Nařízení GDPR a zaměstnavatelé

9. říjen 2017

Do účinnosti nového nařízení Evropské unie upravujícího oblast ochrany osobních údajů[1] dne 25. května 2018 ještě stále zbývá několik měsíců. Správci a zpracovatelé tak stále mají prostor přizpůsobovat své postupy a prostředky zpracování osobních údajů nové právní úpravě. Záměrem tohoto článku je proto shrnout základní změny, které nařízení GDPR do oblasti zpracování osobních údajů přináší, a to s akcentem na vybrané aspekty specificky se týkající zaměstnavatelů, když tito z povahy věci tvoří významnou skupinu subjektů zpracovávajících osobní údaje.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 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 v tomto textu jako „nařízení GDPR“.

Úvodem nutno předeslat, že základní principy, kterými se zpracování osobních údajů bude řídit, zůstávají víceméně stejné. Správci a zpracovatelé, včetně zaměstnavatelů, by tedy nadále měli dbát toho, aby úkony a operace, které s osobními údaji provádějí, byly (i) zákonné, korektní a transparentní, (ii) omezené na konkrétní výslovně vyjádřené a legitimní účely, s nezbytně minimálním rozsahem zpracovávaných osobních údajů, a zejména (iii) k těmto účelům přiměřené a zajišťující náležité zabezpečení osobních údajů. V případě jakékoliv nejasnosti pak zásady zpracování osobních údajů představují vodítko a výkladový korektiv.

1. Souhlas se zpracováním osobních údajů

Podstata institutu souhlasu subjektu údajů se zpracováním osobních údajů se nemění, nicméně právní úprava souhlasu a jeho získání (viz zejména čl. 4 odst. 11, čl. 7 a čl. 8 nařízení GDPR) byla zpřesněna a doplněna. Nařízení GDPR v této oblasti přináší vysoké nároky s tím, že důraz se klade na to, aby souhlas subjektu údajů se zpracováním osobních údajů, ať už se jedná o zaměstnance nebo klienta, byl:

- **svobodný a aktivní**

à souhlas nesmí být předpokládán např. před-zaškrtnutým políčkem v elektronickém dokumentu – subjekt údajů musí souhlas udělit aktivně sám;

à plnění smlouvy nesmí být podmíněno udělením souhlasu v případě, že by dané zpracování nebylo pro plnění smlouvy nutné (tzv. zákaz „take it or leave it“) – zaměstnavatel by tedy neměl nutit zaměstnance k udělení souhlasu pro nestandardní a nikoli nezbytné zpracování osobních údajů, např. ke zveřejnění jeho fotografií na různých sociálních sítích v rámci prezentace zaměstnanců, zaměstnavatele či jeho aktivit;

- **jednoznačný a konkrétní**

à souhlas musí být velmi jasně a konkrétně vyjádřen;

à britský Information Commissioner's Office, který je obdobou českého Úřadu pro ochranu osobních údajů, dokonce doporučuje, aby souhlas byl získán samostatně pro jednotlivé účely či jednotlivé úkony zpracování – dle názoru autorek se může jednat o jeden dokument, ve kterém bude vyjádřen souhlas jednotlivě pro určité účely či úkony zpracování např. samostatnými políčky;

- **ve své formulaci srozumitelný a subjektům údajů jazykově přístupný**

à vyžaduje se použití jasných a jednoduchých jazykových prostředků, což může působit potíže při současném uplatňování dalších požadavků nařízení (jednoznačnost souhlasu, informační povinnost vůči subjektům údajů);

- **zřetelně oddělen v případě, že je součástí jiného dokumentu**

à pokud souhlas není udělován na samostatném dokumentu, měl by být dostatečně graficky oddělen od zbytku textu (např. od pracovní smlouvy);

- **snadno odvolatelný**

à subjekt údajů může svůj souhlas kdykoliv odvolat, aniž by tím byla dotčena zákonnost zpracování provedeného před odvoláním souhlasu, o čemž musí být subjekt údajů poučen;

à odvolání souhlasu by mělo být stejně snadné, jako jeho udělení – je-li souhlas získáván např. písemným formulářem, lze doporučit vytvoření písemného formuláře na odvolání souhlasu, který bude snadno dostupný.

Je vcelku běžné, že zaměstnavatelé automaticky žádají o souhlasy svých zaměstnanců se zpracováním osobních údajů. Autorky článku proto doplňují, že se nedoporučuje získávat souhlas od subjektu údajů v případech, kdy správci nebo zpracovateli svědčí jiný právní titul pro zpracování osobních údajů, než je souhlas (viz ust. § 5 odst. 2 zákona o ochraně osobních údajů, resp. čl. 6 či čl. 9 nařízení GDPR). Nejenom že se tím správce či zpracovatel vyhne komplikacím se získáváním souhlasu, ale zároveň se nejedná o postup matoucí subjekty údajů, které by se mohly domnívat, že po odvolání uděleného souhlasu již příslušný správce či zpracovatel nebude jejich osobní údaje zpracovávat.

Zaměstnavatelé nepotřebují a nadále nebudou potřebovat souhlas například se zpracováním osobních údajů, které provádějí za účelem plnění svých zákonných povinností v oblasti sociálního a zdravotního pojištění, výpočtu mzdy či informační povinnosti vůči státním orgánům, nebo které je nezbytné před uzavřením pracovní smlouvy v rámci procesu přijímání nových zaměstnanců.

V praxi je častá otázka, zda správci a zpracovatelé budou povinni získat od subjektů údajů nové souhlasy se zpracováním osobních údajů. K tomu lze uvést, že daný postup nebude nezbytný v případech, kdy stávající souhlasy odpovídají požadavkům nařízení GDPR. Je proto podstatné, aby zaměstnavatelé provedli v rámci auditu svých systémů zpracování rovněž kontrolu a analýzu již získaných souhlasů subjektů údajů, jejich obsahu, formy a způsobu získání.

2. Práva subjektů údajů

Nejenom při udělování souhlasu se zpracováním osobních údajů by subjekt údajů měl být poučen o právech, která mu v souvislosti se zpracováním jeho osobních údajů náleží (viz čl. 12 a čl. 13 nařízení GDPR). Tato informace by přitom měla být stručná, srozumitelná a snadno přístupná použitím jasného a jednoduchého jazyka. Kromě stávajících práv, tj.

- práva na přístup k vlastním osobním údajům a informacím o jejich zpracování,

- práva na opravu či omezení zpracování (dle stávající terminologie blokace) osobních údajů,

- práva na výmaz osobních údajů (které nařízení GDPR však dále podrobně upravuje),

- práva vznést námitku proti zpracování osobních údajů a práva nestát se předmětem automatizovaného rozhodnutí,[1]

subjektům údajů dle nařízení GDPR náleží zcela nové právo na přenositelnost údajů. Jedná se o možnost subjektu údajů za stanovených podmínek získat osobní údaje, které se ho týkají a jež poskytl správci, a to ve strukturovaném, běžně dostupném a strojově čitelném formátu, a dále tyto údaje předat jinému správci (např. dalšímu zaměstnavateli). Je-li to technicky proveditelné, subjekt údajů může žádat i přímé předání osobních údajů jedním správcem správci druhému. K právu na přenositelnost údajů se vyjádřila i pracovní skupina WP29 v podobě výkladového materiálu.[2]

Právo na výmaz /„právo být zapomenut“ je v nařízení GDPR podrobně upraveno v návaznosti na dříve přijatou judikaturu soudních institucí Evropské unie. Jedná se o povinnost správce zlikvidovat osobní údaje, je-li naplněn jeden z vymezených důvodů (viz čl. 17 nařízení GDPR). Zaměstnavatel tak bude povinen vymazat osobní údaje zaměstnance např. v případě, kdy osobní údaje již nebude potřebovat pro původní účely

zpracování. Právo na výmaz však není bezvýjimečné, a zaměstnavatel si vyhodnotí, zda nebo do jaké míry se v konkrétním případě uplatní některá z výjimek.

Dle nařízení GDPR pro práva subjektů údajů obecně platí, že správce usnadňuje jejich výkon subjektům údajů, např. zpřístupněním různých formulářů pro uplatnění práv. Rovněž platí, že veškerá sdělení a veškeré úkony v souvislosti s uplatněním práv činí správci a zpracovatelé vůči subjektu údajů bezplatně, ledaže je žádost subjektu údajů zjevně nedůvodná, nepřiměřená nebo se často opakuje.

3. Záznamy zpracování a DPIA

Nařízení GDPR již nově neupravuje povinnost správců předem oznámit započetí zpracování osobních údajů či jeho změnu Úřadu pro ochranu osobních údajů („ÚOOÚ“). Zdánlivé administrativní zjednodušení však nařízení GDPR vyvažuje zavedením jiných povinností. Jedná se zejména o povinnost správců a zpracovatelů vést záznamy o činnostech zpracování (viz čl. 30 nařízení GDPR), a povinnost za stanovených podmínek provést posouzení vlivu na ochranu osobních údajů, a v návaznosti na to případně projít předchozí konzultací s dozorovým úřadem (viz čl. 35 a čl. 36 nařízení GDPR).

Záznamy

Povinnost vést záznamy o zpracování osobních údajů se vztahuje na správce i na zpracovatele, kteří zaměstnávají 250 nebo více osob, nebo na správce a zpracovatele, u nichž zpracování představuje pravděpodobně riziko pro práva a svobody subjektů údajů, nebo u nichž není příležitostné, anebo zahrnuje zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či zvláštních kategorií osobních údajů, tj. citlivých údajů – u zaměstnanců by se mohlo jednat např. o údaje o členství v odborové organizaci. Lze se domnívat, že povinnost vést záznamy o zpracování bude dopadat na všechny zaměstnavatele, neboť osobní údaje zpracovávají z povahy věci standardně a opakovaně, nikoliv jenom příležitostně, a někteří zaměstnavatelé mohou zpracovávat i údaje o členství v odborové organizaci[3].

Předmětem záznamové povinnosti je vedení písemných záznamů (přípustná je i elektronická forma) o jednotlivých činnostech a úkonech zpracování osobních údajů, přičemž vyžadovaný obsah záznamů je obdobný obsahu dřívější oznamovací povinnosti vůči ÚOOÚ. Do jisté míry tedy jde o náhradu za tuto oznamovací povinnost. Vedené záznamy by měly sloužit jak pro správce a zpracovatele pro jejich přehled a průběžnou aktualizaci jimi zavedeného systému zpracování, tak pro případnou kontrolu dozorového úřadu (a prokázání souladu s nařízením GDPR).

Předchozí posouzení vlivu

DPIA („Data Protection Impact Assessment“) neboli předchozí posouzení vlivu zamýšleného zpracování osobních údajů na jejich ochranu bude vyžadováno, bude-li pravděpodobné, že určitý druh zpracování přinese vysoké riziko pro práva a svobody

subjektů údajů. Nařízení GDPR příkladem uvádí, že posouzení bude nezbytné mj. pro případy rozsáhlého zpracování citlivých údajů nebo systematického a rozsáhlého vyhodnocování osobních aspektů (např. profilování) jako podkladu pro určitá automatizovaná rozhodnutí – může se to tedy dotknout nemocnic či e-shopů. Dozorovými úřady členských států Evropské unie by navíc měly být sestaveny seznamy druhů operací podléhajících požadavku tohoto posouzení. Lze předpokládat, že u většiny zaměstnavatelů, konkrétně ve vztahu k jejich zaměstnancům, tato povinnost nevznikne, ledaže by zaměstnavatel například využíval nové technologie skýtající vysoké riziko pro práva zaměstnanců coby subjektů údajů, např. různé monitorovací softwary (viz také bod 7 tohoto článku).

Základem DPIA bude posouzení rizik a možných opatření pro jejich zmírnění. V případě, že by z tohoto posouzení vyplývalo, že zamýšlené zpracování přinese vysoké riziko, pokud by správce nepřijal příslušná opatření k jeho zmírnění, bude povinností správce předběžně konzultovat svůj záměr s dozorovým úřadem (ÚOOÚ). Nelze vyloučit, že dozorový úřad v závažných případech zpracování osobních údajů zakáže.

Některá preventivní opatření

V souvislosti s nastíněnými povinnostmi stojí za zmínku, že nařízení GDPR přináší novou (nikoliv však převratnou) zásadu „záměrné a standardní ochrany osobních údajů“ (viz čl. 25). Ta v podstatě znamená, že správce by již při úmyslu zpracovávat osobní údaje měl naplánovat nastavení systému zpracování tak, aby odpovídal nařízení GDPR a dostatečně chránil práva subjektu údajů. Znamená to také, že správce by měl před započetím zpracování osobních údajů zavést vhodná technická a organizační opatření.
U zaměstnavatelů by tato opatření určitě měla zahrnovat *pravidelná školení zaměstnanců*, kteří s osobními údaji pracují, zejména zaměstnanců v HR oddělení, oddělení payroll apod. V opačném případě lze očekávat zcela zbytečná porušení práv subjektů údajů (ostatních zaměstnanců), která by zaměstnanci nakládající s osobními údaji nevědomě způsobovali, např. poskytnutím některých údajů neoprávněným subjektům k jejich (zdánlivě legitimnímu) dotazu či žádosti. V této souvislosti lze zcela jistě doporučit také *vypracování manuálu či kodexu pro potřeby těchto zaměstnanců*, zejména v případech, kdy je zaměstnanců zpracovávajících osobní údaje více. Pokud má k osobním údajům přístup větší množství těchto zaměstnanců, *záznamy* o zpracování osobních údajů by měly obsahovat také informace, kdo, kdy a jaký měl přístup k osobním údajům, resp. jak tyto údaje zpracovával. Nakonec lze také zmínit, že obecně nařízení GDPR preferuje pseudonymizaci nebo šifrování osobních údajů, tedy opatření, která znemožňují přístup k osobním údajům bez použití dodatečných informací.

4. Pověřenec pro ochranu osobních údajů („Data Protection Officer“)

Výraznou novinkou nařízení GDPR je funkce „Data Protection Officer“ neboli pověřence pro ochranu osobních údajů (viz čl. 37-39 nařízení GDPR). Povinnost jmenovat pověřence budou mít zaměstnavatelé (správci a zpracovatelé), (i) kteří jsou orgány veřejné moci a

veřejnými subjekty (s výjimkou soudů); (ii) jejichž hlavní činnosti vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo (iii) jejichž hlavní činnosti spočívají v rozsáhlém zpracování citlivých údajů, či rozsudků v trestních věcech a trestných činů.[4] Uvedená povinnost se tedy dotkne např. bank, pojišťoven, nemocnic či e-shopů provádějících profilování zákazníků (hodnocení osobních aspektů, včetně preferencí) atp.

Náplní činnosti pověřence pro ochranu osobních údajů bude zejména „compliance", tedy sledování souladu zpracování osobních údajů správcem či zpracovatelem s nařízením GDPR a dalšími předpisy v oblasti ochrany osobních údajů a také s jeho koncepcí v této oblasti, dále poskytovaní poradenství a informací správci či zpracovateli, včetně jeho zaměstnanců zpracovávajících osobní údaje a také působení jako kontaktního místa pro dozorové úřady, včetně ÚOOÚ, nebo pro subjekty údajů. Pověřencem může být jmenován zaměstnanec správce nebo zpracovatele, nebo i externí poskytovatel – dle ÚOOÚ vždy musí být odpovědnou konkrétní fyzická osoba, i kdyby poskytovatelem služby byla osoba právnická. Podstatné však bude, aby pověřenec detailně znal systém zpracování osobních údajů „svého" správce či zpracovatele, a aby disponoval potřebnými znalostmi a praxí – podle povahy subjektu se bude jednat o osobu s právní nebo technickou expertízou. Nařízení GDPR také zdůrazňuje nezávislost pověřence, který ohledně své činnosti nesmí dostávat žádné pokyny a je vázán mlčenlivostí. K institutu pověřence pro ochranu osobních údajů se vyjádřila i pracovní skupina WP29.[5]

Dobrou zprávou je možnost jmenovat společného pověřence, ať už se jedná o skupinu podniků (pověřenec musí být v tomto případě snadno dosažitelný, nikoli nutně fyzicky, pro všechny zúčastněné podniky) nebo několik orgánů veřejné moci či veřejných subjektů.

5. Povinnost správců ohlašovat a oznamovat tzv. DATA BREACHES

Nově je dle nařízení GDPR (viz čl. 33) každý zaměstnavatel v roli správce povinen ohlásit dozorovému úřadu jakýkoliv případ porušení zabezpečení osobních údajů – např. útok hackerů nebo jiné případy úniku nebo zničení osobních údajů – s výjimkou případu, kdy je nepravděpodobné, že by porušení představovalo riziko pro práva a svobody subjektů údajů. Správce je povinen učinit ohlášení bez zbytečného odkladu, nejpozději do 72 hodin od zjištění jednotlivého případu. Je-li navíc pravděpodobné, že porušení zabezpečení osobních údajů představuje vysoké riziko pro práva a svobody subjektů údajů, je zaměstnavatel (správce) povinen případ porušení oznámit rovněž dotčeným subjektům údajů, tedy dotčeným zaměstnancům a/nebo klientům, a to za použití jasných a jednoduchých jazykových prostředků (viz čl. 34 nařízení GDPR). Součástí oznámení je mj. informace o povaze porušení zabezpečení osobních údajů, jeho pravděpodobné důsledky a popis následně správcem přijatých nebo navržených opatření k řešení situace. Oznamovací povinnost přitom zjednodušeně řečeno nevzniká v případech přijetí dostatečných předběžných opatření (např. šifrování nebo pseudonymizace údajů) nebo následných opatření (viz čl. 34 odst. 3 nařízení GDPR). Vyžadovalo-li by oznámení

nepřiměřené úsilí, subjekty údajů mohou být informovány pomocí veřejného oznámení nebo podobného opatření.

S ohledem na nové výše uvedené povinnosti správců se zaměstnavatelům doporučuje připravit a zavést, např. v rámci manuálů a různých interních politik zpracování osobních údajů, postup při ohlašování a oznamování porušení zabezpečení osobních údajů, včetně rozdělení rolí a odpovědnosti mezi jednotlivé zaměstnance, přípravy formulářů ohlašování a oznamování, zaškolení zaměstnanců či posouzení možných následných opatření pro jednotlivé případy.

6. Pozor na mnohem vyšší sankce

Neméně podstatnou a praktickou je také informace, že možná výše sankcí za porušení povinností *se výrazně zvýší* – dnes je možné uložit pokutu do 10 mil. Kč, od účinnosti nařízení GDPR to bude až do 10 mil. EUR či 2 % celkového ročního světového obratu v případě méně závažných porušení a **až do 20 mil. EUR či 4 % celkového ročního světového obratu** u závažnějších porušení povinností.

7. Zaměstnavatelé coby správci

Specificky zaměstnavatele nutno upozornit na stanovisko pracovní skupiny WP29, která se v tomto dokumentu z června 2017 vyjadřuje ke zpracování osobních údajů v rámci pracovněprávních vztahů. Ačkoliv obsažená doporučení a vodítka nejsou závazná, zmíněný poradní orgán tvoří zástupci dozorových úřadů členských států EU, proto lze vyjít z toho, že takto budou pravděpodobně ze strany těchto úřadů povinnosti vyplývající z nařízení GDPR v budoucnu vykládány. Pracovní skupina zdůraznila důležitost základních principů zpracování, zejména nutnost dostatečného právního důvodu pro zpracování osobních údajů zaměstnanců (souhlas subjektu údajů nebo jiný zákonný důvod) a transparentnost a přiměřenost zpracování. Dále ze stanoviska vyplývá, že zamýšlí-li zaměstnavatel použít jakoukoliv monitorovací technologii nebo aplikaci[6], původně třeba zaměřenou na ochranu před únikem dat zaměstnavatele, která by nicméně mohla „sledovat zaměstnance“, měl by zvážit přiměřenost zaváděných opatření, ale také kroky, které by omezily dopad těchto opatření na soukromí zaměstnanců.[7] Namístě je i předchozí posouzení vlivu zamýšleného zpracování osobních údajů (monitorovací aktivity), tzv. DPIA. Také se doporučuje, aby zaměstnavatel zavedl pravidla upravující povolené užívání jeho zařízení a sítí, která by zároveň poskytla zaměstnancům podrobné informace o zpracování osobních údajů, k němuž na pracovišti, případně i mimo něj, dochází. Ohledně osob ucházejících se o zaměstnání stanovisko uvádí, že zaměstnavatelé by neměli automaticky užívat sociálních sítí k jejich prověřování, nicméně učiní-li tak v případě, že je to nezbytné a důležité pro výkon práce, měli by minimálně případné kandidáty na danou skutečnost upozornit.

Z hlediska zaměstnavatelů je důležitá také informace, že nařízení GDPR v čl. 88 umožňuje členským státům přijmout pro kontext pracovněprávních vztahů konkrétnější pravidla

zpracování osobních údajů. Zatím se zdá, že český zákonodárce této možnosti nevyužije, nicméně členské státy mají možnost oznámit Evropské komisi přijatá pravidla až do dne účinnosti nařízení GDPR, tj. do 25. května 2018. Do té doby by měl být v České republice přijat nový zákon o zpracování osobních údajů, který nahradí původní zákon a naváže na nařízení GDPR. Je tedy potřeba případné novinky v této oblasti nadále sledovat.

JUDr. Michaela Mackovičová, advokátka

JUDr. Michaela Hájková, LL.M., advokátka

[1] Nařízení GDPR výslovně zdůrazňuje také právo subjektu údajů na odvolání souhlasu se zpracováním osobních údajů a právo podat stížnost u dozorového úřadu.

[2] Dostupné zde: https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750. Pracovní skupina WP29 je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie, jejímž úkolem bylo mj. přispívat k jednotnému uplatňování národních úprav členských států. Účinností nařízení bude transformována na Evropský sbor pro ochranu osobních údajů.

[3] Nutno mít na paměti, že zaměstnavatel dle ust. § 316 odst. 4 písm. e) zákoníku práce nesmí vyžadovat od zaměstnance informace o členství v odborové organizaci, nicméně tato informace mu může být poskytnuta z iniciativy zaměstnance či odborové organizace.

[4] Povinnost jmenovat pověřence vzniká dle čl. 37 odst. 4 nařízení GDPR také v dalších případech, kdy to vyžaduje právo Evropské unie nebo členského státu, nicméně takové specifické případy zatím v platném právu upraveny nejsou.

[5] Dostupné zde: https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750

[6] V této oblasti je aktuálně zajímavý rozsudek Evropského soudu pro lidská práva, konkrétně tzv. Velkého senátu, který rozhodl odchylně od původního rozhodnutí Senátu, ve věci rumunského zaměstnance Barbulescu týkající se sledování jeho elektronické komunikace zaměstnavatelem. Dle tohoto rozsudku by zaměstnavatel měl před započetím monitorování komunikace upozornit zaměstnance na tuto možnost a na povahu monitorování. Zaměstnavatel by také měl mít konkrétní legitimní důvod pro monitorování komunikace, přičemž monitorování by mělo představovat přiměřené opatření. Nakonec, používání pracovní elektronické komunikace pro soukromé účely zaměstnancem nemusí být automaticky dostatečným důvodem pro výpověď z pracovního poměru.

[7] Z hlediska českého právního řádu nesmí být případné monitorování zaměstnanců v rozporu ani s ust. § 316 odst. 1 až 3 zákoníku práce.

HOLEC, ZUSKA & PARTNEŘI

ADVOKÁTI | ATTORNEYS | RECHTSANWÄLTE

Kontaktujte nás

Radlická 1c/3185
150 00 Praha 5
Česká republika
[mapa]

- Telefon: (+420) 296 325 235
- Fax: (+420) 296 325 240
- recepce@holec-advokati.cz