# A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít – část I.

Ochrana osobních údajů a soukromí fyzických osob, zejména dětí, je v dnešním světě plném nových technologií velmi důležitá. Obrovská vlna hysterie kolem Obecného nařízení o ochraně osobních údajů (GDPR), která se Českem prohnala a která je dle našeho názoru nedůvodná, však způsobila, že se velká část společností, které se dosud této problematice spíše vyhýbaly, či v lepším případě ji měly někde vzadu v povědomí, začala pod hrozbou vysokých pokut ochranou osobních údajů cíleně zabývat.

Zdálo by se, že tím, jak tato hysterie utichá, můžete tuto problematiku opět odsunout. Opak je ale pravdou. Právě teď je totiž vhodná doba se s ochranou osobních údajů v klidu popasovat. K tomu Vám může napomoci i tento článek, ve kterém bychom se s Vámi rádi podělili o naše zkušenosti z provedených právních auditů ochrany osobních údajů a upozornili na nejčastější chyby, na které při nich naše advokátní kancelář naráží. Současně poradíme, jak těmto chybám předejít.

## Nadbytečné užívání souhlasu

Začněme, jak jinak, nadbytečným užíváním souhlasu. Asi klasickým příkladem je ustanovení pracovní smlouvy či poslední věta pracovního dotazníku, kde zaměstnanec dává souhlas se zpracováním svých osobních údajů pro, například, mzdové účely. Podnikatelé se často vůbec nezabývají hledáním jiného právního titulu ke zpracování a volí souhlas jako zdánlivě správné a snadné řešení. Souhlas je však v tomto případě nesprávným právním titulem. Dle stanoviska Úřadu pro ochranu osobních údajů (dále „ÚOOÚ“) č. 3/2014 je vyžadování souhlasu se zpracováním osobních údajů protiprávní v případě, kdy správce tento souhlas nepotřebuje (a nepotřebuje jej v drtivé většině běžných případů). Podle názoru ÚOOÚ totiž takový postup fakticky znamená, že správce subjekt údajů nesprávně informuje. A my dodáváme, že to taktéž fakticky znamená, že daná společnost nemá vůbec přehled o právních titulech pro svá zpracování.

Doporučujeme tedy všem správcům, aby si rozdělili jednotlivé činnosti zpracování, které provádí, a k nim si přiřadili odpovídající právní titul dle GDPR (jednotlivé tituly najdete v článku 6 GDPR, v případě „citlivých“ osobních údajů v článku 9 GDPR). A přestože je souhlas jako právní důvod pro zpracování v GDPR uveden hned na prvním místě, používejte jej (nejen) v pracovněprávních vztazích, co nejméně. K důvodům blíže v části týkající se otisků prstů.

## Porušení zásady minimalizace

Zásada minimalizace je jednou z hlavních zásad zpracování osobních údajů a je výslovně zakotvena v čl. 25 GDPR. Rozsah zpracovávaných osobních údajů musí být přiměřený, relevantní a omezený ve vztahu k účelům, pro které jsou zpracovávány. Z kontrolní činnosti ÚOOÚ vychází, že zaměstnavatelé nadbytečně zpracovávají informace například o tom, že je zaměstnanec voják, údaje manželky, přestože se nejedná o vyživovanou osobu, údaje o členství v odborech (pokud zaměstnavatel nesráží příspěvky pro odborovou organizaci), údaje kontaktní osoby bývalého zaměstnance apod. Projděte si tedy své dotazníky pro zaměstnance a ptejte se, zda všechny požadované údaje skutečně potřebujete. Dotazníky poté upravte tak, abyste od zaměstnance získali skutečně pouze nezbytné údaje. Náš tip: např. u kolonky „Údaje o manželce“ přidejte poznámku – Vyplňte, pokud uplatňujete daňové zvýhodnění.

Dalším velmi častým pochybením je, že v pracovní smlouvě jsou kromě jména, data narození a bydliště, uvedeny i jiné údaje (např. kontakty, číslo občanského průkazu, rodné číslo apod.) a tyto jsou dále kopírovány do dotazníku, dohody o mzdě, dohody o srážkách ze mzdy a jiných dokumentů, které zaměstnavatel se zaměstnanci uzavírá. Dochází tak k nadbytečné duplicitě zpracování a zvýšení rizika jejich zneužití.

Tuto zásadu neprolomíte ani tím, že budete mít vše podloženo souhlasy. Není-li dané zpracování účelné, pak ani platný souhlas nezhojí porušení této zásady (narážíme zde na souhlasy, se kterými jsme se v praxi setkali, a které připomínají spíše známou hru „bingo“ než kvalifikovaný právní dokument, kde subjekt má zaškrtnout k čemu uděluje souhlas a má jej udělit ke všemu, co už reálně správce nadbytečně shromažďuje).

## Porušení zásady minimalizace – kopírování dokladů

Porušení zásady minimalizace spočívá také v tom, že zaměstnavatelé často kopírují osobní doklady zaměstnanců. Přitom zákaz pořizování kopií občanských průkazů a cestovních dokladů je dán výslovně zákonem.[1] U řidičských průkazů se doporučuje tyto nekopírovat, případně kopírovat jen tam, kde je to nezbytné, např. u řidičů z povolání. Vhodné opatření je také udělat jen částečnou kopii tak, aby nemohlo dojít ke zneužití dokladu.

Ve smyslu § 316 zákoníku práce platí, že zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem jeho práce. Dejte tedy pozor, kdy například vyžadujete a ukládáte originály či kopie výpisů z Rejstříku trestů (nejde paušálně u všech), případně dokladů o vzdělání (je-li někdo zaměstnán například na pozici vrátný, není nezbytné o něm uchovávat kopii maturitního vysvědčení. My se domníváme, že v takovém případě nemusíte tento údaj vůbec evidovat).

[1] v § 15a odst. 2 zákona o občanských průkazech, § 2 odst. 3 zákona o cestovních dokladech.

### Neplnění informační povinnosti

Článek 13 GDPR stanoví právo subjektu údajů na informace. Tomuto právu odpovídá povinnost správce mu tuto informaci poskytnout, a to v okamžiku, kdy osobní údaje získá. Zde by měl správce promyslet, jak s co nejmenší administrativní zátěží informovat všechny subjekty údajů o všech činnostech zpracování, které provádí. Přestože tato povinnost byla dána i předchozí právní úpravou, v praxi je velmi časté, že správci tuto povinnost neplní.

Z našeho pohledu se jedná o povinnost porušovanou v nejvyšší míře zejména vůči zaměstnancům, kteří nebývají buďto informováni vůbec nebo zcela nesprávně. Velmi velký význam má informační povinnost např. při jakémkoliv monitoringu zaměstnanců (nejčastěji v případě kamerových systémů, GPS systémů apod.), kdy nesplněním této povinnosti se zaměstnavatel dopouští nejen porušení pravidel GDPR, ale rovněž i pravidel zákoníku práce, za něž mu hrozí nemalé pokuty od Státního úřadu inspekce práce.

### Neexistence skartačních lhůt

Každá činnost zpracování má své „datum spotřeby". Jinými slovy, osobní údaje mohu zpracovávat pouze tehdy, pokud mi trvá účel, pro který tak činím a pokud mám k tomuto účelu právem aprobovaný důvod (právní titul). Je třeba projít jednotlivé činnosti zpracování a stanovit si u nich skartační lhůty s ohledem na účel, pro který osobní údaje zpracovávám. Zpracovávám-li osobní údaje na základě titulu plnění smlouvy, pak trvá po dobu smlouvy. Zpracovávám-li osobní údaje na základě titulu plnění právní povinnosti, pak musím hledat v právním předpisu, jak dlouho mám tyto osobní údaje zpracovávat. Zpracovávám-li osobní údaje na základě oprávněného zájmu, pak musím s ohledem na trvání mého oprávněného zájmu stanovit přiměřenou dobu (tuto je vhodné stanovit s trochou zdravého rozumu a s ohledem na praktické potřeby).

Autorky: Mgr. Lucie Demeterová, advokátka, Mgr. Kateřina Hakrová, advokátní koncipientka (DEMETER LEGAL, advokátní kancelář)

*(Právní prostor 3. 10. 2018)*

# A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít – část II.

Ochrana osobních údajů a soukromí fyzických osob, zejména dětí, je v dnešním světě plném nových technologií velmi důležitá. Obrovská vlna hysterie kolem Obecného nařízení o ochraně osobních údajů (GDPR), která se Českem prohnala a která je dle našeho názoru nedůvodná, však způsobila, že se velká část společností, které se dosud této problematice spíše vyhýbaly, či v lepším případě ji měly někde vzadu v povědomí, začala pod hrozbou vysokých pokut ochranou osobních údajů cíleně zabývat.

Zdálo by se, že tím, jak tato hysterie utichá, můžete tuto problematiku opět odsunout. Opak je ale pravdou. Právě teď je totiž vhodná doba se s ochranou osobních údajů v klidu popasovat. K tomu Vám může napomoci i tento článek, ve kterém bychom se s Vámi rádi podělili o naše zkušenosti z provedených právních auditů ochrany osobních údajů a upozornili na nejčastější chyby, na které při nich naše advokátní kancelář naráží. Současně poradíme, jak těmto chybám předejít.

### Nejsou smlouvy se zpracovateli

Uzavřít či neuzavřít smlouvu o zpracování osobních údajů? To je, oč tu (zejména v posledních týdnech) běží. Obdobně jako u souhlasů se se smlouvami o zpracování roztrhl pytel. Nejsou výjimkou situace, kdy Vás osloví obchodní partner s tím, že jeho právník tvrdí, že jste Vy zpracovatel nebo naopak on je Vaším zpracovatelem, a musíte s ním uzavřít smlouvu o zpracování. Necháte si situaci posoudit Vaším právním poradcem a ten k tomu zaujme zcela odlišné stanovisko – smlouvu mít uzavřenou nemusíte. A teď, babo, raď! Pokud je to i Váš případ a Vy se rozhodnete zpracovatelskou smlouvu neuzavřít, nezapomeňte si připravit zdůvodnění, proč se domníváte, že právě Vy či Váš obchodní partner nejste zpracovatelem.

Na druhou stranu existují poskytovatelé, kteří budou zpracovateli s pravděpodobností blížící se jistotě. Typickým příkladem je externí poskytovatel účetních služeb či poskytovatel cloudových služeb. Zpracovatelem bývá také bezpečnostní agentura, která pro vás zajišťuje bezpečnost objektu a kamerové systémy.

Působí ve Vaší společnosti odborová organizace? Provádíte jako zaměstnavatel srážky ze mzdy svých zaměstnanců na úhradu členských příspěvků? Pokud jste si odpověděli ano, jste zpracovatelem osobních údajů naopak vy. V tomto případě dokonce zpracováváte údaje citlivé, na něž se vztahuje přísnější režim a celá řada povinností (např. na takové zpracování může dopadnout čl. 30 odst. 2 GDPR, zabezpečení apod.).

Naopak zpracovatelem osobních údajů zpravidla nebude lékař, který zajišťuje pro zaměstnavatele pracovně-lékařské služby. Dle našeho názoru zpracovatelem osobních údajů nejsou ani poskytovatelé přepravních služeb, kteří jsou využíváni v rámci e-shopů,

kdy si tyto přepravce volí při objednávce sám zákazník. Zpracovatelem nebude ve většině případů ani advokát či auditor. Všichni tito poskytovatelé jsou tzv. dalšími příjemci, neboť si sami stanoví své účely zpracování.

Případy, u nichž doporučujeme vždy individuálně posoudit, zda se o zpracovatele jedná či nikoliv, jsou poskytovatelé různých IT služeb, např. hostingových služeb, dodavatelé IT systémů či poskytovatelé IT podpory. Posouzení zde bývá často složitější, jelikož v řadě případů není vůbec uzavřena písemná smlouva k poskytování těchto služeb, která by jasně definovala jejich rozsah. Nejen s ohledem na to, k jakým datům se IT specialisté mohou často dostat, ale i s ohledem na význam IT systémů a souvisejících služeb, kdy tyto představují významnou podporu Vašeho podnikání či jiné činnosti, doporučujeme IT smlouvám věnovat náležitou pozornost.

Ohledně zpracovatelů je tedy vhodné začít tím, že si uděláte kompletní seznam všech poskytovatelů (dodavatelů), určíte, kdo z nich je zpracovatelem, a prověříte, zda skutečně se všemi máte uzavřenou smlouvu o zpracování v písemné formě (včetně elektronické). Zde je nutné si uvědomit, že uzavřít smlouvu o zpracování osobních údajů je nejen povinností správce, který v případě, že smlouva není uzavřena předává (tedy zpracovává) osobní údaje nezákonně, ale také povinností zpracovatele, který je ve stejném případě v pozici neoprávněného správce.

Nebude-li zřejmé, zda daný poskytovatel je zpracovatelem a domníváte se, že spíše nebude, provedenou analýzu si uchovejte pro případnou kontrolu ze strany ÚOOÚ. A pokud daný poskytovatel dojde (byť i nahodile) do styku s osobními údaji, za jejichž ochranu nesete odpovědnost, doporučujeme uzavřít alespoň dohodu o mlčenlivosti (neboli NDA).

Za vhodné považujeme také doplnit, že není nezbytné mít smlouvu nazvanou Smlouva o zpracování, je však nezbytné, aby dohoda mezi Vámi a zpracovatelem obsahovala všechny nezbytné náležitosti stanovené v článku 28 GDPR. V praxi je zcela běžné, že IT dodavatelé mají tuto smlouvu zahrnutou ve svých obchodních podmínkách.

V neposlední řadě prosím nezapomeňte, že každý správce, využívá-li ke zpracování osobních údajů třetí osobu, která na její pokyn zpracovává osobní údaje, by měl důsledně daného zpracovatele ověřit. Tedy vybírejte si jen takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření. Pro případný spor doporučujeme správcům, aby byli schopni doložit, jakým způsobem ověřili důvěryhodnost zpracovatele. K ověření přitom může postačit využití všech běžných nástrojů pro posuzování poskytovatelů, tj. ověření identity, majetkové struktury, délky existence, listin ve sbírce listin, ověření dlužnických registrů, insolvenčního rejstříku apod. V některých společnostech je toto samozřejmost, v některých tento postup ověření zcela chybí. Takové ověření poskytovatele i klienta Vám může ušetřit mnoho nepříjemností i v běžném obchodním styku.

## Nesprávné zpracování osobních údajů uchazečů o zaměstnání

Obecně platí, že zaměstnavatel je oprávněn od uchazečů o zaměstnání požadovat pouze takové informace, které bezprostředně souvisejí s uzavřením pracovní smlouvy[1]. V případě dodržení zásady minimalizace dle GDPR, lze zpracování osobních údajů pro účely výběrového řízení opřít o právní důvod dle článku 6/b GDPR (tj. plnění smlouvy/provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů). Ke zpracování osobních údajů uchazeče pro účely účasti ve výběrovém řízení tedy není zapotřebí souhlasu, jak často v praxi bývá nesprávně vyžadováno.

Jiná situace však nastane ve chvíli, kdy je výběrové řízení u konce. Poté lze teoreticky pro účely dalšího oslovení zpracovávat osobní údaje uchazečů po dobu trvání zkušební doby vybraného uchazeče na základě oprávněného zájmu zaměstnavatele dle článku 6/f GDPR (aby nemusel opakovat výběrové řízení v případě, kdy se původně vybraný uchazeč neosvědčí).

Bude-li však zaměstnavatel uchovávat životopisy k tomuto účelu po dobu delší, bude už pro takové zpracování zapotřebí souhlasu uchazeče. Tento souhlas však musí být udělen svobodně, ideálně tedy až po skončení výběrového řízení, neboť kdyby jej zaměstnavatel získával dříve, mohla by zde na straně uchazeče vzniknout domněnka, že souhlas musí dát, jinak nebude zařazen do výběrového řízení. Stejně doporučujeme postupovat v případě, že Vám případný uchazeč zašle své osobní údaje v rozsahu životopisu a vy v současné chvíli místo nemáte, ale rádi byste si jeho životopis uchovali.

Setkali jsme se také s názorem, že osobní údaje uchazečů v rozsahu životopisu lze uchovávat z důvodu oprávněného zájmu pro účely prokázání správného postupu při výběrovém řízení (nediskriminace). Takové zpracování však vidíme jako rizikové, jednak totiž uchování těchto životopisů svádí zaměstnavatele zneužít je i pro jiný účel (tedy pro opětovné oslovení), a dále je diskutabilní, zda by prostřednictvím životopisů mohl vůbec zaměstnavatel nějak svou nevinu v případě podezření z diskriminace prokázat.

## Neexistence záznamů o činnostech zpracování

Článek 30 GDPR stanoví správci povinnost vést tzv. záznamy o činnostech zpracování. Tato povinnost se v souladu s článkem 30/5 GDPR nepoužije na podnik, který zaměstnává méně než 250 zaměstnanců, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování citlivých údajů.

Současný výklad článku 30 GDPR tenduje spíše k tomu, že tato povinnost dopadne na většinu správců s ohledem na to, že výjimka se uplatní pouze na ty správce, kteří provádí příležitostné zpracování. Z tohoto důvodu a také proto, že vypracování záznamů nepřestavuje nadměrnou administrativní zátěž, naopak může být vhodným nástrojem pro zpřehlednění, doporučujeme záznamy o činnostech vypracovat.

[1] Viz § 30/2 zákoníku práce a obdobně § 12 zákona č. 435/2004 Sb., zákona o zaměstnanosti.

### Zaměstnanci/studenti měsíce

Oblíbeným nástrojem pro motivaci zaměstnanců či studentů je pořádání nejrůznějších anket, kdy zaměstnavatel, případně škola, vyzvedne šikovnost některého z kolegů v jakési dobré víře, že takováto pozitivní publicita nikomu neškodí a nemůže tak nikomu vadit. To však nemusí být vždy pravda. Při pořádání takových anket proto doporučujeme postupovat tak, že například budou hodnoceny týmy („tým směny A" není osobní údaj). Bude-li tato anketa pořádána za použití osobních údajů, kloníme se spíše k názoru, že je třeba pro takové zpracování zapotřebí souhlasu.

### Chybné srážení ze mzdy zaměstnance za účelem hrazení odborových příspěvků

Jak jsme již výše naznačili, v tomto vztahu je to zaměstnavatel, kdo je zpracovatelem. Z našich zkušeností vyplývá, že zaměstnavatelé, resp. odborové organizace tento vztah zpravidla nijak ošetřen nemají.

Současně, při provádění auditů často zjišťujeme, že zaměstnavatelé neprovádí srážky ze mzdy zaměstnanců za tímto účelem ani v souladu se zákoníkem práce. Zákoník práce s tímto výslovně počítá, konkrétně v § 146 písm. c), kde se uvádí, že srážky ze mzdy mohou být provedeny k úhradě členských příspěvků zaměstnance, který je členem odborové organizace. Musí však být splněny dvě podmínky, kterými jsou ujednání v kolektivní smlouvě nebo v písemné dohodě mezi odborovou organizací a zaměstnavatelem a současně je třeba souhlasu zaměstnance s prováděním srážek.

S ohledem na to, že je třeba také ošetřit vztah správce – zpracovatel, doporučujeme, aby již samotná dohoda o provádění srážek mezi zaměstnavatelem a odbory či kolektivní smlouva reflektovala náležitosti smlouvy o zpracování.

Opět považujeme za vhodné upozornit na fakt, že údaj o členství v odborech patří do zvláštní kategorie osobních údajů (citlivé osobní údaje), u nichž je třeba důsledně dbát na zabezpečení a také na to, aby zaměstnavatel nezpracovával tyto osobní údaje za jiným účelem (tedy například, že neuvádí skutečnost, že daný zaměstnanec je v odborech, v osobním spise či v personálním systému apod.).

Autorky: Mgr. Lucie Demeterová, advokátka, Mgr. Kateřina Hakrová, advokátní koncipientka (DEMETER LEGAL, advokátní kancelář)

*(Právní prostor 5. 10. 2018)*

# A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít – část III.

Ochrana osobních údajů a soukromí fyzických osob, zejména dětí, je v dnešním světě plném nových technologií velmi důležitá. Obrovská vlna hysterie kolem Obecného nařízení o ochraně osobních údajů (GDPR), která se Českem prohnala a která je dle našeho názoru nedůvodná, však způsobila, že se velká část společností, které se dosud této problematice spíše vyhýbaly, či v lepším případě ji měly někde vzadu v povědomí, začala pod hrozbou vysokých pokut ochranou osobních údajů cíleně zabývat.

Zdálo by se, že tím, jak tato hysterie utichá, můžete tuto problematiku opět odsunout. Opak je ale pravdou. Právě teď je totiž vhodná doba se s ochranou osobních údajů v klidu popasovat. K tomu Vám může napomoci i tento článek, ve kterém bychom se s Vámi rádi podělili o naše zkušenosti z provedených právních auditů ochrany osobních údajů a upozornili na nejčastější chyby, na které při nich naše advokátní kancelář naráží. Současně poradíme, jak těmto chybám předejít.

### Kamerové systémy

Kamerové systémy se záznamem jako forma zpracování osobních údajů je v praxi natolik rozšířená, že již v minulosti ÚOOÚ vydal návodnou metodiku nazvanou Provozování kamerových systémů.[1] Metodika ÚOOÚ jednoduchým a přehledným způsobem seznamuje správce s povinnostmi, které mají při implementaci kamerových systémů dodržet. Jelikož je metodika vypracována v souladu se starou právní úpravou, je potřeba její aplikaci v několika málo bodech přizpůsobit nové úpravě.

Vždy je třeba si uvědomit, že zde dochází ke střetu dvou základních lidských práv, a sice práva provozovatele kamerového systému na ochranu majetku a dále práva jedince na ochranu soukromí.

O tom, že se nejedná o plané strašení, svědčí i fakt, že právě kamerové systémy jsou velmi častým předmětem kontrol ze strany ÚOOÚ; kontroly jsou ve většině případů zahajovány na podnět, např. nespokojeného zaměstnance (odkazujeme na webové stránky ÚOOÚ www.uoou.cz v sekci „Dozorová činnost").

Specifickou kategorií jsou kamerové systémy na pracovišti. Jejich režim je upraven v § 316 zákoníku práce, kdy jejich prostřednictvím zpravidla dochází k monitoringu zaměstnanců. Provozovat kamerové systémy, které fakticky sledují zaměstnance, může

[1] https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf

zaměstnavatel pouze ze závažného důvodu spočívajícího ve zvláštní povaze jeho činnosti. Pokud je tento závažný důvod dán, je zaměstnavatel povinen přímo zaměstnance informovat o rozsahu kontroly a o způsobech jejího provádění.

Za nesprávné či nezákonné provozování kamerového systému hrozí nejen sankce dle GDPR od Úřadu pro ochranu osobních údajů, ale také pokuty od inspektorátu práce. Inspektoráty práce to v minulosti dělaly tak, že když na nezákonný kamerový systém narazily, daly podnět ÚOOÚ. Dnes už mohou pokutu dát sami, a to až do výše 1 mil. Kč, nebo 100 tis. v případě, kdy zaměstnavatel neposkytne zaměstnancům výše zmíněnou informaci o rozsahu kontroly a o způsobech jejího provádění.

Dokumentace ke kamerovému systému (dále „CCTV") tak, aby byla nápomocná, by se měla sestávat z analýzy používání CCTV, identifikace CCTV a jeho popisu, plánku rozmístění jednotlivých kamer, analýzy rizik, popisu technicko-organizačních opatření, směrnice na provozování kamerového systému, informační tabulky a podrobné informace o zpracování osobních údajů, ze záznamů o školení, z evidence žádostí o poskytnutí kamerového záznamu a předávacích protokolů, z projektové dokumentace a náhledů jednotlivých kamer.

Co všechno jednotlivé dokumenty mají obsahovat najdete ve výše zmíněné metodice ÚOOÚ. Před každým zavedením kamerového systému tedy doporučujeme správcům prostudovat tuto metodiku a vypracovat si kompletní dokumentaci. S přípravou této dokumentace Vám může pomoci jednak společnost, která Vám instalaci kamer nabízí, případně advokátní kancelář, která se na tuto oblast specializuje. Dokumentace je velmi užitečným podkladem a cenným dokladem toho, že jste se výše zmíněnou rovnováhou skutečně zabývali.

## Používáte otisky prstů Vašich zaměstnanců (subjektů údajů) v přístupových a docházkových systémech?

Do 25. května 2018 bylo v zásadě možné, dle dosavadního zákona o ochraně osobních údajů, a na to navazujícího stanoviska ÚOOÚ[2], odlišovat dvě technická řešení s odlišnými právními důsledky.

První řešení spočívá v sejmutí otisků prstů, které jsou následně převedeny na číselnou řadu (šablonu) způsobem, který neumožňuje zpětnou rekonstrukci biometrických charakteristik, a nadále je pracováno pouze s touto šablonou, nikoli s otiskem prstu jako takovým. Dle dosavadního výkladu se v tomto případě nejednalo o zpracování citlivých osobních údajů, ale pouze údajů obecných. Dle ÚOOÚ zde nedochází k uchování ani k aktivnímu využívání biometriky při identifikaci či autentizaci, a tudíž se tak nejedná o zpracování citlivých osobních údajů. Výsledkem je, že zde není zapotřebí výslovného souhlasu a lze využít oprávněný zájem správce (za dodržení hlediska přiměřenosti).

Druhým řešením jsou systémy, které s biometrickými údaji aktivně pracují, např. při ověřování každého dalšího podpisu dané osoby, spuštění či aktivaci mobilního telefonu nebo počítače atd. Zde se jedná o zpracování citlivých osobních údajů a pro jejich provoz je nezbytné disponovat výslovným souhlasem osob, jejichž údaje jsou takto zpracovávány.

S příchodem GDPR se však tento přístup mění. Nové nařízení totiž považuje každé zpracování otisku prstů (tedy biometrických údajů) za zpracování citlivých osobních údajů. Jen ztěžka budete v článku 9 GDPR, který upravuje právní tituly zpracování pro zvláštní kategorii (citlivých) údajů, hledat jiný právní titul než souhlas.

Je důležité zdůraznit, že zpracovávání citlivých údajů obvykle představuje vyšší riziko pro práva dotčených osob a je tedy krom výhod takového systému nutné náležitě zvážit i povinnosti, které se k tomu vážou, např. zajistit zvýšenou úroveň ochrany či povinnost provést posouzení vlivu.

Upozorňujeme také na skutečnost, že podle stanoviska skupiny WP 29 č. 2/2017 (skupina, která dává výkladová stanoviska k GDPR) není svobodnost souhlasu v pracovněprávních vztazích obvykle dána, což se může při kontrole ÚOOÚ jevit jako problematické. Společnost bude muset prokázat, že byl souhlas zaměstnance opravdu svobodný. Pochybnost o svobodném souhlasu by mohla vyvolat například situace, kdy by v rámci organizace udělili souhlas všichni zaměstnanci.

Jak vyplývá i z našich zkušeností, změny, které v souvislosti s biometrickými údaji nastaly, dopadají na celou řadu společností, které tyto systémy zavedly, a dosud používaly v režimu popsaném v prvním případě. Současný výklad může vést k tomu, že společnosti reálně nebudou moci tyto systémy používat, jelikož nezískají platné souhlasy subjektů údajů či nesplní přísnější povinnosti vztahující se ke zpracování citlivých osobních údajů. I z tohoto důvodu se tato otázka stala předmětem diskuze na celoevropské úrovni a předpokládá se, že k ní bude v budoucnu vydáno upřesňující stanovisko. Doporučujeme tak sledovat webové stránky ÚOOÚ.

## Máte ve služebních vozech GPS technologie?

Používání GPS technologií ve služebních vozech je monitoringem zaměstnanců, při němž rovněž dochází ke zpracování osobních údajů – záznamů z GPS systémů. Vzhledem k tomu, že používání GPS systémů ve služebních vozech, resp. monitoring zaměstnanců obecně, představuje významný zásah do soukromí zaměstnanců, je důsledně právně regulován, a to nejen pravidly GDPR.

Monitoring zaměstnanců je primárně zakázaný především zákoníkem práce. Z tohoto zákazu však existují výjimky. Stěžejní výjimka je definována v § 316 zákoníku práce, který říká, že zaměstnavatel musí mít k takovému monitoringu závažný důvod spočívající

[2] Stanovisko č. 3/2009

v povaze jeho činnosti, kterým zavedení kontrolních mechanismů ospravedlní. Jak jsme již uvedli výše, zaměstnavatel je povinen stanovit pro monitoring pravidla a je povinen zaměstnance informovat o rozsahu kontroly a způsobu jejího provádění. Předpoklad závažnosti důvodu k monitoringu prostřednictvím GPS neobejdete ani případným souhlasem zaměstnance. Takový souhlas by byl totiž z pohledu zákoníku práce shledán neplatným. V případě kontroly ze strany Státního úřadu inspekce práce byste se tak vystavili riziku značné pokuty viz informace v části Kamerové systémy výše.

Samotné použití GPS technologií za účelem monitoringu zaměstnanců je vždy třeba řádně zvážit s ohledem na všechny okolnosti, a zejména je náležitě odůvodnit. Nutnost využívání GPS technologie může uhájit obecně například společnost, která se potýká s černými jízdami svých zaměstnanců apod. Obhájit by je mohla také stavební firma, která potřebuje kontrolovat, jestli byl materiál zavezen všude, kam měl, a řidiči nastoupili do práce včas, společnost zajišťující bezpečný převoz peněz, společnost využívající obchodní zástupce, jejich neúspěšné obchody nelze ověřit atd. Jako legitimní důvod využívání GPS se považuje i potřeba zajištění využití GPS jako dokladu o povinném odpočinku během řízení motorového vozidla.

Jako nepřiměřené by se naopak jevilo využití GPS například v provozu advokátní kanceláře, jejíž koncipienti jsou jednou za čas vysláni na jednání u soudu, k němuž se dopravují služebním vozidlem. Jako nepřiměřené opatření byl také posouzen nepřetržitý dlouhodobý (po dobu 11 měsíců) monitoring poštovních doručovatelů za účelem zefektivnění poštovních služeb.

Před každým monitoringem tedy doporučujeme zvážit, zda zájmy zaměstnavatele v tomto konkrétním případě převažují nad zájmem zaměstnance na soukromí, monitoring náležitě odůvodnit, doložit incidenty z minulosti a minimalizovat zpracování osobních údajů na rozsah nezbytně nutný pro stanovený účel. Právním titulem zpracování přichází v úvahu oprávněný zájem, bude-li shledán. Dovolíme si také upozornit, že ve valné většině případů se bude jednat o rizikové zpracování, tedy bude vhodné například provést posouzení vlivu atd.

A co použití GPS technologií za účelem vedení knihy jízd? I zde doporučujeme spíše opatrnější přístup. Je pravdou, že v tomto případě se primárně nejedná o monitoring zaměstnance, tj. sledování konkrétního zaměstnance za účelem zjištění jeho určitého jednání, ale důvodem je zajištění evidence jízd – podkladu pro daňové účely. K monitoringu tak dochází v tomto případě nepřímo. Pokud využíváte GPS systém za tímto účelem, nejedná se tedy o monitoring zaměstnanců, nicméně stále se jedná o zpracování osobních údajů. Musíte tedy disponovat platným právním titulem. Z dotazu, který jsme směřovali na ÚOOÚ vyplynulo, že právním titulem v tomto případě bude souhlas zaměstnance. Pozor však na to, aby tento souhlas splňoval veškeré náležitosti, zejména aby byl svobodný. Svobodnost v tomto případě můžete zajistit např. tím, že zaměstnance řádně informujete a dáte mu na výběr, zda chce vést knihu jízd klasickým způsobem sám (v papírové či elektronické podobě) či zda chce využít možnosti GPS sledování, prostřednictvím kterého bude kniha jízd vedena automaticky, a jemu usnadní práci. V případě, že je zaměstnanec oprávněn využívat služební vůz i pro soukromé účely, doporučujeme využívat takové zařízení, které bude možné v takových případech vypnout.

## Nejsou stanoveny postupy pro ohlašování případů porušení zabezpečení osobních údajů ÚOOÚ

Velkou novinkou je zavedení ohlašovací povinnosti v případě porušení zabezpečení OÚ. S ohledem na novou povinnost je zcela pochopitelné, že je na její plnění připraven málokdo. Doporučujeme, aby správce osobních údajů (i) zajistil, aby všichni jeho zpracovatelé bezodkladně hlásili porušení zabezpečení (lze tak učinit ve zpracovatelské smlouvě), (ii) zajistil, aby všichni jeho zaměstnanci bezodkladně hlásili případy porušení (ztráty notebooků, výmaz dat, podezřelé aktivity v systémech apod. – lze tak učinit např. ve směrnici) odpovědné osobě a (iii) zajistil, aby odpovědná osoba zdokumentovala všechny případy porušení zabezpečení a tam, kde vznikne povinnost ohlásit ÚOOÚ či oznámit subjektům údajů, takto v daném čase učinila.

Když už zmiňujeme směrnici o ochraně osobních údajů, dovolíme si ještě upozornit, že nestačí mít vypracovanou směrnici, je také třeba zajistit, aby s ní všichni zaměstnanci byli seznámeni a aby jejímu obsahu porozuměli.

## Internet je zahlcen informacemi o GDPR, můžete se na ně spolehnout?

Odpovíme Vám následovně. Bolí Vás hlava. Zadáte si „bolest hlavy“ do vyhledávače a najdete nespočet odkazů na to, co by Vám mohlo být, a jak to léčit. Odpoví Vám ale opravdu přesně na otázky, co Vám je a jak to máte léčit? Budou tyto odpovědi opravdu správné a užitečné. Možná budete mít štěstí a najdete řešení svého zdravotního problému, možná (spíše) ale ne. Na první pohled rychlé a levné, případně zdarma, řešení, které Váš problém v dané chvíli vyřeší, se časem ukáže jako nesprávné a přinese Vám mnohem více komplikací. V důsledku Vás to tak bude stát více času i peněz, než kdybyste si na začátku došli k lékaři, který Váš stav odborně posoudí, zohlední všechny okolnosti a zvolí vhodnou léčbu.

Internet je zahlcen tolika informacemi, že vybrat ty správné je opravdu složité. S tím, jak se blížila účinnost GDPR (25. 5. 2018), objevilo se na webových stránkách velké množství informací. Bohužel, řada z nich byla a stále je nepřesná, zkreslená či úplně nesprávná. Současně, v případě, kdy naleznete solidní zdroj informací, jsou tyto informace buďto obecné, nebo jsou pro aplikaci na Vaši společnost úplně nevhodné, protože nezohledňují veškeré okolnosti.

Jako jeden z mála opravdu zaručených zdrojů proto doporučujeme sledovat stránky a na nich zveřejněná stanoviska ÚOOÚ (zejména výše zmíněnou část Dozorová činnost, kde možná natrefíte na případ podobný Vašemu) a Evropského sboru pro ochranu osobních údajů, který vznikl z původní pracovní skupiny WP29, a který i nadále zveřejňuje výkladová stanoviska k GDPR, tentokrát už závazná.

V souvislosti s prováděním auditů se velmi často setkáváme s tím, že společnosti používají různé právní dokumenty, včetně těch týkajících se GDPR, volně dostupných z internetu. Velmi oblíbené je to zejména u pracovních smluv či dohod o provedení práce / pracovní činnosti. Zdánlivě snadné a levné řešení se však může velmi prodražit. Tyto smlouvy jsou zde k dispozici již řadu let, neodpovídají často vůbec současné právní úpravě a možná ani té, ke které byly zveřejněny. Pamatujte, že i jedno nevhodně použité slovo může způsobit, že uzavřete pro Vaši společnost zcela nevýhodnou smlouvu, na kterou dříve či později můžete doplatit.

Autorky: Mgr. Lucie Demeterová, advokátka, Mgr. Kateřina Hakrová, advokátní koncipientka (DEMETER LEGAL, advokátní kancelář)

*(Právní prostor 5. 10. 2018)*

# Seznam akcionářů a GDPR

**Tzv. nařízení GDPR, které nahradilo stávající zákon o ochraně osobních údajů, se vedení seznamu akcionářů a záležitostí s ním souvisejících nijak zvlášť nedotklo. Podle stanoviska Úřadu pro ochranu osobních údajů ze dne 3. 1. 2018, č. j. UOOU-11100/17-2 totiž platí, že předávání osobních údajů akcionářů jiným akcionářům podle ustanovení § 266 z. o. k. je právní povinností akciové společnosti a GDPR nemá na tuto povinnost žádný vliv.**

Údaje zapsané v seznamu akcionářů je tak i nadále třeba považovat za **údaje osobní**[1] (čl. 4 odst. 1 GDPR). Předmětné nařízení tedy dopadá toliko na ochranu osobních údajů akcionářů (fyzických osob[2] neboli subjektů údajů, viz čl. 4 odst. 1 GDPR). Akcionářům (právnickým osobám) je pak možné (za určitých podmínek) poskytnout ochranu v režimu § 135 odst. 2 o. z.

Vzhledem k tomu, že vedení seznamu akcionářů odpovídá definici zpracování osobních údajů, jak je vymezena v čl. 4 odst. 2 GDPR, **je akciová společnost jejich správcem** ve smyslu legislativní zkratky uvedené v čl. 4 odst. 7 GDPR, čili na akciovou společnost dopadají příslušná ustanovení nařízení, která hovoří o správci osobních údajů (srov. zejména povinnost správce zavést vhodná technická a organizační opatření za účelem zajištění ochrany osobních údajů včetně jejich revize a aktualizací – čl. 24 odst. 1 GDPR).

**Zpracovávat osobní údaje akcionářů v souvislosti s vedením seznamu akcionářů (včetně vydávání opisů z něj) je možné bez souhlasu akcionářů**, neboť zpracování je v tomto případě nezbytné **pro splnění právní povinnosti**, která se na akciovou společnost coby správce vztahuje [čl. 6 odst. 1 písm. c) GDPR ve spojení s § 264 a násl. z. o. k.]. **Zpracování těchto osobních údajů není třeba (jak tomu bylo i za předchozí úpravy) nikomu oznamovat.**

Fyzická nebo právnická osoba (typicky ostatní akcionáři), orgán veřejné moci nebo jiný subjekt, kterým budou akciovou společností poskytnuty osobní údaje ze seznamu akcionářů (např. dle § 266 z. o. k.), budou jejich **příjemcem** (čl. 4 odst. 9 GDPR). Jestliže příjemce začne zpracovávat osobní údaje ze seznamu akcionářů, stane se správcem se všemi důsledky z tohoto vyplývajícími. Pokud by příjemce již jako správce následně zpracovával osobní údaje akcionářů v rozporu se zákonem, nejedná se o porušení zákona na straně akciové společnosti, která poskytla údaje při plnění své právní povinnosti.

**Soudím však, že pokud akcionář použije údaje z opisu seznamu akcionářů např. za účelem kontaktování ostatních akcionářů ohledně odkupu jejich akcií, zvolení strategie hlasování na nadcházející valné hromadě apod., byť půjde o zpracování osobních údajů ve formě použití těchto údajů, nebude k takovému použití souhlasu ostatních akcionářů třeba**, jelikož zpracování je v tomto případě nezbytné pro účely oprávněných zájmů příslušného správce (akcionáře), přičemž před těmito zájmy nemají přednost zájmy nebo základní práva a svobody subjektů údajů (ostatních akcionářů) [čl. 6 odst. 1 písm. f) GDPR].

O jinou situaci by šlo však již tehdy, pokud by akcionář chtěl tyto údaje použít např. **za účelem nabízení zboží a služeb ostatním akcionářům či zpřístupnit je třetí osobě za stejným účelem. K takovému zpracování osobních údajů akcionářů by již souhlas ve smyslu čl. 6 odst. 1 písm. a) GDPR nutný byl** (srov. § 266 odst. 2 z. o. k.). To platí také pro použití údajů ze seznamu akcionářů akciovou společností k jiným účelům než pro její potřeby ve vztahu k akcionářům, tj. k účelům které nijak nesouvisí se statusem dané osoby coby akcionáře společnosti (§ 267 odst. 1 z. o. k.).

**Sporné je, zdali se souhlas ostatních akcionářů se zpřístupněním jejich osobních údajů uvedených v seznamu akcionářů vyžaduje i v případě jejich poskytnutí potencionálnímu kupujícímu akcií v rámci kontraktačního procesu (§ 266 odst. 2 z. o. k.)**. Mám za to, že v těchto případech postačí ke zpracování osobních údajů prodávajícímu titul uvedený v čl. 6 odst. 1 písm. f) GDPR. **Je totiž jistě legitimním zájmem kupujícího být při prodeji akcií seznámen prodávajícím rovněž s akcionářskou strukturou dané společnosti, která dotváří obraz o kvalitě a kvantitě akcionářských práv a povinností spojených s převáděnými akciemi**. Bez těchto informací by např. prodávající nevěděl, jestli zcizovaný 40% balík akcií je vskutku ovládacím balíkem ve smyslu § 75 odst. 2 z. o. k. atd. **Soudím proto, že zpřístupnit tyto údaje půjde i bez souhlasu subjektů údajů.**

**Za zamyšlení rovněž stojí, jestli akciová společnost může (bez souhlasu subjektů údajů) sdělit údaje o akcionářích uvedené v seznamu akcionářů osobě, která činí veřejný návrh smlouvy na odkoupení nebo směnu účastnických cenných papírů.** Podle § 323 odst. 1 z. o. k. totiž platí, že navrhovatel (jímž může být právě osoba, která není akcionářem) uveřejní veřejný návrh

[1] Nikoliv však za osobní údaje citlivé (čl. 9 GDPR).
[2] Srov. recitál č. 14 GDPR.

smlouvy způsobem stanoveným zákonem o obchodních korporacích a stanovami společnosti, jejíž účastnické cenné papíry hodlá nabýt, pro svolání valné hromady. Vzhledem k tomu, že tyto údaje (zejména jméno a bydliště nebo sídlo akcionářů) mít navrhovatel k dispozici nemůže, musela by mu je akciová společnost vydat. V takovém případě by však šlo § 266 odst. 2 z. o. k. jednoduše obcházet. Stačilo by totiž, aby se navrhovatel (extraneus) obrátil na cílovou společnost se žádostí o sdělení těchto údajů pod záminkou, že veřejný návrh později spolu se stanoviskem cílové společnosti uveřejní. Takovou povinnost mu však zákon neukládá. Nakonec by navrhovatel mohl od záměru uveřejnění veřejného návrhu upustit a jednotlivé akcionáře kontaktovat v rozporu se zákonem individuálně. Otázkou tedy je, zdali by neměl být upřednostněn výklad, podle něhož by veřejný návrh měla uveřejňovat sama akciová společnost (pochopitelně na náklady navrhovatele). **Zdá se však, že zákonodárce implicitně počítá s tím, že společnost navrhovateli tyto údaje poskytne i bez souhlasu akcionářů.**

Akcionáři mají právo žádat akciovou společnost **o opravu nepřesných osobních údajů zapsaných v seznamu akcionářů, které se jich týkají, resp. o doplnění neúplných osobních údajů evidovaných v tomto seznamu (čl. 16 GDPR)**. Akcionářům náleží také (pokud jde o jejich osobní údaje zapsané v seznamu akcionářů) ostatní práva uvedená v kapitole III GDPR, jako je např. právo na poskytnutí informace o tom, jakým příjemcům[3] byly zpřístupněny jejich osobní údaje [čl. 15 odst. 1 písm. c) GDPR] včetně kupř. práva na náhradu újmy zakotveného v čl. 82 GDPR kapitola VIII či jiných práv nacházejících se na ostatních místech nařízení, pokud nařízení nestanoví výslovně jinak či pokud to nevylučuje povaha věci či zvláštní právní úprava (kupř. právě zákon o obchodních korporacích). Soudím např. že § 266 odst. 1 z. o. k. je lex specialis k čl. 15 odst. 3 a 4 GDPR.

Hovoří-li § 266 a § 267 odst. 1 z. o. k. o souhlasu akcionářů s poskytnutím údajů ze seznamu akcionářů, rozumí se jím souhlas ve smyslu čl. 4 odst. 11 GDPR, tj. jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů (akcionář) dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Podmínky vyjádření souhlasu (včetně možnosti jeho odvolání) jsou pak upraveny v čl. 7 GDPR.

Autor: Mgr. Vladimír Janošek (ARROWS)

*(www.epravo.cz 8. 10. 2018)*

[3] Akciová společnost by proto měla vést evidenci o tom, komu všemu poskytla např. opis seznamu akcionářů dle § 266 odst. 1 z. o. k. či údaje ze seznamu akcionářů podle § 266 odst. 2 z. o. k.

# Ochrana osobních údajů při poskytování platebních služeb a možné aplikační problémy Směrnice PSD2 ve světle GDPR

Nedávno vstoupilo v platnost Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“). V souvislosti s tím vyvstala otázka výkladu a aplikace některých dalších norem EU, kdy jednou z takových norem je právě směrnice č. 2015/2366, o platebních službách na vnitřním trhu (dále jen „PSD2“).

V tomto článku uvedeme některá problematická ustanovení a možná řešení případné kolize mezi PSD2 a GDPR s ohledem na stanovisko Evropské rady pro ochranu údajů[1].

## Problematika výslovného souhlasu

Po vstupu GDPR v platnost vyvstala problematika udělování a odvolávání souhlasu, přičemž jednou z hlavních otázek je, zda má termín „výslovný souhlas“ tak, jak je nastaven v čl. 94 odst. 2 PSD2, stejný význam, jaký je dáván tomuto termínu v rámci GDPR.

Evropská rada pro ochranu údajů (dále jen „EDPB“) zastává stanovisko, že „výslovný souhlas“ tak, jak je chápán směrnicí PSD2, je souhlasem smluvním, když platební styk je umožněn na základě smluvního vztahu mezi poskytovatelem a uživatelem platebních služeb. Tento názor pak posiluje také odst. 89 důvodové zprávy k PSD2.

V rámci GDPR je právním základem pro zpracovávání osobních dat článek 6 odst. 1 písm. b), který stanovuje, že zpracování osobních údajů je zákonné, pokud je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.

EDPB uvádí, že čl. 94 odst. 2 PSD2 má být interpretován v tom smyslu, že při uzavírání smlouvy s poskytovatelem platebních služeb musí být subjekty dat plně informovány o účelu zpracování osobních dat a s tímto zpracováním musí souhlasit. Ke splnění této podmínky pak poskytovatel může např. předkládat subjektům dat samostatné formuláře, ve kterých právě způsob a účel zpracování jejich osobních údajů uvede a který subjekt údajů odsouhlasí.

[1] Toto stanovisko je k dispozici zde.

Zvláště je třeba upozornit na to, že dle čl. 7 odst. 1 GDPR nese důkazní břemeno ohledně udělení souhlasu subjektem údajů poskytovatel, a musí být tedy schopen poskytnutí souhlasu subjektem údajů dokázat, jinak může dojít k udělení sankcí poskytovateli za porušení jeho povinností.

S ohledem na výše uvedené tak lze shrnout, že institut výslovného souhlasu dle čl. 94 odst. 2 PSD2 je pouze smluvního charakteru a neshoduje se s institutem výslovného souhlasu tak, jak je chápán v rámci GDPR.

## Údaje třetích stran

V souvislosti s GDPR vyvstala také otázka, zda je legitimní zpracovávání údajů třetích stran v případech, kdy byl výslovný souhlas (viz výše) dán jiným subjektem dat.

Typicky jde o situaci, kdy subjekt A jakožto subjekt údajů, který dal s jejich zpracováním souhlas, má smlouvu s poskytovatelem platebních služeb – subjektem B, jehož prostřednictvím uskutečňuje své platby. Ovšem v okamžiku, kdy subjekt A např. v obchodě zaplatí platební kartou, vydanou mu subjektem B, vstupuje do vztahu taktéž subjekt C – předmětný obchod. V této chvíli subjekt B zpracovává data nejen subjektu A, který mu udělil souhlas, ale taktéž subjektu C, který stojí mimo smluvní vztah mezi A a B, a žádný souhlas neudělil.

K uvedenému problému se EDPB staví tak, že ve smyslu odst. 47 důvodové zprávy k GDPR je takové zpracování dat možné v případech, kdy je dán legitimní zájem, a zároveň nejsou-li neproporcionálně porušena základní práva a svobody subjektů dat, přičemž musí být vzato v úvahu legitimní očekávání těchto subjektů dat jakožto třetích stran, zakládající se na jejich vztahu ke zpracovateli údajů.

Legitimní zájem je pak dán zejména tehdy, existuje-li mezi subjektem a zpracovatelem údajů relevantní vztah. Vždy je tak třeba posoudit, zda může subjekt údajů jakožto třetí strana důvodně očekávat, že v souvislosti se shromažďováním osobních údajů může být zpracování údajů uskutečněno. Pokud zde důvodné očekávání není, pak zájem na ochraně základních práv subjektu dat převáží nad legitimním zájmem zpracovatele.

V souladu s výše uvedeným tak lze dojít k závěru, že shromažďování dat jako takové není zakázáno, pokud se tak děje v souladu se zásadou proporcionality, omezení, minimalizace zásahu a transparentnosti.

## Regulační technické normy

Bezpochyby lze tedy říci, že mezi oběma předpisy dochází ke kolizi. Částečným vodítkem pro řešení těchto kolizí mohou být i tzv. Regulační technické normy, které byly vytvořeny na základě čl. 98 PSD2. Tyto normy poskytují pokyny pro autentifikaci a bezpečnou komunikace ve vztahu podnikatele a spotřebitele, a jsou tak klíčem k dosažení cíle PSD2 – posílení ochrany spotřebitele a podpora rozvoje ve vztahu k bezpečnosti platebních služeb napříč celou Evropskou unií.

## Závěr

Vstoupením GDPR v platnost bezpochyby došlo ke zvýšení požadavků a standardů, které byly stanoveny již v rámci PSD2. Jak již bylo uvedeno, poskytovatelům platebních služeb přibylo důkazní břemeno ohledně prokazování splnění jim ukládaných povinností. V souvislosti s tím bude třeba, aby každý poskytovatel platebních služeb pečlivě posoudil vzájemnou souvislost uvedených norem a přizpůsobil tomu svoje jednání tak, aby předešel potenciálnímu riziku v podobě sankcí hrozících za jejich porušení.

Vzhledem k tomu, že sankce dle GDPR mohou dosahovat výše až 20 milionů EUR nebo až 4 % ročního obratu, bude nepochybně lepší, pokud budou poskytovatelé obezřetní a v případě pochybností ohledně získávání souhlasu od subjektů dat budou postupovat způsobem, který je stanoven v Regulačních technických normách.

Autoři: Mgr. Petr Varvařovský, Alice Dajčarová (ARROWS)

*(www.epravo.cz 20. 9. 2018)*