

GDPR a ochrana osobních údajů v praxi

Sborník vzorů a návodů
pro mzdové účetní a personalisty

Autoři:

JUDr. Věra Bognárová, Mgr. et Mgr. Radana Burešová,
Mgr. David Burian, Mgr. Matěj Daněk, Mgr. Vanda Foldová,
Ing. Růžena Klímová, Mgr. Zuzana Dubská, CIPP/E,
JUDr. Dušan Srp, Ph.D., Mgr. Jaroslav Šuchman, LL.M,
Mgr. Jan Vácha

Redakční uzávěrka: 10. 7. 2019

VERLAG
DASHÖFER

Obsah

GDPR z pohledu právního a personálního.	7
GDPR rok poté – nová legislativa, zkušenosti a další vývoj v oblasti ochrany osobních údajů	9
Zákon o zpracování osobních údajů	12
Seznamte se s Nařízením ePrivacy	17
Platí nadále stanoviska a doporučení pracovní skupiny WP 29?.	21
GDPR a práva subjektu údajů	23
Zástupce subjektu údajů	29
Pověřenec pro ochranu osobních údajů	31
Plnění požadavků zákonnosti zpracování a jak přistupovat k souhlasům se zpracováním osobních údajů	37
Dopad GDPR do pracovněprávních vztahů	43
Monitoring služebních vozidel pomocí technologie GPS	51
Ohlašování případů porušení zabezpečení osobních údajů	59
Poznatky z kontrolní a dozorové činnosti Úřadu pro ochranu osobních údajů	63
GDPR z pohledu mzdového účetnictví	73
Povinnosti a práva zaměstnavatele jako správce osobních údajů	75
Práva zaměstnanců jako subjektů údajů	78
Souhlas se zpracováním osobních údajů osoby ucházející se o zaměstnání zařazené do databáze potenciálních zaměstnanců	82
Souhlas se zpracováním osobních údajů zaměstnance	85
Nejdůležitější osobní údaje zaměstnanců, které zaměstnavatel zpracovává	89
Záznamy o zpracování osobních údajů zaměstnanců dle GDPR.	98
Kamerový systém.	111
Checklist na zpracování osobních údajů zaměstnanců	113
Osobní spis zaměstnance.	115
Evidence, uchovávání a vyřazování dokumentů ve mzdové a personální oblasti.	119
Vzory vnitřních firemních předpisů	129
Vnitřní předpis zaměstnavatele upravující postup při výběrovém řízení	129
Vnitřní předpis zaměstnavatele o základních právech a povinnostech vyplývajících z pracovního poměru, o zpracování osobních údajů a o souhlasu se zpracováním osobních údajů	137
Vnitřní předpis zaměstnavatele k ochraně osobních údajů	145
Vnitřní předpis zaměstnavatele o provozování kamerového systému.	153

Vnitřní předpis zaměstnavatele o využívání výpočetní techniky a mobilních telefonů.	159
Organizační řád.	164
Spisový řád.	177
Vzory pracovněprávních písemností	184
Profesní životopis – komentář.	184
Souhlas zaměstnance se zpracováním osobních údajů.	188
Sdělení o nepřijetí uchazeče do zaměstnání.	198
Sdělení o přijetí uchazeče do zaměstnání	203
Smlouva o budoucí pracovní smlouvě	209
Pracovní smlouva.	213
Pracovní smlouva pro vedoucí zaměstnance	219
Pracovní smlouva zakládající pracovní poměr na dobu určitou.	222
Dohoda o provedení práce.	225
Dohoda o pracovní činnosti	229
Záznam o instruktáži zpracování osobních údajů zaměstnance	232
Informační povinnost zaměstnavatele	234
Žádost zaměstnance o nahlédnutí do osobního spisu	237
Vyřízení žádosti o přístup k osobním údajům, nedochází-li k jejich uchování	240
Monitorování elektronické komunikace zaměstnanců zaměstnavatelem.	241
Dohoda o úhradě členských příspěvků členů odborové organizace.	245
Smlouva o zpracování osobních údajů dle GDPR s účetní firmou	249
Ohlášení porušení zabezpečení osobních údajů Úřadu.	257
Protokol o likvidaci osobních údajů	258
Dotazy a odpovědi.	259
Uchovávání osobních údajů bývalých zaměstnanců.	261
Předávání osobních údajů o zaměstnancích pojišťovně z důvodu uzavření cestovního pojištění	262
Softwarová firma jako zpracovatel osobních údajů zaměstnanců	263
Informace o kamerovém systému v pracovní smlouvě	264
Kamerový záznam jako důvod pro výpověď z pracovního poměru	265
Plná moc a souhlas se zpracováním osobních údajů klienta.	267
Osobní údaje zaměstnanců právnických osob	269
Příspěvek zaměstnancům na životní a penzijní spoření.	270
Údaje o zaměstnancích zobrazené viditelně pro všechny	271
Zpracovatelská smlouva s poskytovatelem pracovnělékařských služeb	272
Údaje pro provádění nemocenského a důchodového pojištění	275

Poznatky z kontrolní a dozorové činnosti Úřadu pro ochranu osobních údajů

Mgr. Vanda Foldová

Na základě veřejně dostupných informací lze vysledovat několik tendencí, které se projevují v činnosti Úřadu pro ochranu osobních údajů (dále jen „Úřad“) jako dozorového orgánu pro oblast GDPR, se kterými by měl každý podnikatel počítat. Jedná se přitom nejen o to, jakým způsobem vyhodnocuje určité problémy v oblasti ochrany osobních údajů, ale též o to, jakým způsobem bude k podnikateli přistupovat v případech, že má podezření, že u něj dochází k porušování pravidel, které GDPR stanoví. Není přitom rozhodující, jakým způsobem se Úřad o podezření dozví; zda jde o informaci z veřejných zdrojů nebo jedná na základě stížnosti dotčeného subjektu údajů. Přesto je na tomto místě vhodné uvést, že závažnější je pro podnikatele zpravidla situace, kdy se jedná o stížnost dotčené osoby. Taková osoba má totiž nejen právo si stěžovat u Úřadu jako u dozorového orgánu, ale může se též obrátit přímo na soud (viz čl. 79 GDPR).

Tato skutečnost, spolu s tím, že GDPR klade zvýšený důraz na práva subjektu údajů, vede k závěru, že podnik musí být vždy připraven řešit žádosti a jiná podání těchto osob, aby se vyhnul případným následným problémům. Aby mohl takové žádosti řešit efektivně, je nezbytné nastavit vnitřní postupy tak, aby bylo každému zodpovědnému zaměstnanci zřejmé, jakým způsobem má žádost vyřídit, případně na koho se může obrátit, pokud si není jistý, jaký je správný postup. Procesy v rámci organizace musí být na standardní řešení i potenciální problémy nastaveny a zaměstnanci s nimi musí být nutně (a prokazatelně) seznámeni. Pokud by tomu tak bylo u všech podnikatelů, zřejmě by se neobjevovaly případy, které budou zmíněny níže a které Úřad v rámci své činnosti řešil a případně postihoval.

Postup Úřadu při podezření z porušení pravidel ochrany osobních údajů

Začněme tedy u toho, jakým způsobem Úřad v případě podezření z porušení pravidel ochrany osobních údajů zpravidla postupuje. Jak je zřejmé z dostupných informací¹³, volí v případech, které zjevně nevykazují prvky závažného porušení, **nejprve kontakt se správcem**. Ten je upozorněn na své povinnosti, na to, v čem spočívá podezření z porušení GDPR, a případně je mu stanovena i lhůta k neprodlené nápravě. Teprve poté, co podnikatel v rámci tohoto postupu stav nenapraví, Úřad mu uloží sankci. Přestože sankce nejsou nijak vysoké, je zjevné, že je pro podnikatele (nejen) ekonomicky mnohem výhod-

¹³ Příkaz čj. UOOU-08244/18-15 ze dne 10. ledna 2019; viz www.uoou.cz, sekce Povinně zveřejňované informace.

Záznamy o zpracování osobních údajů zaměstnanců dle GDPR

Ing. Růžena Klímová

Záznamy o činnostech zpracování jsou záznamy, které jsou níže specifikovaní správci osobních údajů povinni vést o jejich zpracování a na žádost je zpřístupnit dozorovému orgánu, kterým je Úřad pro ochranu osobních údajů.

Vést záznamy o činnostech zpracování **se netýká správců zaměstnávajících 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.

GDPR vymezuje, jaké **konkrétní** údaje musí být součástí takové dokumentace o zpracování osobních údajů. Jsou to jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů.

Jsou-li osobní údaje zpracovávány zpracovatelem, je možné tuto povinnost přenést na zpracovatele. GDPR uvádí výjimky, kdy není správce povinen vést dokumentaci o zpracování (správce s méně než 250 osobami). Ovšem i menší organizace mohou zpracovávat velký objem dat a provádět vysoce rizikové zpracování, při kterém hrozí únik či zneužití osobních údajů. Výjimka je tudíž omezena jen na taková zpracování, která není možné považovat za riziková a závažným způsobem nezasáhnou do práv a svobod jednotlivců. V případě, že zpracování je možné považovat za rizikové a současně se jedná o správce s méně než 250 osobami, a zpracování není výjimečné, je nutné záznamy o zpracování vést.

Kamerový systém, který je aplikován z důvodu ochrany majetku zaměstnavatele a předmětů a věcí zaměstnanců, které se obvykle do zaměstnání nosí, a dále z důvodu ochrany a bezpečnosti zdraví zaměstnanců, představuje určité riziko pro práva a svobody fyzických osob. Navíc se jedná o zpracování osobních údajů, které není příležitostné, ale permanentní. Z uvedených důvodů bude nutné, aby provozovatel kamerového systému vedl vždy záznamy o činnosti zpracování **bez ohledu na počet osob**.

Záznamy o zpracování osobních údajů v oblasti mzdové a personální oblasti, jedná-li se o správce s alespoň 250 osobami, jsme diferencovali podle druhu a povahy osobních údajů.

Je-li správce osobních údajů povinen jmenovat pověřence, je vhodné tuto skutečnost uvést v záznamu o zpracování pouze v obecné rovině, neboť s ohledem na možné budoucí změny v osobě pověřence by bylo vždy nutné záznamy aktualizovat.

Záznam o zpracování osobních údajů týkajících se srážek ze mzdy dle § 146 ZP a souvisejících právních předpisů

Správce osobních údajů	Etona, s. r. o., Kolmá 555, 110 00 Praha 1 IČ: 89555551 Kontaktní osoba: <i>Je-li správce povinen jmenovat pověřence, je vhodné tuto skutečnost v záznamu uvést pouze obecně s ohledem na případné změny v osobě pověřence.</i>
Účel zpracování	Provádění srážek ze mzdy na základě exekučních titulů, usnesení insolvenčních soudů, dohod o srážkách ze mzdy, žádosti člena odborové organizace týkající se srážky členského příspěvku
Právní důvod	Plnění právní povinnosti dle zákonů č. 99/1993 Sb., č. 182/2006 Sb., § 144a až 150 zákona č. 262/2006 Sb., § 2045 až 2047 zákona č. 89/2012 Sb. a oprávněných zájmů správce v případě dohody o srážkách ze mzdy
Popis kategorií subjektu údajů	Zaměstnanci
Popis kategorie osobních údajů	Pořadí závazku, výše závazku, druh závazku zaměstnance, zůstatek závazku, počet vyživovaných osob
Informace poskytované subjektům údajů	Výše provedených srážek se uvádí na výplatním lístku. Ostatní údaje jsou k dispozici ve mzdové účtárně. Jedná se o pořadí srážek, výše splacených závazků atd.
Příjemci osobních údajů	Orgán, který vydal exekuční titul, insolvenční správce, okresní správa sociálního zabezpečení, souběžný plátce na základě žádosti, následující plátce (viz povinné náležitosti zápočtového listu).
Lhůta pro výmaz osobních údajů	Doba uchování údajů o srážkách ze mzdy se řídí § 150 ZP – 30 let po roce, kterého se záznam týká.
Organizační opatření	Osobní údaje týkající se srážek ze mzdy jsou zavedeny v softwaru pro zpracování mezd, doklady obsahující tyto osobní údaje jsou uloženy ve mzdové účtárně.
Pověřenec pro ochranu osobních údajů	Správce není/je povinen mít pověřence. Správce jmenoval pověřence a jeho kontaktní údaje jsou zveřejněny samostatným dokumentem: „Pověřenec pro ochranu osobních údajů“.

Vnitřní předpis zaměstnavatele k ochraně osobních údajů

JUDr. Věra Bognárová, na GDPR vzor adaptoval JUDr. Jaroslav Šuchman, LL.M, advokát HAVEL & PARTNERS

Pravidla zaměstnavatele k ochraně osobních údajů

Zaměstnavatel (uvést jeho přesné označení, sídlo, IČO)
zastoupený

V zájmu zajištění ochrany osobních údajů zaměstnanců, jakožto subjektů údajů, vydávám v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon“) a 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) („nařízení“) a po projednání s odborovou organizací tato pravidla:

1. Tato pravidla se vztahují na všechny zaměstnance (název společnosti, podniku, družstva apod. – „zaměstnavatel“) v pracovněprávním vztahu a, jde-li o management zaměstnavatele, též ve vztahu smluvním.
2. Všichni zaměstnanci, na něž se vztahují tato pravidla (bod 1), jsou povinni dodržovat při shromažďování, evidenci a zpracování osobních údajů ustanovení zákona a nařízení, které též stanoví, co se těmito údaji a nakládáním s nimi rozumí (čl. 4 nařízení). Stejně tak jsou povinni se řídit příslušnými ustanoveními zákoníku práce upravujícími tuto problematiku (zejména § 312 ZP a § 316 odst. 4 ZP).
3. Všechny osoby, které zpracovávají osobní údaje pro zaměstnavatele, jakož i další osoby, které přijdou do styku s osobními údaji u zaměstnavatele nebo zpracovatele, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních přijatých zaměstnavatelem. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo poměru obdobného.

Uchovávání osobních údajů bývalých zaměstnanců

Mgr. et Mgr. Radana Burešová

Dotaz:

Disponujeme osobními údaji bývalých pracovníků (důchodců), kterým posíláme přání k výročí a zveme je na různé akce. Jak máme ošetřit uchovávání těchto údajů?

Odpověď:

Zasílání blahopřání apod. je v praxi Úřadu pro ochranu osobních údajů považováno za obchodní sdělení, protože se jedná o „sdělení na podporu image“ [srov. definici obchodních sdělení v § 2 písm. f) zákona č. 480/2004 Sb., o některých službách informační společnosti]. Totéž lze soudit i v případě pozvánek na firemní akce.

Podle bodu 47 odůvodnění GDPR lze zpracování osobních údajů za účelem přímého marketingu považovat za zpracování prováděné z důvodu oprávněného zájmu, tj. vztahuje se na něj účel zpracování uvedený v čl. 6 odst. 1 písm. f) GDPR a v zásadě k němu není třeba souhlasu dotčené osoby, ovšem s jednou zásadní výjimkou, která vyplývá právě ze zákona č. 480/2004 Sb.

Podle § 7 odst. 2 tohoto zákona lze obchodní sdělení, na která se nevztahuje výjimka uvedená v § 7 odst. 3, šířit elektronickými prostředky pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas ve smyslu GDPR. Elektronickými prostředky se rozumí především e-mail a telefon [§ 2 písm. c) zákona č. 480/2004 Sb.].

Upozornění: Pokud tedy přání a pozvánky zasíláte klasickou poštou, není třeba souhlasu adresátů. Pokud je však rozesíláte e-mailem, potřebujete souhlas se zpracováním osobních údajů, nikoli však kvůli GDPR, ale kvůli zákonu č. 480/2004 Sb.

V každém případě však nesmíte zpracovávat více (druhů) osobních údajů, než kolik je nezbytné.