPR panuje (a existujících sankcí).
 - Proto je uvedena varianta souhlasu „se vším“, nikoliv jen na vybrané kategorie údajů.
- Pokud by SRO mělo další činnosti, u nichž by byly osobní údaje citlivé (viz například marketingové akce), souhlas dotčených osob a zpracování by mělo být individuální.
 - V předložené směrnici není takový případ samostatně podrobně řešen.
- Některé oblasti může zajišťovat jako ucelenou subdodávku externí firma, stává se zpracovatelem (ne vždy je subdodavatel „zpracovatelem“ podle GDPR) pro vymezený sektor a je třeba spolupráci se zástupcem zmínit ve směrnici (s popisem základních pravidel).
 - Ve směrnici je krátká zmínka v části 5.

Směrnice pro zabezpečení ochrany osobních údajů

Vedení společnosti zpracovalo organizační a technické postupy pro zajištění ochrany osobních údajů v souladu s platným Nařízením účinným od 28. 5. 2018.

Obsah

1. Nařízení – cíl směrnice
2. Účel zpracování osobních údajů
3. Evidence osobních údajů
4. Přehled osobních údajů
5. Zabezpečení osobních údajů
6. Pravidla pro zaměstnance
7. Podmínky pro obchodní partnery
8. Rekapitulace povinností
9. Související interní předpisy, kontroly, součinnost a poskytování údajů
10. Účinnost směrnice, a její schválení
11. Příloha: Seznámení a podpisy

Ad 1) Nařízení – cíl směrnice

Tato směrnice upravuje podmínky pro shromažďování a ochranu osobních dat, která je obecně uložena Nařízením 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) – dále „Nařízení“.

Základní cíl

Cílem směrnice je realizace Nařízení – to znamená mimo jiné určit osobní údaje a jejich rozsah, způsob zpracování evidovaných osobních údajů, jejich ochranu a povinnosti společnosti jako správce.

Základní pravidla

Tato směrnice v jednotlivých článcích mimo jiné upravuje konkrétně obecná pravidla stanovená GDPR:

- co je účelem zpracování osobních údajů (2), jejich evidenci (3), kategorie (4), zabezpečení (5), pravidla pro zaměstnance a obchodní partnery (6 a 7), rekapitulaci povinností jednotlivých oddělení (8), archivace, okruh příjemců aj. (9).

Ad 2) Účel zpracování osobních údajů a souhlas

Osobní údaje, které získává naše společnost, jsou používány výlučně pro splnění povinné personální a mzdové agendy, včetně vazeb na sociální a zdravotní pojištění (viz část 5) a dále pro zajištění plynulé činnosti, a to pro běžný provoz a jednání s obchodními partnery (viz část 7).

Souhlas zaměstnance

Souhlas zaměstnanců se zpracováním jejich osobních údajů a rozsah těchto údajů je zajištěn písemnou formou a je doložen v personálním oddělení. Souhlas je automaticky požadován také u nových zaměstnanců, resp. je

samostatnou součástí pracovní smlouvy mezi zaměstnancem a zaměstnavatelem. Zaměstnanec má právo souhlas odvolat.

Pracovní smlouva a souhlas

Souhlas zaměstnance je zajištěn při podpisu pracovní smlouvy a je koncipován následovně:

- Potvrzuji, že jsem se seznámil se Směrnicí GDPR a souhlasím se zpracováním mých osobních údajů všech tří kategorií:
 - Běžných - například základní osobní data, která jsou nutná pro zpracování mezd, odvody sociálního a zdravotního pojištění aj.,
 - Citlivých - zdravotní stav, účast v odborech aj., potřebných např. pro uplatnění nároku na daňové výhody,
 - Specifických - rodinné poměry, informace o dětech, opět pro účely daní apod.

Stávající pracovní smlouvy

Souhlas je zajištěn dodatkem k současné pracovní smlouvě, který stávající zaměstnanec podepíše (náležitosti dodatku jsou prakticky shodné).

Informovanost zaměstnanců

Směrnice je k dispozici zaměstnancům kdykoliv k nahlédnutí v sekretariátu jednatele.

Souhlas a informovanost obchodních partnerů

Souhlas obchodních partnerů je zabezpečen výslovným a nezaměnitelným souhlasem s obecnými obchodními podmínkami, a to u každého z obchodních partnerů samostatně.

Základní pravidla jsou součástí obchodních podmínek, které jsou vždy sděleny každému partnerovi a jsou k dispozici v obchodním oddělení, na sekretariátu jednatele a v prodejně.

Ad 3) Evidence osobních údajů

Společnost zajišťuje evidenci osobních údajů podle jejich typu, resp. dotčených subjektů údajů, jak je dále specifikováno v částech 6 a 7.

Způsob evidence

Evidence osobních údajů je zpravidla zpracovávána používaným softwarovým vybavením, tj. například mzdovým modulem a účetními moduly. Přístup k jednotlivým programům je upraven v části 9 podle odpovědnosti konkrétních pracovníků a jejich pracovní náplně.

Některé osobní údaje, a to podle jejich povahy, jsou evidovány v listinné podobě a zpracovávány jednotlivými pracovišti.

Kategorie osobních údajů podle oddělení

Osobní údaje jsou obecně rozděleny do jednotlivých kategorií – viz část 4 a jsou evidovány v listinné nebo elektronické podobě podle dané povahy.

Pro účely směrnice jsou členěny do následujících oblastí v návaznosti na oddělení společnosti, které je zpracovávají (viz též část 8).

V naší společnosti se jedná o čtyři základní okruhy:

- daň z příjmů FO, sociální a zdravotní pojištění,
- daň z příjmů PO, daň z přidané hodnoty, účetnictví,
- mzdová,
- obchodní činnost a
- personální.

Ad 4) Přehled konkrétních osobních údajů

Těmito osobními údaji se rozumí pouze relevantní data týkající se zaměstnanců, které je zaměstnavatel povinen shromažďovat a archivovat, případně skartovat (tzv. výmaz) podle obecných zákonných norem (Zákoník práce aj.).

Podle Nařízení jsou tři kategorie: a) běžné, b) citlivé a c) ostatní, jak jsou zmíněny v části druhé u souhlasu zaměstnance.

Kategorie osobních údajů podle věcné náplně

Jedná se u zaměstnanců zejména o:

- mzdovou a personální agendu (rodná čísla, osobní pozice - rodinný stav, informace o manželovi, dětech aj.),
- podklady pro daň z příjmů fyzických osob, sociální a zdravotní pojištění, a to včetně údajů pro povinné testování podmínek pro poskytování benefitů (tj. též nutné informace o rodinných příslušnících, jiných rodinných poměrech apod.),
- zdroje potřebné například pro výplatu sociálních dávek (třeba zdravotní stav a jiné okolnosti),
- další potřebné podklady různých právních souvislostí (například exekuce, tj. srážky ze mzdy),
- doplňující, často podle konkrétních potřeb zaměstnanců při vyřizování jejich osobních záležitostí.

Osobní údaje a obchodní partneři

Osobními údaji rozumíme také data obchodních partnerů, která jsou nutná pro zajištění odpovídajících právních úkonů a pro zajištění údajů potřebných pro účetnictví a daně.

U obchodních partnerů právnických osob se může jednat například o osobní kontaktní údaje pracovníků těchto partnerů (zpravidla mailové adresy), pověřených k jednání s naší společností.

To znamená, že jsou evidovány osobní údaje – vždy s výše uvedeným souhlasem - například:

- fyzických osob - zákazníků a odběratelů, DIČ a rodná čísla, adresy, bankovní spojení,

- právnických osob - obdobně jako u fyzických osob, neboť vystupují jménem obchodního partnera.

Ad 5) Zabezpečení osobních údajů – bezpečnostní opatření

Jedná se o popis základních procesů, v některých bodech navazujících na směrnici oběh účetních a daňových dokladů, kterou tato směrnice v některých bodech rozšiřuje.

Průběžné zálohy dat

Oddělení IT zajišťuje pravidelné denní archivace dat, tj. osobních údajů, uložených v jednotlivých programech.

Podklady v listinné podobě jsou ukládány v pořadačích v jednotlivých odděleních.

Oprávnění osob

Přístup k jednotlivým údajům je selektivní a je dán pracovní pozicí toho kterého zaměstnance, který plní své pracovní povinnosti v souladu s pracovní smlouvou. Viz jednotlivé okruhy uvedené v části třetí.

Archivace a skartace

Průběžně probíhá archivace osobních údajů, a to v návaznosti na archivační lhůty stanovené pro jednotlivé typy (například daň z přidané hodnoty, daň z příjmů, mzdové, resp. personální).

Data uložená v elektronické podobě jsou zálohována také na externích nosičích, zpravidla po uzavření konkrétního účetního období. Jsou uložena v sekretariátu jednatele.

Podklady v listinné podobě jsou ukládány do samostatné místnosti určené pro archivování dokladů.

Externí spolupráce

Společnost může v konkrétních případech použít externí spolupracovníky, například subdodávku v oblasti daňové, zpracování účetnictví, mezd, IT aj.

V takových situacích musí být součástí uzavřené písemné smlouvy ustanovení, že dodavatel (stává se zpracovatelem pro vybranou oblast, pokud bude souviset se zpracováním a ochranou osobních údajů) je povinen se řídit pravidly společnosti pro oblast GDPR.

Ad 6) Pravidla pro zaměstnance

Každý zaměstnanec společnosti při podpisu pracovní smlouvy samostatně potvrzuje, že souhlasí s evidováním svých osobních údajů v rozsahu potřebném pro splnění zákonných povinností zaměstnavatelem.

Citlivé a další údaje

Osobní údaje se mohou týkat například též rodinných příslušníků, třeba pro doložení nároků na slevy na dani a jiné benefity, které jsou podmíněny pravidly zákona o daních z příjmů, jak je popsáno v části 4.

Jiné údaje

Na druhé straně je možné, aby zaměstnanec poskytl zaměstnavateli dobrovolně další osobní údaje, které mohou mít i povahu citlivých dat.

Může se jednat o doložení některých skutečností (sociální dávky, bankovní úvěry aj.).

Předávání údajů třetí straně

V těchto případech je zaměstnavatel podle pokynu zaměstnance oprávněn poskytnout příslušné osobní údaje třetí straně.

Není požadován samostatný výslovný souhlas pro poskytování údaje státním orgánům, například finančnímu úřadu, pojišťovnám atd.

Jiné použití údajů

Pouze s výslovným souhlasem konkrétního zaměstnance je možné použít jeho osobní údaje pro účely podnikových reklamních akcí, například pro různé marketingové akce.

Zaměstnavatel v těchto případech postupuje při ochraně těchto dalších osobních údajů podle principů stanovených obecně GDPR a dále zásad specifikovaných směrnicí v části osmé.

Ad 7) Podmínky pro obchodní partnery

Obchodní partneři vyslovili souhlas se získáním jejich osobních údajů písemným odsouhlasením obchodních podmínek. V této oblasti se jedná o osobní údaje nikoliv právnických osob, ale například fyzických osob zastupujících právnické osoby, podnikající fyzické osoby, dále klienty, kteří vystupují jako fyzické osoby (jak je rozebráno v části čtvrté).

Způsob informování klientů

Vzhledem k tomu, že se jedná o data potřebná pro účetnictví a daně podle obecných předpisů, za takový souhlas je považováno i přijetí mailové zprávy obsahující obchodní podmínky a následná realizace obchodního případu.

Dále jsou obecné podmínky k dispozici na každé prodejní jednotce s tím, že u tohoto typu obchodního kontraktu se shromažďují pouze údaje standardní, které jsou nutné pro účetnictví a daně v souladu s příslušnými předpisy.

V těchto konkrétních případech není vyžadován samostatný souhlas obchodního partnera – jedná se například o odběr zboží přímo v podnikové prodejně za hotové apod., neboť se jedná pouze o údaje potřebné pro daňové a účetní účely, případně elektronickou evidenci tržeb.

Ad 8) Rekapitulace povinností

Pro naplnění povinností společnosti jsou stanoveny následující práva a povinnosti (dále kompetence) jednotlivých zaměstnanců společnosti a také jednatele společnosti.

Nejedná se však o určení tzv. zástupce podle Nařízení, ale jde o dodržení organizačních a technických postupů souvisejících s ochranou osobních údajů.

Proto je členěno podle typu osobních údajů a základních souvisejících povinností.

Oblast	Zpracování a ochrana dat	Odpovědná osoba
--------	--------------------------	-----------------

Archivace dat	Pravidelná archivace	Vedení IT, jednatel
Obchodní činnost	Údaje o partnerech, kontakty	Obchodní referenti
Podniková prodejna	Údaje o zákaznících	Pracovníci prodejny
Skartace	Navazuje na archivaci, ale může se jednat o jiné (obchodní) údaje apod.	Jednatel
Směrnice - schválení	Obsah a aktualizace	Jednatel
Účtárna	Běžná provozní účetní a daňová agenda	Pracovníci Finančního (účetního) oddělení
Zabezpečení dat	Průběžná archivace, antivir aj.	Pracovníci IT oddělení
Zaměstnanci - personální	Pracovní smlouvy apod.	Jednatel, Asistentka
Zaměstnanci – mzdy	Zpracování osobních údajů	Pracovníci Mzdového oddělení
Zpracovatel	Smlouva se subdodavatelem	Jednatel

Směrnice bude aktualizována případně podle nových skutečností a seznam odpovědných osob může být upraven.

Ad 9) Související interní předpisy a kontroly, součinnost zaměstnanců, poskytování údajů

Tato směrnice navazuje na další interní předpisy společnosti, například na Organizační řád, Oběh účetních a daňových dokladů, obsahující také Archivační řád a jiné provozní interní normy.

Kontrola realizace této směrnice je uložena jednatelem s tím, že probíhá průběžně – vždy k 31. 1. za předchozí kalendářní rok.

V roce 2018, a to v součinnosti s vedoucím mzdového oddělení, obchodního oddělení a IT oddělení bude provedena kontrola plnění povinností podle článku osm nejpozději do 30. 6. 2018.

Zaměstnancům se ukládá povinnost neprodleně písemně informovat vedení společnosti, pokud se vyskytne podle jejich názoru jakýkoli problém s ochranou osobních údajů.

Osobní údaje mohou být poskytnuty pouze příslušným orgánům, například finančním úřadům, pojišťovnám a ve specifických případech bankovním ústavům apod.

V souladu s obecnými právními povinnostmi shromažďuje účetní a daňové oddělení v této oblasti standardně dostupné údaje. To platí také pro mzdové oddělení. Tyto útvary předávají povinně určené osobní údaje státním orgánům.

Shromažďování případných dalších údajů o obchodních partnerech je v gesci obchodního oddělení, které také může mít obdobnou oznamovací povinnost.

Ad 10) Účinnost směrnice a schválení

Směrnice nabývá účinnosti podpisem jednatele a k datu 28. 5. 2018.

V, dne

Jednatel společnosti

C2) Námět na smlouvu mezi správcem a zpracovatelem

Uvádíme dále konkrétní námět, co by mohla obsahovat smlouva se zpracovatelem.

Jako vzor si zvolíme účetní firmu, která pro správce zajišťuje daně a účetnictví, příp. mzdovou agendu.

Koncept

Ve smlouvě je třeba přesně definovat rozsah osobních údajů a základní povinnosti zpracovatele ve vztahu ke GDPR.

Smlouva by měla obsahovat mimo jiné:

- Potvrzení správce, že je oprávněn konkrétní osobní údaje shromažďovat (tzv. oprávněný zájem).
- Jasné pověření, tj. zadání pro zpracovatele: a) získání dat a b) jejich zpracování.
- Popis povinností zpracovatele konkretizovat podle typu zakázky: uvést okruh osobních údajů – třeba přehled údajů pro zpracování mezd nebo účetnictví/daní (v zásadě stačí odkazy na právní normy určující, která data jsou nezbytná).
- Způsob zpracování dat u zpracovatele a jak budou zabezpečena. Někdy „subdodavatel“ také data pro správce bude též archivovat a skartovat.
- Dále se musí sjednat, jak bude probíhat komunikace (vč. předání podkladů a následně výstupů, v jaké formě) mezi správcem a zpracovatelem, určení kontaktních osob. Jinými slovy, jen vybrané osoby mohou nahlížet do dat (jde o problém obecně řešený jako zveřejnění osobních údajů).
- Sjednat se musí ukládání dat, neboť například u účetních nebo daňových kanceláří se vyskytuje používání různých externích úložišť.
- Další náměty lze odvodit z konceptu Směrnice.

Ad 11) Příloha

V příloze jsou uvedeny odpovědné osoby podle článku 8, které současně potvrzují, že se s obsahem směrnice seznámily a jejich povinnosti jsou jim srozumitelné.

Pracovník	Funkce	Datum	Podpis

Autor: Ing. Jan Ambrož, auditor a daňový poradce

Aktuálně k DPH

Kontrolní hlášení, Sdružení a Zálohy

V praxi se v poslední době setkáváme nejvíce se třemi problémy, které jsou zmíněny v názvu článku. Jedná se o možnost nepodání kontrolního hlášení – především u plátců daně z přidané hodnoty Fyzických osob (1. kapitola).

Mnoho plátců si dále neví rady s novelou zákona o DPH, která je účinná od **1. 7. 2017**, a to jak vlastně funguje sdružení bez právní subjektivity (2.) a hledá se odpověď na otázku, jestli nyní patří inkasované zálohy do daně z přidané hodnoty (3.).

Ad 1) Kontrolní hlášení

Jako první problém, který ve skutečnosti není žádným daňovým oříškem, je situace, zda plátce DPH, je-li jím fyzická osoba se čtvrtletním zdaňovacím obdobím:

- Opravdu nemusí podávat kontrolní hlášení za každý kalendářní měsíc (na rozdíl od právnické osoby)?
- **Ano**, je tomu tak, ale další výjimka platí pro Fyzické i Právnické osoby!

Nulové kontrolní hlášení

Navazující téma je trochu komplikovanější. Je totiž pravdou, že jakýkoliv plátce DPH je:

- povinen podat „prázdné“ daňové přiznání, přestože žádné plnění neuskutečnil, jak stanoví § 101 ZDPH, resp. „...*mu nevznikla povinnost přiznat daň*“.
- ale u kontrolního hlášení je tato povinnost odvozena od přijetí nebo uskutečnění konkrétních plnění podle § 101c zákona o DPH: „...*je povinen podat kontrolní hlášení, pokud*...“.

Fyzická osoba

To znamená, že např. každý plátce DPH, jde-li o fyzickou osobu se čtvrtletním zdaňovacím obdobím, musí do **25. 4. 2018** odevzdat daňové přiznání k DPH za první čtvrtletí roku 2018, třeba i „nulové“.

Příklad 1.

Pan Nováček je čtvrtletním plátcem DPH, ale „podniká“ hlavně v letní sezóně, neboť provozuje kemp ve známé rekreační oblasti. Za období leden až březen 2018 neeviduje žádné vstupy a ani výstupy. Daňové přiznání za první čtvrtletí 2018 musí podat, kontrolní hlášení nikoliv.

Výzvy správy daní

Na zaslouženou dovolenou do teplých krajů si raději pan Nováček bere notebook. Musí totiž na případnou výzvu, proč nepodal „nulové“ kontrolní hlášení, včas reagovat. Zvolí variantu „*rychlá odpověď*“, kterou potvrzuje, že (ne)činil nic.

Důkazní břemeno je samozřejmě na daňovém subjektu – je nutné, aby v záznamní evidenci (podle zákona o DPH, § 100, „Evidence pro účely daně

z přidané hodnoty“) skutečně nebyly zaznamenány žádné údaje v předmětném období, které by zakládaly povinnost podat kontrolní hlášení.

Právnícká osoba

Aby nedošlo k omylu, varianta „nulového“ kontrolního hlášení není omezena jen na plátce fyzické osoby.

Příklad 2.

Čtvrtletní plátce DPH, firma STÁNEK s.r.o. má obecné povinnosti:

- *za leden a únor podat kontrolní hlášení, a*
- *v dubnu za první čtvrtletí daňové přiznání a kontrolní hlášení za březen.*

Tato firma shodou okolností podniká ve stejném oboru jako pan Nováček. Jestliže nemá žádné položky v záznamní evidenci za první čtvrtletí, postupuje shodně a žádná kontrolní hlášení za leden, únor a březen nejsou podána. Daňové přiznání za první čtvrtletí je odevzdáno „prázdné“.

Ad 2) Sdružení

Zásadní novinkou je změna přístupu zákona o dani z přidané hodnoty ke sdružení bez právní subjektivity, přesně „společnosti“ a jejím „společníkům“ (dříve účastníkům sdružení).

Nový vs. starý model

Podle novely zákona o DPH musí pro účely daně z přidané hodnoty jednat každý společník „**sám za sebe**“. Jinými slovy jako kdyby ani společnost neexistovala, proto také byla drtivá většina specifických ustanovení zákona o DPH, dosud věnovaná společnosti, zrušena. Tento **nový** model musí povinně aplikovat každá společnost, jestliže vznikla po **30. 6. 2017**!

Starý model, podle kterého za společnost jedná pověřený společník, je podle přechodných ustanovení zákona o DPH možný, ale jen do konce letošního roku, od **1. 1. 2019** běží pouze nový model.

Častá nedorozumění se týkají především fyzických osob, pro které je forma podnikání „společnost“ zajímavá zejména u daně z příjmů fyzických osob. Nesprávně se domnívají, že od loňského července je „vše jinak...“. Pravdou je, že mohou používat zavedený starý model – nesmí však učinit právní úkon, kterým by správci daně sdělili, že přecházejí na **nový** model.

Příklad 3.

Kadeřnice, paní Bílá a Černá, podnikají ve společnosti již několik let, Obě jsou plátcí DPH a evidenci a další povinnosti za společnost zajišťuje paní Bílá, neboť její manžel je zdatným účetním...

Tímto způsobem mohou dámy fungovat bez problémů do konce letošního roku, jestliže se dobrovolně nerozhodnou změnit systém. Toto právo volby nemá nová společnost.

Příklad 4.

Pan Bílý se domluvil s daňovým poradcem panem Modrým a založili společnost dne 1. 7. 2017. Musí postupovat podle nového modelu – „každý sám za sebe“ plní povinnosti k dani z přidané hodnoty.

Plátce plus Neplátce?

Proto také s účinností od 1. července 2017, neboť jde o dva „nezávislé“ daňové subjekty, může existovat společnost, v níž je společníkem plátce DPH (třeba pan Modrý) a neplátce (pan Bílý). V takovém případě je pan Bílý v pozici osoby povinné k dani a samozřejmě si musí kontrolovat výši obrátu, jestli mu nevznikla povinnost registrace k DPH (nikoliv však z důvodu vzniku společnosti, jak tomu bylo do 30. 6. 2017).

Názor daňové správy

Doplňujeme, že jsme Vás již na stránkách našeho DISu informovali o „výkladu“ daňové správy k této problematice, konkrétně v čísle **11/2017**.

Ad 3) Zálohy

Do 30. června 2017 byla každá inkasovaná záloha („přijatá úplata“) podkladem pro povinnost přiznat daň (na výstupu), pokud se jednalo o zálohu na budoucí zdanitelné plnění (s výjimkou plnění v režimu přenesení daňové povinnosti na příjemce plnění). Novela zákona o DPH (nové ustanovení § 20a) nám všem zamotalo hlavu, neboť původní železné pravidlo zrezivělo.

ANO nebo NE?

Podle novely patří záloha do DPH, jen je-li „...*zdanitelné plnění ke dni přijetí úplaty dostatečně určité*...“. Je proto na každém plátcu, aby důkladně zvážil, jestli přijatou zálohu zdanit či nikoliv.

Příklad 5.

Firma NÁKUP s.r.o. přijala dvě zálohy od svých obchodních partnerů. První byla na dodávku 20 ks televizorů, druhá nespecifikovaná – na plánovaný odběr zboží ve druhém čtvrtletí. Asi je možné druhou zálohu vyřadit z režimu DPH.

V praxi se většina plátců, aby se vyhnula jakýmkoliv problémům, tváří jako kdyby žádný nový paragraf 20a neexistoval. Je to rozumné, ale přeci jen je riziko na straně poskytovatele zálohy, protože může být teoreticky zpochybněn jeho nárok na odpočet DPH.

Názor daňové správy

Také pro tuto novinu připravila daňová správa svůj výklad, na který jsme Vás již upozornili v našem DISu číslo **7-8/2017**.

Autor: Ing. Jan Ambrož, auditor a daňový poradce