BALCAR, POLANSKÝ & SPOL.

Březen – červen 2017

# Škola ochrany osobních údajů

*advokátní kanceláře Balcar, Polanský & Spol. s.r.o.*

---

*Nařízení EP a Rady (EU) 2016/679 z 27. dubna 2016, tzv. Všeobecné nařízení o ochraně údajů („Nařízení") zrušilo směrnici 95/46/ES („Směrnice"), která je nyní transformována do českého právního řádu zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Nařízení vstoupí v účinnost dnem 25. května 2018, kdy se stane přímo účinným rovněž v České republice a dotkne se všech, kteří osobní údaje zpracovávají, jakož i fyzických osob, jejichž osobní údaje jsou předmětem zpracování, tedy téměř každého.*

*Vzhledem k dosud nejvýznamnější legislativní změně evropského rozměru v oblasti ochrany osobních údajů Vám s týdenní frekvencí přinášíme pravidelné informace pro snadnější a efektivnější orientaci v množství povinností, které Nařízení přináší.*

---

*Lekce 1 z 16*

## Věcná a územní působnost Nařízení

**V textu se dozvíte:**

*Důležité změny*

- Bude mít podstatně širší dosah na ty, kteří údaje zpracovávají
- Bude se vztahovat i na společnosti / instituce, které nejsou usazené přímo v EU, pokud
  - budou zpracovávat osobní údaje dotčených osob, nacházejících se v EU v souvislosti s nabídkou zboží nebo služeb; anebo
  - půjde-li o sledování činnosti dotčených osob v rámci EU (např. prostřednictvím technických zařízení jako jsou *cookies*).

*Compliance: Akční plán*

- Společnosti / instituce by měly posoudit, zda se na ně nové Nařízení vztahuje
- Pokud ano, sledujte nás dále pro zjištění, jak zajistit *compliance* a minimalizovat riziko vysokých pokut
- Pokud ne, doporučujeme zavést průběžné monitorovací procesy na zajištění tohoto postavení v budoucnosti

### Věcná působnost

Nařízení se bude vztahovat na zpracovávání osobních údajů:

- prováděné zcela nebo částečně automatizovanými prostředky (prostřednictvím IT techniky), a na
- zpracovávání jinými než automatizovanými prostředky (např. záznamy v listinné podobě) v případě osobních údajů, které:
  - tvoří součást informačního systému (tj. databáze údajů), nebo
  - jsou určené k tomu, aby tvořily součást takové databáze.

Nařízení se nebude vztahovat na určité druhy zpracovávání, jako např. pro osobní a domácí účely, zpracovávání související s vnitřní bezpečností států EU atp.

Většina zpracovatelských operací ve veřejné a zejména v komerční sféře však bude Nařízení podléhat.

### Územní působnost

*Správci nebo zpracovatelé „usazení" v EU*

Nařízení se bude vztahovat v první řadě na fyzické i právnické osoby, které jsou „usazené" v EU, pokud v rámci své činnosti zpracovávají osobní údaje. Je to široce koncipované pravidlo zajišťující, aby se Nařízení vztahovalo jak na správce[1], tak i na zpracovatele[2] zpracovávající osobní údaje, jsou-li usazení v EU, a to bez ohledu na to, zda vlastní zpracovávání bude prováděno v Unii anebo mimo ni.

[1] ten, kdo sám nebo společně s jinými určí účel a prostředky zpracovávání osobních údajů
[2] ten, kdo zpracovává osobní údaje jménem správce

Novinkou je, že Nařízení rozšířilo svou působnost právě o zpracovatele, usazené v Unii. Podle stávající úpravy platí, že pokud správce není usazen v EU, avšak zpracováváním osobních údajů pověřil zpracovatele, který je v EU usazený, pak toto zpracovávání nepodléhá úpravě Směrnice.

Důležité přitom je, že koncept „usazení se" společnosti v Unii byl v poslední době přesněji definovaný rozhodnutími SD EU. Převratným v tomto ohledu je rozhodnutí SD EU ve věci *Weltimmo v. NAIH* z roku 2015 (C-230/14), které má význam zejména pro osoby podnikající prostřednictvím internetu ve více státech EU. Společnost Weltimmo měla sídlo na Slovensku, avšak přeshraničně poskytovala prostřednictvím internetu služby rovněž obyvatelům Maďarska. SD EU rozhodl, že slovenská společnost, přestože nemá pobočku ani jinou formu zastoupení v Maďarsku, podléhá pravomoci orgánu dohledu nad ochranou osobních údajů v Maďarsku. SD EU vyslovil, že pokud společnost nabízí služby v oficiálním jazyce země (v daném případě v maďarštině) a v dané zemi má zástupce – fyzickou osobu, v takovém případě podléhá kontrolní pravomoci orgánů dohledu v tomto státě bez ohledu na to, že není zapsaná v tamním obchodním rejstříku. Podle SD EU existence pobočky společnosti v určitém státě není nezbytným kritériem při určení, zda v něm společnost je nebo není usazená. Naopak, o usazení může jít tam, kde společnost vykonává byť jen minimální, avšak reálnou a efektivní činnost prostřednictvím např. webové stránky v místním jazyce, zástupcem operujícím na daném území, popř. má tam poštovní adresu nebo bankovní účet, jako tomu bylo v případě Weltimmo.

### *Společnosti neusazené v EU*

Rozšíření územní působnosti Nařízení rovněž i na ty společnosti, které nejsou usazené v členském státě EU, avšak zpracovávají osobní údaje dotčených osob nacházejících se v Unii, je jednou z nejvýznamnějších změn, které Nařízení přináší. Pokud takové společnosti nebo instituce se sídlem mimo EU budou splňovat jednu ze stanovených podmínek, automaticky se na ně bude Nařízení vztahovat. Budou muset dodržovat principy zpracovávání a zavést opatření k zajištění ochrany osobních údajů, stanovených Nařízením, budou podléhat určeným orgánům dozoru a budou muset strpět jimi uložené sankce.

Nařízení se bude vztahovat na mimoevropské společnosti, pokud budou zpracovávat osobní údaje dotčených osob v Unii a pokud jejich zpracovatelská činnost bude souviset:

- s nabídkou zboží nebo služeb dotčeným osobám bez ohledu na to, zda se požaduje platba, anebo
- se sledováním jejich činnosti, pokud půjde o aktivity na území Unie.

Co se rozumí „dotčenými osobami, nacházejícími se v Unii", není zatím zcela jasné. Dá se však předpokládat, že půjde o široký koncept a bude tendence vykládat jej tak, aby zahrnul co nejvíce dotčených osob pod „deštník" ochrany, kterou chce Nařízení poskytnout. Směrodatným při výkladu tohoto pojmu by mohlo být místo fyzické přítomnosti a místo pobytu dotčené osoby.

Poprvé je působnost Nařízení založená na faktu, zda společnost sleduje činnost dotčených osob na území Unie. O sledování půjde nejčastěji prostřednictvím internetu za použití malých textových souborů zasílaných těmi, kteří získávají údaje, do zařízení dotčené osoby (počítač, smartphone atd.), tzv. *cookies.*

Za předchozí právní úpravy podle Směrnice se orgány dozoru snažily založit svou pravomoc vykonávat dohled nad mimoevropskými podniky, zpracovávajícími osobní údaje obyvatel Unie, za pomoci ustanovení, podle něhož společnosti využívaly technická zařízení nacházející se na území EU na zpracovávání osobních údajů, přičemž za technické zařízení se považovaly právě *cookies*. Tyto snahy se nyní nahradí jednoznačným ustanovením o aplikovatelnosti Nařízení v případě, že společnost bude sledovat činnost dotčených osob v Unii. Relevantní přitom bude také další zpracovávání např. profilování, kterým se rozumí jakákoliv forma automatizovaného zpracovávání osobních údajů, jímž se sleduje analýza anebo předvídání aspektů souvisejících s pracovní výkonností, majetkovými poměry, zdravím, osobními preferencemi, zájmy, spolehlivostí, chováním, polohou nebo pohybem.

Při určení, zda se mimoevropská společnost považuje za usazenou v Unii, budou určující kritéria, stanovená výše uvedeným rozhodnutím SD EU ve věci *Weltimmo*. To znamená, že například samotná skutečnost, že určitou webovou stránku je možno otevřít ze země EU, nebude stačit k závěru o existenci usazení v Unii. Musí být prokázáno, že aktivity společnosti mají být zaměřené na dotčené osoby v EU. Pokud by například stránky existovaly v některém z místních jazyků států EU, obsahovaly ceny v měnách států EU (např. EUR, GBP, CZK), nebo kontaktní údaje (např. telefonní čísla) s evropskými předvolbami, tyto okolnosti by byly relevantní pro závěr o usazení společnosti v Unii.

Do jaké míry bude dohled evropských orgánů dozoru nad společnostmi mimo Unii efektivní, nebylo zatím testováno; reálná vykonatelnost rozhodnutí mimo EU (např. rozhodnutí Úřadu na ochranu osobních údajů ČR o uložení pokuty společnosti se sídlem v Číně) zůstává otevřenou otázkou. Uvedený koncept ochrany dotčených osob v Unii vůči společnostem mimo EU je však přelomový. Důvodem pro jeho zavedení bylo přesvědčení, že dotčené osoby v EU by neměly být zbaveny ochrany při zpracovávání svých osobních údajů jen proto, že společnost si zřídí sídlo mimo EU.

### *Co dále*

Na začátek by společnost nebo instituce měla zjistit, zda se na ni bude Nařízení vztahovat vzhledem k rozšířené územní působnosti. Pro mimoevropské společnosti se doporučuje obezřetnost při zjišťování, zda se považují za „usazené" v EU.

Pokud budou aktivity společnosti nebo instituce spadat do působnosti Nařízení, bude třeba se seznámit s četnými povinnostmi, stanovenými Nařízením a seznámit s nimi také osoby, které budou jménem společnosti nebo instituce nakládat s osobními údaji. Povinnosti provozovatelů a práva dotčených osob, jakož i principy zpracovávání osobních údajů, budou obsahem dalších lekcí Školy ochrany osobních údajů.

### *Další informace*

| | |
|---|---|
| Věcná působnost: | Recitály 6-18 Nařízení; článek 2 Nařízení |
| Územní působnost: | Recitály 22-24 Nařízení; článek 3 Nařízení |

*Lekce 2 z 16*

## Zásady ochrany osobních údajů

**V textu se dozvíte:**

*Důležité změny*

- V důsledku nově zavedené zásady odpovědnosti budou společnosti/instituce zpracovávající si samy osobní údaje (správci) povinny nejen dodržovat, ale také prokázat, že osobní údaje zpracovávají v souladu se zásadami ochrany osobních údajů

*Compliance: Akční plán*

Správci by měli před nabytím účinnosti Nařízení:

- provést audit zpracovávání osobních údajů, zaměřený na nové povinnosti;
- vytvořit (resp. aktualizovat existující) vnitřní předpisy upravující zpracovávání, aktualizovat pracovní řád v rozsahu monitorování zaměstnanců a ochrany jejich osobních údajů, zrevidovat pracovní smlouvy zaměstnanců oprávněných zpracovávat osobní údaje a všechny ostatní dokumenty týkající se zpracovávání;
- zajistit a moci prokázat vyškolení svých zaměstnanců, kteří mají přístup k osobním údajům, ohledně jejich práv a povinností a poučit je o následcích porušení jejich povinností.

**K zásadám ochrany osobních údajů**

Zásady ochrany osobních údajů ve smyslu Nařízení jsou podobné těm, které upravovala Směrnice a které jsou obsaženy také v aktuálním znění zákona č. 101/2000 Sb., o ochraně osobních údajů. Nařízení je však podrobněji specifikuje a rozšiřuje.

*Zákonnost, korektnost, transparentnost*

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem.

Pro účely splnění podmínky transparentnosti se společnosti / instituce budou muset vypořádat s povinností poskytnout subjektům údajů, jejichž osobní údaje zpracovávají, rozsáhlý balík informací. Subjekty údajů by měly být dostatečně jasně a srozumitelně informovány o podmínkách zpracovávání a o právech, která mají v této souvislosti.[3]

Seznam informací, které budou správci povinni prokazatelně oznámit subjektům údajů před zahájením zpracovávání, je v porovnání se Směrnici podstatně širší a zahrnuje kromě jiného právo na vymazání (tj. „právo být zapomenut“[4]), právo napadnout zpracovávání nebo podat stížnost orgánu dohledu nebo právo, aby se na subjekt údajů nevztahovalo rozhodnutí založené výhradně

[3] Za nelegitimní zpracovávání je z logiky věci považováno utajené a neviditelné instalování spywaru (viz případ provozovatele webových stránek, který zveřejňoval e-mailové adresy účastníků internetové diskuse; WP 29 - Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováváním osobních údajů (čl. 29)

[4] Dosud pouze judikatorně zakotveno SDEU, viz věc C-131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Spor mezi skupinou Google a P. Gonzálezem, který si přál vymazat z veřejného povědomí nepříjemnou epizodu, kdy byla v tisku zveřejněna informace o nuceném prodeji jeho nemovitosti z důvodu nesplaceného dluhu na sociálním pojištění, který byl následně splacen. Španělský úřad nařídil společnosti Google Inc., aby přijala opatření nezbytná k odstranění osobních údajů týkajících se p. Gonzáleze ze svého indexu a zabránila přístupu k těmto údajům v budoucnosti.

na automatizovaném zpracovávání včetně profilování[5]. Subjekty údajů musí být také vedle poučení o jejich právech informovány o specifické povaze zpracovávání včetně toho, k jakým účelům se údaje budou zpracovávat a na jakém právním základě (např. souhlas, zákonné ustanovení apod.). Oznamovací povinnosti se budeme podrobněji věnovat v samostatné lekci.

### *Účelové omezení*

Osobní údaje musí být získávány ke konkrétně určeným, výslovně uvedeným a legitimním účelům a nesmí se dále zpracovávat způsobem, který je s těmito účely neslučitelný[6]. Další zpracovávání za jiným účelem, než pro který byly osobní údaje získány, bude oproti stávající úpravě za určitých podmínek již dovolené. Toto je podstatná změna v českých podmínkách zpracovávání a znamená, že i když správce získá osobní údaje ke konkrétnímu účelu, za splnění určitých podmínek může tyto údaje zpracovávat i k jiným než původním účelům.

Další zpracovávání pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu nebo pro statistické účely se ve smyslu Nařízení nepovažuje za neslučitelné s původním účelem, za předpokladu, že zpracovatel zajistí přiměřené záruky pro práva a svobody subjektů údajů. Správce resp. zpracovatel by měl zavést technická a organizační opatření, která mohou zahrnovat minimalizaci údajů, pseudonymizaci[7] či anonymizaci.

Za neslučitelné s primárním účelem tak bude podle našeho názoru nadále považováno zpracovávání osobních údajů shromážděných při projednávání přestupku k sekundárnímu účelu, kterým bude např. zveřejnění v místním periodiku nebo prostřednictvím internetu, anebo zveřejnění údajů o existenci dluhů majitele bytu, zpracovávaných primárně v souvislosti se správou bytového domu, anebo zpřístupnění shromážděných osobních údajů jednotlivých účastníků zájezdu bez jejich souhlasu všem ostatním cestujícím, aj.

### *Minimalizace údajů*

Osobní údaje musí být přiměřené, relevantní a omezené na rozsah, který je nezbytný vzhledem k účelům, ke kterým se zpracovávají.

Přiměřenost osobních údajů ve vztahu k účelu zpracovávání není vždy jednoznačně určitelná. Zjištění, zda je zpracovávání konkrétních osobních údajů přiměřené, bude vyžadovat posouzení, zda je zásah do práv subjektu údajů, ke kterému v důsledku zpracování dojde, přiměřený legitimnímu účelu zpracovávání. Pokud se zpracovávání konkrétního osobního údaje k určitému účelu ukáže jako nadbytečné, nebude takové zpracovávání v souladu s Nařízením. Nepřiměřené by bylo např. zpracovávání rodného čísla osoby k marketingovým účelům, jelikož k těmto účelům není nezbytné tento údaj zpracovat.

### *Přesnost*

Osobní údaje musí být přesné a podle potřeby aktualizované. Správce je povinen zajistit, aby se osobní údaje, které jsou nepřesné, bezodkladně vymazaly nebo opravily.

---

[5] Viz čl. 4 odst. 4 Nařízení, tj. „jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;".

[6] Tzn., že jde o obecný zákaz dalšího zpracovávání pro sekundární účely, neslučitelné s primárním účelem, přičemž „slučitelností" se rozumí „přímá souvislost" s primárním účelem.

[7] Viz čl. 4 bod 5) Nařízení, tj. zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;".

### *Minimalizace uchovávání*

Osobní údaje musí být uchovávány v podobě, která umožňuje identifikaci subjektů údajů nejdéle po dobu, po kterou je to potřebné k účelům, ke kterým se údaje zpracovávají.

Osobní údaje se mohou uchovávat déle, pokud se budou zpracovávat výhradně pro účely archivace ve veřejném zájmu, pro vědecký nebo historický výzkum nebo pro statistické účely za předpokladu přijetí přiměřených technických a organizačních opatření požadovaných Nařízením k ochraně práv a svobod subjektů údajů.

Nadále tak bude platné stanovisko českého ÚOOÚ, že při provozování kamerového systému u trvale střeženého soukromého objektu je přípustným časovým limitem např. doba 24 hod., v zásadě však nepřesahující několik dnů. Omezení se však neuplatní při pořízení záznamů Policií ČR podle zvláštního zákona nebo v případě bezpečnostního incidentu, kdy záznam bude poskytnut jako důkaz příslušným orgánům pro další řízení.

### *Integrita a důvěrnost*

Osobní údaje musí být zpracovávány způsobem, který zaručuje přiměřenou bezpečnost osobních údajů, včetně ochrany před neoprávněným nebo nezákonným zpracováváním a náhodnou ztrátou, zničením nebo poškozením, a to pomocí přiměřených technických nebo organizačních opatření.

### *Odpovědnost*

Správce je odpovědný za zpracovávání osobních údajů v souladu s výše uvedenými zásadami a musí být schopen tento soulad také prokázat. K prokázání souladu je možno např. vypracovat písemné podklady o tom, že všechny aspekty zpracovávatelských operací v rámci společnosti či instituce byly interně posouzeny a výsledkem tohoto posouzení je soulad s ustanoveními Nařízení.

Nařízení zavádí nový koncept ochrany osobních údajů, a to specificky navrženou („*data protection by design*“) a standardní („*data protection by default*“) ochranu osobních údajů.

Specificky navržená ochrana osobních údajů znamená, že správce je před začátkem zpracovávání povinen, se zřetelem na různé aspekty zpracovávání (např. nejnovější poznatky, povahu, rozsah a účel zpracovávání, rizika pro práva subjektů údajů), přijmout přiměřená technická a organizační opatření a záruky na ochranu osobních údajů a tyto přiměřeně přizpůsobit aktuálním podmínkám zpracovávání. Tento koncept tedy zavazuje všechny společnosti / instituce zpracovávající osobní údaje, aby provedly vnitřní audit zpracovávání osobních údajů. Je nezbytné, aby se ochranou osobních údajů aktivně zabývaly, vyčlenily lidské, finanční a technické zdroje pro účely posouzení zákonnosti zpracovávání a zavedly opatření na jejich ochranu.

Standardní ochrana osobních údajů znamená, že správce zajistí, aby se zpracovávaly pouze osobní údaje nezbytné pro každý konkrétní účel zpracovávání. Je též povinen zajistit, aby osobní údaje nebyly bez zásahu fyzické osoby běžně dostupné neomezenému počtu fyzických osob.

Pokud správce zpracovává osobní údaje prostřednictvím třetí osoby – zpracovatele, je tento oprávněn zpracovávat osobní údaje pouze na základě pokynů správce s výjimkou případů, kdy je to vyžadováno unijním právem nebo právem členského státu.

### *Co dále*

Společnosti / instituce, kterých se to týká, jsou povinny provést audit zpracovávání osobních údajů a zajistit jednak soulad, ale také možnost prokázání, že osobní údaje zpracovávají zákonně a s odbornou péčí, a k tomuto účelu přijmout organizační a technická opatření a záruky. Návrhy na zajištění uvedeného najdete výše v části *Compliance*.

*Další informace*

Recitály 39, 40, 22

Články 5, 6, 24, 25, 29, 89 odst. 1

*Lekce 3 z 16*

## Zákonnost zpracovávání a dalšího zpracování

**V textu se dozvíte:**

*Důležité změny*

- Nařízením se mění okruh právních základů zpracování osobních údajů
- V určitých případech bude zpracovávání k jinému účelu, než k jakému byly osobní údaje původně získány, přípustné
- Zavádějí se kritéria testu kompatibility účelu zpracovávání

*Compliance: Akční plán*

- Kontrola právních základů zpracovávání osobních údajů a zajištění, aby tituly byly aktuální i po nabytí účinnosti Nařízení
- Zajištění prokazatelnosti provedení testu kompatibility, pokud se osobní údaje zpracovávají k jinému než původnímu účelu

### K zákonnosti zpracování

Jak jsme uvedli v Lekci 2, jednou ze zásad zpracovávání osobních údajů je zákonný způsob zpracovávání[8]. Pojem „zákonný způsob" je značně široký a bez dalšího upřesnění vágní a právně neurčitý. Nařízení ho proto blíže upravuje v článku 6.

Podmínka zákonnosti stanoví, že pokud se na zpracovávání nevztahuje některá z výjimek upravených Nařízením, je správce vždy povinen mít souhlas subjektu údajů se zpracováním. Kromě souhlasu subjektu údajů, který je základním právním titulem zpracování (budeme se mu věnovat v samostatné lekci), je tedy zpracování zákonné pouze tehdy a v takovém rozsahu, je-li splněna alespoň jedna z těchto dalších podmínek (tzv. právní základ zpracovávání),[9] kdy zpracování je nezbytné pro:

a) splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů[10];

b) splnění právní povinnosti, která se na správce vztahuje[11];

c) ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby[12];

d) splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce[13];

---

[8] Čl. 5 odst. 1 písm. a) Nařízení: *Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem.*

[9] Zákonnosti zpracování citlivých osobních údajů se budeme věnovat v samostatné lekci.

[10] Např. spotřebitel si objedná zboží v on-line obchodě, prodávající musí pro účely doručení zpracovat jeho jméno, příjmení, adresu, případně jiný kontaktní údaj.

[11] Základ pro zpracovávání musí být stanovený buď unijním právem, nebo právem členského státu vztahujícím se na správce. Takový právní předpis může upravovat konkrétní okolnosti zpracovávání, jako jsou všeobecné podmínky vztahující se na zákonnost zpracovávání správcem, druhy zpracovávaných údajů, subjekty údajů, subjekty, kterým se mohou osobní údaje poskytnout, účely, ke kterým je možné je poskytnout, omezení účelu, doby uchovávání, zpracovatelské operace a postupy včetně opatření k zabezpečení zákonného a korektního zpracovávání.

[12] Zpracovávání osobních údajů k účelům životně důležitého zájmu jiné fyzické osoby by se mělo uskutečnit pouze tehdy, kdy takové zpracovávání nelze založit na jiném právním základě.

[13] Viz pozn. 4.

e) účely oprávněných zájmů příslušného správce nebo třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě[14].

V podmínkách obchodních společností bude kromě souhlasu subjektu údajů relevantní zejména právní základ zpracovávání uvedený v bodech a), b) a e) výše.

Nařízení umožňuje státům stanovit další konkrétní požadavky a zavést opatření pro zpracování z důvodů, uvedených pod písm. b) a d) shora. Totéž je umožněno i v dalších zvláštních situacích, kdy dochází ke zpracování.[15]

Právními základy zpracování osobních údajů po nabytí účinnosti Nařízení tak budou rovněž:

- v návaznosti na čl. 85 Nařízení zpracování osobních údajů nezbytné pro účely akademické, umělecké, literární nebo žurnalistické, pokud to pro správce vyplývá z předmětu jeho činnosti, s výjimkou případů, kdy by takové zpracování porušilo právo subjektu údajů na ochranu osobnosti a soukromí nebo by takové zpracování bez souhlasu subjektu údajů bylo v rozporu se zvláštním zákonem nebo mezinárodní smlouvou, kterou je Česká republika vázána;
- v návaznosti na čl. 88 Nařízení zpřístupnění, poskytování nebo zveřejnění osobních údajů v rozsahu titul, jméno, příjmení, pracovní, služební nebo funkční zařazení, odborný útvar, místo výkonu práce, telefonní číslo, faxové číslo nebo adresa elektronické pošty na pracoviště a identifikační údaje zaměstnavatele, je-li správce zaměstnavatelem subjektu údajů;
- v návaznosti na čl. 87 Nařízení možnost využití pro účely určení fyzické osoby národní identifikační číslo, určené zvláštním zákonem, pouze v případech, kdy je jeho použití nezbytné pro dosažení daného účelu zpracování a zároveň poskytl-li subjekt údajů písemný nebo jinak průkazný souhlas s jeho zpracováním;
- v návaznosti na čl. 89 Nařízení zpracovávání pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely;
- v návaznosti na čl. 49 odst. 5 Nařízení oprávnění uskutečnit přenos zvláštní kategorie osobních údajů a všeobecně použitelného identifikátoru třetí straně se sídlem ve třetí zemi, která nezaručuje přiměřenou úroveň ochrany osobních údajů, pouze s předchozím výslovným souhlasem subjektu údajů, nestanoví-li zvláštní zákon jinak;
- v návaznosti na čl. 9 odst. 4 Nařízení zpracování genetických údajů, biometrických údajů a údajů o zdravotním stavu, je-li to nezbytné pro splnění zákonné povinnosti správce.

Uvést ochranu osobních údajů do souladu s právem na svobodu projevu a informací bude vždy povinností států i v takových zvláštních případech.

Povinností také bude oznámit Komisi, do data nabytí účinnosti Nařízení, podrobnější pravidla, odchylky a výjimky pro zpracování osobních údajů pro novinářské účely a účely akademického, uměleckého či literárního projevu, pro zpracování v souvislosti se zaměstnáním a v souvislosti se zákonnou povinností mlčenlivostí.

### *Zrušované právní základy*

V porovnání s aktuální právní úpravou[16] („zákon“) budou dnem účinnosti Nařízení zrušeny následující právní základy zpracování:

[14] Existence oprávněného zájmu vyžaduje důkladné posouzení včetně toho, zda subjekt údajů může v daném čase a kontextu získávání osobních údajů přiměřeně očekávat, že se zpracovávání k tomuto účelu může uskutečnit. Zájmy a základní práva subjektu údajů by mohly převážit nad zájmy správce zejména tehdy, kdy se osobní údaje zpracovávají za okolností, kdy subjekty údajů přiměřeně neočekávají další zpracovávání.
[15] Viz kapitola IX Nařízení

- právní základ podle § 5 odst. 5 zákona, za účelem nabízení obchodu nebo služeb subjektu údajů, pokud byly údaje získané z veřejného seznamu nebo v souvislosti s činností správce, a předání těchto údajů jinému správci za splnění zákonem stanovených podmínek.

**K zákonnosti dalšího zpracovávání**

Jak jsme uvedli v Lekci 2, další ze zásad zpracovávání osobních údajů je zásada omezení účelu. Ukládá správcům povinnost získávat údaje pro konkrétní, výslovně určený a legitimní účel a zakazuje jim zpracovávat osobní údaje v rozporu s takto určeným účelem.[17] Nařízení však ustanovením čl. 6 odst. 4 dovoluje, aby se osobní údaje za určitých podmínek zpracovávaly také pro jiný než původní účel (tzv. další zpracování). Jedná se o zpracovávání pro jiný, ale s původním účelem kompatibilní účel na stejném právním základě (tj. účel zpracovávání se mění, právní základ nikoliv).

Uvedeným ustanovením Nařízení se „vnáší světlo" do šedé zóny, která existovala v otázce dalšího zpracovávání v podmínkách předchozí právní úpravy. Nařízení výslovně upravuje, že další zpracovávání pro tzv. privilegované účely (tj. archivace ve veřejném zájmu, vědecký nebo historický výzkum nebo statistické účely) se nepovažuje za neslučitelné s původním účelem, pokud správce zajistí přiměřené záruky pro práva a svobody subjektu údajů.[18] Kromě toho Nařízení upravuje také pravidla týkající se kritérií, která správci musí vzít v potaz při zjišťování, zda je nový účel slučitelný s účelem, pro který byly údaje původně získané.

Pokud tedy správce zvažuje, zda může osobní údaje zpracovávat také pro jiný účel, je povinen provést tzv. test kompatibility účelů zpracovávání. Test kompatibility se provede podle konkrétně stanovených podmínek, kterými jsou:

- jakoukoliv vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;
- okolnosti, za nichž byly osobní údaje shromážděny (zejména pokud jde o vztah mezi subjekty údajů a správcem);
- povaha osobních údajů (zejména zda jsou zpracovávány zvláštní kategorie osobních údajů nebo osobní údaje týkající se rozsudků v trestních věcech);
- možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;
- existence vhodných záruk (např. šifrování nebo pseudonymizace).

Nařízení uvedená kritéria uvozuje slovním spojením „mimo jiné", což znamená, že pro účely testu kompatibility je možno zvážit ještě další vhodná kritéria. Pokud je však zpracovávání pro původní účel založeno na souhlasu subjektu údajů nebo na zvláštním právním předpisu (upravujícím např. veřejný zájem, národní bezpečnost apod.), měl by správce mít možnost dalšího zpracování osobních údajů bez ohledu na slučitelnost účelů.

Výše uvedené podmínky pro přípustnost dalšího zpracování se vztahují pouze na původního správce. Pokud by zpracováním mělo dojít k poskytnutí osobních údajů jinému správci, tento by musel rovněž disponovat právním základem pro takovéto zpracování. Správce je zároveň povinen s předstihem informovat subjekt údajů o případném dalším zpracování.

---

[16] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[17] Čl. 5 odst. 1 písm. b) Nařízení: *Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.*

[18] Správce by k tomuto účelu měl zavést technická a organizační opatření, která mohou zahrnovat minimalizaci údajů, pseudonymizaci nebo anonymizaci.

*Co dále*

Ve výše uvedeném smyslu je třeba, aby si společnosti a instituce před účinností Nařízení ověřily, že zpracovávají osobní údaje na základě právních titulů, upravených Nařízením.

Pro účely zajištění zákonnosti dalšího zpracovávání bude rovněž nutné provést test kompatibility podle stanovených kritérií.

*Další informace*

Recitály 40, 41, 44 - 47, 50, 153, 155

Články 5 odst. 1 písm. a) a b), 6, 23 odst. 1, kapitola IX (články 85 – 91)

*Lekce 4 z 16*

## Souhlas se zpracováním osobních údajů
## Zpracovávání osobních údajů nezletilých

**V textu se dozvíte:**

*Důležité změny*

- Nařízení přináší nové požadavky na udělení souhlasu se zpracováním osobních údajů
- Zvláštní požadavky jsou kladeny na zpracování osobních údajů v souvislosti s vědeckým výzkumem a osobních údajů nezletilých[19]

*Compliance: Akční plán*

- Společnosti/instituce by měly zajistit, aby osobní údaje zpracovávaly na základě přesných a existujících právních základů
- Jsou-li osobní údaje zpracovávány na základě souhlasu, je nutné především zajistit, aby:
    - souhlas byl dán aktivním úkonem subjektu údajů, nikoliv mlčením, nečinností anebo dopředu označenými políčky;
    - souhlas byl odlišitelný od dalších ustanovení, byl konkrétní a jasný;
    - subjekty údajů byly informovány o možnosti udělený souhlas odvolat a odvolání bylo stejně jednoduché jako jeho udělení;
    - poskytnutí služeb nebylo podmíněné souhlasem se zpracováním údajů, které nejsou nezbytné;
    - zvláštní souhlas byl udělen k zvláštním zpracovatelským operacím;
    - souhlas nebyl udělen za podmínek zjevné nerovnováhy mezi postavením správce a subjektu údajů (např. v případě orgánu veřejné moci)

**K souhlasu se zpracováním osobních údajů**

Jak jsme uvedli v Lekci 3, pokud se na zpracovávání osobních údajů nevztahuje žádná z výjimek uvedených v Nařízení, správce musí vždy disponovat souhlasem subjektu údajů se zpracováním. Nařízení definuje souhlas jako jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením svolení ke zpracování svých osobních údajů.[20]

Podle současné české právní úpravy[21] je souhlas definovaný jako svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu se zpracováním osobních údajů. Nová právní úprava tedy oproti současné výslovně stanoví, že souhlas bude moci být udělen také konkludentně (např. určitým jednáním, ale nikoliv nejednáním), avšak svobodně, konkrétně, jednoznačně a na základě úplných a srozumitelných informací, poskytnutých subjektu údajů. K zpracování citlivých osobních údajů bude však požadován výslovný souhlas subjektu údajů (pokud nebude stanovena jiná výjimka).

---

[19] Nařízení užívá pojem „dítě", my používáme pojem „dítě" a „nezletilý" zaměnitelně, ve shodném významu.
[20] Čl. 4 odst. 11 Nařízení
[21] § 4 písm. n) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

*Náležitosti udělení souhlasu*

Nařízení stanoví, že správce musí být schopen prokázat, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů. Jinými slovy, důkazní břemeno prokázání, že souhlas byl dán a že byl udělen platně, spočívá na správci. Formální i obsahové podmínky platnosti udělení souhlasu upravuje Nařízení v čl. 7 takto:

- *Svoboda projevu, určitost, informovanost, jednoznačnost:* souhlas vyžaduje jasný projev vůle, který je svobodným, konkrétním, informovaným a jednoznačným vyjádřením subjektu, že souhlasí se zpracováním svých osobních údajů.

  K zajištění, že souhlas byl poskytnut svobodně, by se správce neměl spolehnout na souhlas za situace, je-li mezi jeho postavením a postavením subjektu údajů jednoznačný nepoměr, zejména pokud je správcem orgán veřejné moci, a je proto nepravděpodobné, že za všech okolností dané konkrétní situace byl souhlas udělen svobodně.

  Za svobodně udělený souhlas se nepovažuje, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo jej odvolat, aniž by byl poškozen.

  Zásada informovanosti vyžaduje, aby si byl subjekt údajů vědom, že souhlas dává a v jakém rozsahu a měl by také znát identitu správce a účel zpracování.

- *Uvedení konkrétního účelu:* souhlas se musí vztahovat na všechny zpracovatelské činnosti prováděné za týmž účelem nebo účely; pokud se zpracovávání děje za více účely, souhlas má být udělen, resp. má být daný ke každému z nich samostatně, aby byla zachována reálná možnost subjektu údajů odmítnout souhlas pro kterýkoliv z uvedených účelů.

  Souhlas se nepovažuje za svobodně udělený, pokud jej nelze udělit samostatně k jednotlivým zpracovatelským operacím, i když je to v konkrétním případě vhodné.

  V praxi nebude tedy přijatelný „plošně" udělený souhlas, slučující různé nesouvisející účely zpracování.

- *Odlišitelnost, jasnost, jednoduchost*: pokud je souhlas udělován v rámci písemného prohlášení, které se týká rovněž dalších skutečností, žádost o vyjádření souhlasu musí být předložená tak, aby byla snadno odlišitelná od jiných skutečností, a musí být formulována jasně a jednoduše; porušení tohoto ustanovení má za následek neplatnost udělení souhlasu.

  V praxi to bude znamenat, že část dokumentu obsahujícího žádost o souhlas bude muset být oddělená, např. od smluvních ujednání, textu objednávek, prohlášení, atd.

- *Srozumitelnost, dostupnost:* souhlas má být formulovaný v srozumitelné a snadno přístupné formě, jasně a jednoduše.

  Tento požadavek může být zvlášť těžko splnitelný zejména vzhledem k rozsahu informací, které je správce povinný subjektu údajů poskytnout (více k informační povinnosti správce v samostatné lekci).

- *Odvolatelnost:* odvolání souhlasu musí být stejně jednoduché, jako jeho poskytnutí; o možnosti kdykoliv souhlas odvolat musí být subjekt údajů informován před jeho poskytnutím.

  V praxi se bude od společností a institucí požadovat, aby umožnily odvolání souhlasu stejným způsobem, jakým byl souhlas udělen (např. webová stránka, e-mail, nastavení ochrany soukromí v aplikaci apod.). Nařízení stanoví, že odvolání souhlasu nemá vliv na zákonnost zpracování, založeného na souhlasu před jeho odvoláním (t.j. zákaz retroaktivity); o tom by měly být subjekty údajů před udělením souhlasu rovněž informované.

- *Zákaz nepatřičného podmiňování:* plnění ze smlouvy nesmí být podmíněné souhlasem se zpracováváním osobních údajů, které není nezbytné k plnění smlouvy (např. splnění kupní

smlouvy uzavřené on-line nesmí být vázané na souhlas se zpracováním osobních údajů k marketingovým účelům). V opačném případě by existovala důvodná pochybnost o svobodném projevu vůle, a tedy o platnosti souhlasu.

Souhlas se nepovažuje za svobodně udělený, pokud se plnění ze smlouvy včetně poskytnutí služby podmiňuje udělením tohoto souhlasu, i když takový souhlas není pro toto plnění nezbytný.

Recitál 32 Nařízení stanoví, že souhlas může být vyjádřen například písemným prohlášením, včetně elektronickými prostředky, nebo ústně. Souhlas je možné udělit i jinak než výslovně, a to např. označením políčka při návštěvě internetového webového sídla (princip *opt-in*), zvolením technického nastavení služeb informační společnosti (např. nastavením pravidel ochrany osobních údajů na sociálních sítích) nebo jakýmkoli jiným prohlášením či úkonem, který v daném kontextu jasně znamená, že subjekt souhlasí s navrhovaným zpracováváním osobních údajů. Mlčení, dopředu označená políčka nebo nečinnost se za souhlas nepovažují.

### *Souhlas pro účely vědeckého výzkumu*

Nařízení připouští, že pokud se mají osobní údaje zpracovávat pro účely vědeckého výzkumu, často není možné v době získávání údajů v úplnosti určit účel zpracování. Proto se subjektům údajů umožňuje udělit souhlas jen pro určité oblasti výzkumu, budou-li dodržené uznávané etické normy vědeckého výzkumu. Subjekty údajů by měly mít možnost také omezit svůj souhlas pouze na určité oblasti výzkumu nebo na části výzkumných projektů v rozsahu, který umožňuje zamýšlený účel.

Vyslovení souhlasu s účastí ve vědeckém výzkumu v klinických hodnoceních se bude řídit zvláštním nařízením.[22]

## K zpracování osobních údajů nezletilých

Nařízení na více místech upravuje specifické podmínky pro zpracovávání osobních údajů nezletilých. Konkrétně v recitálu 38 stanoví, že zvláštní ochranu osobních údajů si zasluhují děti, neboť si jsou méně vědomy rizik, důsledků, záruk a svých práv souvisejících se zpracováním.

### *Zpracování osobních údajů nezletilých na základě souhlasu*

Nařízení upravuje určité zvláštnosti, týkající se zpracovávání osobních údajů nezletilých na základě souhlasu, následovně:

- zpracování osobních údajů nezletilých je zákonné, pokud se jedná o nabídku služeb informační společnosti (např. sociálních médií) přímo dítěti a to má alespoň 16 let[23];
- pokud má nezletilý méně než 16 let, je zpracování zákonné pouze za podmínky a v rozsahu, v jakém souhlas vyjádřila anebo schválila osoba, vykonávající rodičovskou zodpovědnost (tj. zákonný zástupce nebo opatrovník) nezletilého;
- správce je povinný vynaložit přiměřené úsilí, aby si v uvedených případech ověřil, že osoba s rodičovskou zodpovědností vyjádřila anebo schválila souhlas s tím, že se při tom zohlední dostupná technologie.

Uvedené podmínky se vztahují na osobní údaje poskytované prostřednictvím internetu, t.j. na off-line data se tyto podmínky nevztahují. Rovněž se nevztahují na osobní údaje, které se zpracovávají na jiném právním základě, než na souhlasu. Výše uvedená ustanovení nebudou mít také vliv na

[22] Nařízení Evropského parlamentu a Rady (EU) č. 536/2014 z 16. 4. 2014 o klinických hodnoceních humánních léčivých přípravků.
[23] Členské státy mohou stanovit pro tyto účely nižší věkovou hranici, ne však nižší než 13 let, viz čl. 8 Nařízení.

vnitrostátní obecné smluvní právo členských států, např. na pravidla platnosti, uzavírání nebo účinky smlouvy vzhledem k dítěti.

Souhlasu zákonného zástupce nebo opatrovníka nebude třeba v souvislosti s preventivními anebo poradenskými službami, nabízenými přímo nezletilým (např. linky pomoci ohroženým dětem).[24]

### *Další specifika týkající se nezletilých*

Nařízení deklaruje, jak již bylo uvedeno, že nezletilí požívají zvláštní ochrany osobních údajů. Ta se vztahuje zejména na používání jejich osobních údajů pro účely marketingu nebo vytváření osobnostních anebo uživatelských profilů a shromažďování osobních údajů nezletilých při využívání jim přímo nabízených služeb.

Vzhledem k uvedenému by všechny informace a sdělení při zpracovávání na ně zaměřeném měly být podávány jasně a jednoduše, aby jim byly snadno srozumitelné. Zvláštního významnabývá právo na opravu osobních údajů a „právo být zapomenut" v případech, kdy byl dán souhlas v nezletilosti, kdy si subjekt nebyl plně vědom všech rizik spojených se zpracováním a později chce své údaje, zejména na internetu, odstranit.[25]

Pokud správce zpracovává osobní údaje na základě svého oprávněného zájmu[26], musí být schopen prokázat, že odpovědně a objektivně posoudil, že zájmy nebo základní práva a svobody nezletilého, jehož údaje zpracovává, nepřevažují nad oprávněnými zájmy správce.

Podle čl. 40 odst. 2 Nařízení sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů mohou vypracovat kodexy chování, a to pro upřesnění či rozšíření Nařízení rovněž v souvislosti s informováním a ochranou nezletilých a se způsobem získáním souhlasu nositelů rodičovských práv a povinností. Kromě toho, každý orgán dohledu, t.j. též Úřad na ochranu osobních údajů ČR, je povinný na svém území zvyšovat povědomí veřejnosti a její pochopení rizik, pravidel, záruk a práv souvisejících se zpracováním, přičemž zvláštní pozornost se má věnovat činnostem specificky zaměřeným na děti.

### *Co dále*

Správci by měli zajistit, aby osobní údaje zpracovávali na základě relevantních a Nařízením upravených právních základů. Pokud budou osobní údaje zpracovávané na základě souhlasu, formální a obsahové podmínky souhlasu, jakož i okolnosti jeho poskytnutí by měly odpovídat nové právní úpravě. Při zpracovávání osobních údajů v souvislosti s výzkumem, resp. v souvislosti s nezletilými, je třeba splnit další povinnosti.

### *Další informace*

Souhlas se zpracováním osobních údajů:

Recitály 32, 33, 40, 42, 43

Články 6 odst. 1; 7

Zpracovávání osobních údajů nezletilých:

Recitály 38, 58, 65, 71

Články 6, odst. 1; 8; 40 odst. 2; 57 odst. 1 písm. b)

---

[24] Recitál 38, věta poslední Nařízení
[25] Recitál 65 Nařízení
[26] Čl. 6 odst. 1 písm. f) Nařízení

*Lekce 5 z 16*

## Oprávněný zájem

**V textu se dozvíte:**

*Důležité změny*

- Orgány veřejné moci nebudou moci zpracovávat osobní údaje na základě právního základu „oprávněný zájem" při výkonu jejich působnosti.
- Správci, kteří zpracovávají osobní údaje na základě „oprávněného zájmu", by měli věnovat náležitou pozornost posouzení, zda práva a svobody subjektů údajů nepřevažují nad oprávněným zájmem, jež zpracováním sleduje správce.

*Compliance: Akční plán*

Pokud správce zpracovává osobní údaje na právním základě oprávněného zájmu, musí zajistit, aby

- zpracovávání bylo i po nabytí účinnosti Nařízení prováděno zákonným způsobem (viz Lekce 3 – Zákonnost zpracovávání a dalšího zpracování) a aby tento právní základ byl relevantní pro dané okolnosti;
- k zajištění prokazatelnosti vedl evidenci o tom, jak se vypořádal s právy a svobodami subjektu údajů, dotčenými správcem při zpracování jejich osobních údajů;
- subjekty údajů byly informovány, že jejich osobní údaje budou zpracované na tomto konkrétním právním základě.

**K zvláštnostem právního základu oprávněného zájmu**

Nařízení stanoví, že zpracovávání je zákonné pouze tehdy a pouze v tom rozsahu, pokud je splněna alespoň jedna z dále uvedených podmínek. Jednou z nich je rovněž to, pokud zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.[27]

Pro srovnání, aktuální česká právní úprava („Zákon") uvádí, že správce může rovněž zpracovávat osobní údaje bez souhlasu subjektu údajů, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.[28]

Chráněný zájem správce (uznaný právním řádem, nikoliv pouze jeho subjektivní názor) je tak poměřován ochranou práva na soukromí subjektu údajů (právo na informační sebeurčení) jako garantovaného základního práva a svobody jednotlivce.[29] Při kolizi těchto dvou zájmů resp. práv je nezbytné vyhodnotit, zda v konkrétním případě převažuje právo správce (popř. příjemce či jiné dotčené osoby) anebo právo subjektu údajů na ochranu soukromí. Tzn. je nutné zvážit, který zájem má z hlediska práva i společnosti vyšší hodnotu. Evropské soudy i Ústavní soud posuzují tuto otázku v rámci třístupňového testu proporcionality.[30]

---

[27] Článek 6 ods. 1 písm. f) Nařízení
[28] § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
[29] Čl. 10 odst. 3 Listiny základních práv a svobod, vyhlášené usnesením předsednictva ČNR č. 2/1993 Sb.; čl. 8 Listiny základních práv Evropské unie; čl. 8 Úmluvy o ochraně lidských práv a základních svobod.
[30] Tzn.: *1.* zda je omezení stanoveno zákonem, *2.* zda zásah do práva je nezbytný a odpovídá sledovanému legitimnímu cíli, *3.* zda omezení je přiměřené sledovanému legitimnímu cíli. Viz např. nález Ústavního soudu ČR sp. zn. I. ÚS 321/06 ze dne 18. 12. 2006, náleze pléna Ústavního soudu ČR sp. zn. Pl. ÚS 4/94 ze dne 12. 10. 1994, aj. Použití uvedeného testu viz např. rozsudek SD EU ze dne 20. 5. 2003, ve spojených věcech C-465/00,

Oproti současné právní úpravě je znění Nařízení širší a liší se v následujícím:

- zatímco Zákon legitimizuje zpracování osobních údajů bez souhlasu subjektu údajů účelem *ochrany práv a právem chráněných zájmů* správce nebo třetí strany, Nařízení stanoví, že osobní údaje je možné takto zpracovávat, pokud je to nezbytné pro účely *oprávněných zájmů* správce nebo třetí strany.

  Z uvedeného vyplývá, že výjimka z povinnosti disponovat souhlasem subjektu údajů je v Nařízení oproti Zákonu širší a dá se pod ní zahrnout vícero zpracovatelských operací.

  Zatímco podle aktuální právní úpravy musí být splněna podmínka zpracování osobních údajů za účelem *ochrany* práv a právem chráněných zájmů (t.j. musí jít vysloveně o záměr chránit práva správce nebo třetí strany), Nařízení takový požadavek nestanoví. Podle Nařízení postačí, pokud se osobní údaje budou zpracovávat pro účely oprávněných zájmů správce nebo třetí strany, bez ochranného prvku.

  Nový koncept oprávněného zájmu bude spadat například rovněž zpracování osobních údajů pro účely marketingu či jednorázového vstupu do budovy, tzn. účely, které nemají vysloveně ochranný charakter.

- Nařízení oproti původní právní úpravě ukládá, aby posouzení vyváženosti oprávněného zájmu sledovaného správcem a práv a základních svobod subjektů údajů, do nichž se bude zpracováním osobních údajů zasahovat, bylo prováděno se zvláštním ohledem na nezletilé.[31]

  Nařízení tak sleduje zvýšenou míru ochrany práv a základních svobod nezletilých, neboť si jsou méně vědomi rizik, důsledků a dotčených záruk a svých práv, souvisejících se zpracováním osobních údajů. Nařízení ukládá správcům povinnost pečlivě zdokumentovat, jakým způsobem a s jakým výsledkem posoudili vyváženost svého oprávněného zájmu (příp. oprávněného zájmu třetí strany) a práv a základních svobod nezletilého, jež budou zpracováním dotčeny.

  Pro posouzení, zda práva a svobody subjektu údajů (nejen nezletilých) nepřevažují nad oprávněnými zájmy správce, je třeba zohlednit přiměřená očekávání subjektů údajů na základě jejich vztahu se správcem. Existence oprávněného zájmu vyžaduje důkladné posouzení včetně posouzení toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že k zpracování pro uvedený účel může dojít. Zájmy a základní práva subjektu údajů by tak mohly převážit nad zájmy správce zejména tehdy, pokud ke zpracování osobních údajů dochází za okolností, kdy subjekt údajů jejich další zpracování důvodně neočekává.

- Nařízení rovněž specificky stanoví, že na oprávněný zájem se nebudou moci odvolávat orgány veřejné moci při výkonu své působnosti. Pro tento účel bude třeba zvážit použití jiného právního základu.[32]

### *Oprávněný zájem*

Nařízení uvádí příklady, jaké účely zpracování se dají podřadit pod pojem „oprávněný zájem", následovně:

- zamezení podvodům;
- přímý marketing;
- pokud je správce součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, může mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců;

---

C-38/01 a C-139/01, *Österreichischer Rundfunk*; rozsudek SD EU ze dne 9. 11. 2010, ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Hessensku*.

[31] Viz Lekce 3

[32] Např. čl. 6 odst. 1 písm. c) nebo e) Nařízení

- zabránění neoprávněnému přístupu k sítím elektronických komunikací a šíření škodlivých kódů a zamezení útokům, jejichž důsledkem je odepření služby („denial of service"), a škodám na počítačových systémech a systémech elektronických komunikací;
- oznámení případných trestných činů nebo hrozeb pro veřejnou bezpečnost správcem a předání dotčených osobních údajů příslušnému orgánu.

Účel zpracování, včetně toho, že je jím oprávněný zájem, by měl být řádně oznámen subjektu údajů před zahájením zpracování (informační povinností se budeme zabývat v samostatné lekci).

Nařízení dále výslovně stanoví[33], že sdružení a další subjekty zastupující různé kategorie správců nebo zpracovatelů mohou vypracovat kodexy chování pro upřesnění aplikace Nařízení, jako například v souvislosti s oprávněnými zájmy, jež správci nebo zpracovatelé sledují v konkrétních situacích. Správci by si měli ověřit, zda existuje kodex chování, který by se vztahoval na jimi prováděné zpracovatelské operace.

### *Co dále*

Pokud správce zpracovává osobní údaje z titulu oprávněného zájmu, sledovaného jím nebo třetí stranou, měl by zajistit, aby práva a základní svobody subjektů údajů nepřevažovaly nad jeho oprávněnými zájmy, zvláště v případech, kdy subjektem údajů je nezletilý. Dále je nutné zajistit, aby správce byl schopen prokázat, jakým způsobem posoudil vyváženost jím sledovaných oprávněných zájmů a práv a svobod subjektů údajů.

### *Další informace*

Recitály 47 - 50

Články 6 odst. 1 písm. f), 13 odst. 1 písm. d), 14 odst. 2 písm. b), 40 odst. 2 písm. b)

[33] Čl. 40 odst. 2 písm. b) Nařízení

*Lekce 6 z 16*

## Zvláštní kategorie osobních údajů

**V textu se dozvíte:**

*Důležité změny*

- Nařízení pod zvláštní kategorie osobních údajů (dále též „citlivé údaje") zahrnuje výslovně též genetické a biometrické údaje, pokud se zpracovávají za účelem jedinečné identifikace osoby;
- Právní základy zpracování citlivých údajů se mírně liší od aktuální právní úpravy;
- Členské státy budou moci přijmout vlastní modifikace zpracování citlivých údajů.

*Compliance: Akční plán*

- Pokud správce zpracovává citlivé údaje, je nutné správně definovat příslušný právní základ;
- Je-li právním základem souhlas subjektu údajů, je třeba, aby splňoval požadované obsahové náležitosti.

### Zpracovávání zvláštních kategorií osobních údajů

Nařízení mezi citlivé osobní údaje zahrnuje především osobní údaje, které vypovídají o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborových organizacích. Dále Nařízení jako citlivé osobní údaje výslovně uvádí též genetické údaje[34], biometrické údaje[35] k jedinečné identifikaci fyzické osoby, údaje o zdravotním stavu[36] nebo údaje o sexuálním životě nebo sexuální orientaci fyzické osoby.

Nařízení uznává, že citlivé údaje zasluhují zvláštní ochranu, neboť z kontextu jejich zpracování by pro základní práva a svobody mohla vyplývat významná rizika. Nařízení proto zakotvuje v článku 9 odst. 1 všeobecný zákaz jejich zpracovávání, jež může být prolomen pouze způsoby uvedenými v článku 9 odst. 2. Prolomení všeobecného zákazu zpracovávání citlivých údajů Nařízení upravuje taxativním způsobem, tzn. uvedené okolnosti, za nichž je zpracování citlivých údajů zákonné, není možné rozšiřovat.

*Výjimky ze zákazu zpracování citlivých údajů*

Všeobecný zákaz zpracování citlivých údajů se neuplatní při splnění některého z těchto předpokladů:

a) *subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo právo členského státu stanoví, že zákaz nemůže být subjektem údajů zrušen;*

   Ohledně požadavku na platné udělení souhlasu odkazujeme na Lekci 4, avšak upozorňujeme na specifikum, týkající se udělení souhlasu k zpracování citlivých údajů.

[34] Osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.
[35] Osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.
[36] Osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.

Pokud jde o citlivé údaje, souhlas musí být výslovný (tento požadavek neplatí, nejde-li o citlivé údaje).

Zpracovat citlivé údaje na základě souhlasu není možné, pokud právní předpis stanoví, že ani výslovný souhlas subjektu údajů není způsobilý prolomit zákaz zpracování citlivých údajů.

*b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu či kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;*

Tento právní základ rozšiřuje aktuální právní úpravu, neboť výslovně uvádí, že zpracování citlivých údajů je zákonné, pokud je to nezbytné pro plnění povinností vyplývajících z kolektivní smlouvy.

Zpracování citlivých údajů pro účely pracovního práva, práva sociálního pojištění a sociálního zabezpečení je možné i podle aktuální právní úpravy.[37]

*c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;*

Srovnatelný právní základ je obsažen i v aktuální právní úpravě.[38]

*d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;*

Srovnatelný právní základ je rovněž obsažen v aktuální právní úpravě.[39]

*e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;*

a

*f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;*

Srovnatelný právní základ je obsažen i v aktuální právní úpravě.[40]

*g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;*

Srovnatelný právní základ doposud v aktuální právní úpravě obsažen není.

*h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem;*

a

*i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem*

[37] § 9 písm. d) a f) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
[38] § 9 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
[39] § 9 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
[40] § 9 písm. g) a písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

*kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;*

Tato dvě ustanovení rozšiřují a blíže specifikují právní základ uvedený v aktuální právní úpravě.[41]

Citlivé údaje mohou být zpracovávány k účelům uvedeným v písm. h), pokud je zpracovává odborník, nebo jsou zpracovávány v rámci zodpovědnosti odborníka, který podléhá povinnosti dodržovat profesní tajemství podle práva Unie nebo práva členského státu nebo podle pravidel, která stanovily příslušné vnitrostátní orgány, anebo pokud údaje zpracovává jiná osoba, která rovněž podléhá povinnosti mlčenlivosti podle práva Unie či práva členského státu nebo pravidel, která stanovily příslušné vnitrostátní orgány.

*j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo práva členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.*

Jde o nové ustanovení, podle něhož je zpracování citlivých údajů k daným účelům zákonné, pokud není nepřiměřené s ohledem na práva subjektu údajů, a jsou určeny opatření na jejich ochranu (např. minimalizace údajů, pseudonymizace apod.; viz Lekce 3).

Členské státy jsou oprávněné zachovat anebo zavést další podmínky včetně omezení týkajících se zpracování genetických údajů, biometrických údajů nebo údajů o zdravotním stavu. Z uvedeného důvodu mohou vznikat rozdíly v podmínkách zpracování těchto údajů v právních řádech různých členských států. Proto by subjekty, zpracovávající takové údaje v různých státech, měly věnovat náležitou pozornost těmto nuancím.

### *Změny v zpracování citlivých údajů*

V souvislosti se zpracováním citlivých osobních údajů se povinnosti správce mění následovně:

- správce nebude mít oznamovací a registrační povinnost podle § 16 a násl. Zákona[42], namísto toho bude třeba vést záznamy podle čl. 30 Nařízení;
- v případě zpracování zvláštní kategorie osobních údajů ve velkém rozsahu[43] bude správce povinen posoudit vliv na ochranu osobních údajů a určit odpovědnou osobu;
- přenos zvláštní kategorie osobních údajů třetí straně se sídlem v třetí zemi, která nezaručuje přiměřenou úroveň ochrany osobních údajů, bude dovolen pouze s předcházejícím výslovným souhlasem subjektu údajů, pokud zvláštní zákon nestanoví jinak.

V podmínkách české právní úpravy, na rozdíl od slovenské, nebude novinkou, že zpracování fotografie subjektu údajů nebo grafického zobrazení podpisu se nepovažuje za zpracování zvláštních kategorií osobních údajů, pokud se nebudou zpracovávat jako biometrické údaje, t.j. k jedinečné identifikaci nebo autentifikaci osoby (např. pro účely biometrických cestovních pasů). Podle Úřadu na ochranu osobních údajů ČR[44] je zřejmé, že portrétní fotografie vypovídá o rasovém nebo etnickém původu zobrazené osoby, oblečení nebo pokrývka hlavy může vypovídat o

[41] § 9 písm. c) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

[42] Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

[43] Pojem „ve velkém rozsahu" není definovaný v Nařízení a vzhledem na přímou aplikovatelnost Nařízení Úřad na ochranu osobních údajů není oprávněn navrhnout definici tohoto pojmu do vnitrostátní právní úpravy. Zatím je možné se opřít při výkladu tohoto pojmu o recitály 91 a 97 Nařízení, pokud nebudou publikovaná stanoviska pracovní skupiny WP 29 k aplikaci tohoto pojmu.

[44] Stanovisko č. 12/2012 k použití fotografie, obrazového a zvukového záznamu fyzické osoby.

náboženství apod. Fotografie nebo jiný obrazový záznam fyzické osoby je dokumentem osobní povahy, který mimo jiné obsahuje biometrické i jiné charakteristiky subjektu údajů, které vypovídají o skutečnostech definovaných v § 4 písm. b) Zákona jako citlivý údaj, a může být proto jako nosič informací zdrojem pro zpracování citlivých údajů.

Jestliže jsou však informace z fotografie subjektu údajů používány pro pouhé rozlišení jeho podoby ve srovnání s jinými osobami a tyto informace nejsou dále zpracovávány, nelze takové používání fotografií posuzovat jako zpracování citlivých osobních údajů.

Obdobný názor zastává i Pracovní skupina WP 29, která ve svém stanovisku k internetovým sociálním sítím konstatuje, že *„pracovní skupina obecně nepovažuje snímky na internetu za citlivé údaje, nejsou-li snímky jednoznačně použity k odhalení citlivých údajů o fyzických osobách*".

### *Rejstříky trestů / údaje o přestupcích*

Tyto údaje Nařízení nekategorizuje jako citlivé údaje. I nadále platí, že správcem pro účely zpracování osobních údajů týkajících se:

- rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření; nebo
- zpracovávání osobních údajů v rejstříku trestů podle zvláštního předpisu

může být pouze příslušný státní orgán stanovený zákonem.

Jakýkoliv souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci.

### *Zpracování národního identifikačního čísla*

Členské státy mohou stanovit zvláštní podmínky pro zpracování národních identifikačních čísel nebo jakýchkoliv jiných všeobecně uplatňovaných identifikátorů (např. rodné číslo). V uvedeném případě se národní identifikační číslo nebo jakýkoliv jiný všeobecně uplatňovaný identifikátor použije jen v rámci přiměřených záruk práv a svobod subjektu údajů podle Nařízení.

### *Co dále*

Pokud správce zpracovává citlivé údaje, je nutné prověřit, že tak činí na základě relevantního právního základu podle Nařízení. Je-li právním základem souhlas subjektu údajů, znění a způsob udělení souhlasu je třeba revidovat a aktualizovat podle nových podmínek.

### *Další informace*

Recitály 51 – 56, 91, 97

Články 4 odst. 13 - 15, 9, 10, 87

*Lekce 7 z 16*

## Informační povinnost správce

**V textu se dozvíte:**

*Důležité změny*

- Nařízení podrobněji upravuje rozsah informací, které mají být subjektům údajů poskytnuty;
- Nová právní úprava klade důraz na jasnost a srozumitelnost informování subjektů údajů.

*Compliance: Akční plán*

Správci by měli:

- revidovat stávající znění informace o zpracování osobních údajů a uvést je do souladu s Nařízením;
- prokazatelně seznámit subjekty údajů s informacemi, požadovanými Nařízením;
- zajistit, aby informování subjektů údajů bylo provedeno včas, úplně a srozumitelně.

**K povinnosti správce informovat subjekt údajů**

Jednou ze základních zásad zpracování osobních údajů je zásada transparentnosti. Nařízení proto ukládá správcům povinnost přijmout vhodná opatření, aby subjektům údajů byly poskytnuty všechny informace týkající se zpracování, jejichž okruh Nařízení taxativně upravuje.

Zásada transparentnosti vyžaduje, aby všechny informace byly stručné, snadno přístupné a srozumitelné, jasně a jednoduše formulované a je-li to vhodné, pak i vizualizované. Jsou-li informace určeny veřejnosti, mohou být poskytovány v elektronické podobě, např. prostřednictvím internetových stránek. Zejména to platí v případech, kdy účast celé řady aktérů a technologická složitost znesnadňují subjektu údajů, aby věděl a porozuměl, zda jsou shromažďovány jeho osobní údaje a kdo a za jakým účelem je shromažďuje, jako je tomu např. při reklamě na internetu.

Informační povinnost je upravena poměrně široce, přičemž právní rámec poskytování informací subjektu údajů je upraven takto:[45]

- informace se poskytnou ve stručné, transparentní, srozumitelné a snadno dostupné formě, jasně a jednoduše formulované;
- informace mohou být podány písemně, elektronicky nebo jinými prostředky nebo na vyžádání také ústně;
- informace se poskytnou subjektu údajů bezplatně, v případě nedůvodných nebo nepřiměřených žádostí subjektů údajů má však správce možnost uložit přiměřený poplatek nebo odmítnout žádosti vyhovět (v takovém případě však nese důkazní břemeno prokázání, že žádost je nedůvodná nebo nepřiměřená);
- správce je oprávněn požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů;
- určité informace mohou být doplněny standardizovanými ikonami, které může zavést Komise prováděcím předpisem a jejichž použití se vyprofiluje až praxí.

[45] Čl. 12 Nařízení

### *Jaké informace je třeba poskytnout*

V porovnání se stávající právní úpravou[46] budou správci povinni poskytnout subjektům údajů navíc tyto informace[47]:

- kontaktní údaje[48] správce, event. jeho zástupce a případného pověřence;
- právní základ pro zpracování a v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f)[49] Nařízení, také oprávněné zájmy správce nebo třetí strany;
- doba, po kterou budou osobní údaje uloženy, případně kritéria použitá pro její stanovení;
- skutečnost, zda je poskytování osobních údajů zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;
- konkretizace práv subjektu údajů (pro úplnost uvádíme všechna práva, která Nařízení přiznává subjektu údajů, tzn. nejen ta, která předchozí právní úprava neobsahovala):
    - právo požadovat od správce přístup k svým osobním údajům;
    - právo na opravu, doplnění, výmaz nebo omezení zpracování osobních údajů;
    - právo vznést námitky proti zpracování osobních údajů;
    - právo na přenositelnost údajů;
    - právo souhlas kdykoliv odvolat, je-li zpracování založeno na souhlasu subjektu údajů;
    - právo podat stížnost u dozorového úřadu;
    - právo na informaci, že dochází k automatizovanému rozhodování, včetně profilování.

### *Kdy se informace poskytují?*

Pokud správce získává osobní údaje od subjektu údajů, informuje ho v okamžiku získání[50] údajů.

Pokud správce nezískává osobní údaje přímo od subjektu údajů, tyto informace poskytne:

- v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
- nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
- nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

---

[46] § 11 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, („Zákon"), upravující informační povinnost správce event. zpracovatele.

[47] Čl. 13 a 14 Nařízení

[48] Dosud byla zakotvena povinnost informovat o „*totožnosti*" (viz čl. 10 písm. a), čl. 11 odst. 1, první tiré Směrnice), normovaná v Zákoně náležitostí „*kdo*" (§ 11 odst. 1). V odborné literatuře tato identifikace osoby správce nebo zpracovatele byla traktována jako požadavek uvést u právnické osoby obchodní firmu, IČO a adresu sídla, u fyzických osob jméno, příjmení a bydliště resp. místo podnikání.

[49] *„zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě."*

[50] Dle dikce Zákona se tak má dít při shromažďování údajů, tedy nejpozději, kdy správce údaje od subjektu požaduje. Odborné komentáře však za jedině správný výklad, aby byl naplněn účel ustanovení, považují, že subjekt údajů musí být informován před samotným získáváním osobních údajů (srov. např. Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, s. 211).

V takovém případě je správce kromě výše uvedených informací povinen oznámit subjektu údajů také informace o kategoriích dotčených osobních údajů a to, z jakého zdroje osobní údaje pocházejí, případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů.

### *Výjimky z informační povinnosti*

Správce nemá povinnost poskytnout subjektu údajů informace v případě, že:

- subjekt údajů již uvedené informace má;
- se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí, nebo pokud je pravděpodobné, že uplatnění povinnosti by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme správce vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti;
- je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů[51]; nebo
- osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti; jakož i
- v případech, kdy se na zpracovávání osobních údajů Nařízení nevztahuje, tzn.:
    - zpracovávání prováděné členskými státy při výkonu činností, spadajících do oblasti společné zahraniční a bezpečnostní politiky podle hlavy V, kapitoly 2 Smlouvy o EU;
    - příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, viz Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016.

### *Další zpracování*

Pokud správce zamýšlí dále zpracovávat osobní údaje k jinému účelu, než ke kterému byly získány, poskytne subjektu údajů před tímto dalším zpracováváním informace o tomto jiném účelu a jakékoliv další relevantní informace dle výše uvedeného (pro více informací o zákonnosti dalšího zpracovávání viz Lekce 3).

### *Co dále*

Informační povinnost správců vůči subjektům údajů reflektuje jednu ze základních zásad zpracování osobních údajů, a to zásadu transparentnosti. Pro zajištění transparentnosti zpracování je nezbytné, aby správci srozumitelným a úplným způsobem informovali subjekty údajů o okolnostech zpracování. Rozsah informační povinnosti je upraven přímo Nařízením, bude tedy výzvou, jak skloubit povinnost poskytnout rozsáhlé informace ve stručném oznámení.

---

[51] Výluka je dosud zakotvená jednak v § 3 odst. 6 Zákona z důvodů zejména zajištění bezpečnosti a obrany republiky, veřejného pořádku, předcházení, vyhledávání, odhalování trestné činnosti a stíhání tr. činů, významného hospodářského a finančního zájmu ČR a EU anebo zpřístupnění svazků býv. StB, jednak v § 11 odst. 3, písm. b) Zákona, kdy tak ukládá zvláštní zákon (např. zákon č. 372/2011 Sb., o zdravotních službách,) nebo údajů je třeba k uplatnění práv a povinností správce vyplývajících ze zvláštního zákona. Subjekty vykonávající činnosti podle zvláštních zákonů nejsou vyňaty z působnosti Zákona jako celku, ale pouze z povinností určujících základní parametry zpracování osobních údajů a dále z povinností ve vztahu k subjektu údajů, tj. právě z nyní pojednávané informační povinnosti a povinností souvisejících s právem přístupu subjektu údajů. Např. většina úkolů Policie ČR by byla těžko realizovatelná při aplikaci povinnosti dotyčnou osobu informovat ihned při shromáždění dat, anebo na její žádost jí kdykoli sdělit, jaké osobní údaje o ní zpracovává.

Podle našeho názoru bude i v budoucnu přetrvávat jistá výkladová obtížnost ustanovení o informační povinnosti, neboť ukládané povinnosti a výjimky z nich pro určité druhy zpracování či správců nejsou upraveny zcela jednoznačně a jejich vzájemná provázanost může vyvolávat i nadále aplikační nejasnosti.

*Další informace*

Recitály 58, 60 – 63

Články 12 – 14

*Lekce 8 z 16*

## Práva subjektů údajů (1. část)

**V textu se dozvíte:**

*Důležité změny*

Správci budou mít povinnost:

- seznámit se s obsahem nových práv subjektů údajů, která jim přiznává Nařízení;
- zavést efektivní interní postupy pro zpracování žádostí subjektů údajů, týkajících se zpracování (např. povinnost vydat jim na žádost kopii zpracovaných osobních údajů a prokázat, že je zpracovávají zákonně);
- připravit směrnice a materiály informující, jakým způsobem mohou subjekty údajů uplatnit svá práva u správce.

Subjekty údajů mohou kromě jiného požadovat:

- vymazání svých osobních údajů, není-li zpracování zákonné nebo odvolají-li souhlas se zpracováním;
    - jestliže správce údaje zveřejnil (např. v souvislosti se službami sociálních sítí) a žádost o výmaz je oprávněná, je správce povinen postoupit žádost všem, kteří zveřejněné údaje zpracovávají. Jde o mimořádně široce koncipovanou povinnost, jejíž praktické uplatnění bude zřejmě předmětem testování;
- omezení zpracování svých údajů, např. po dobu vyřízení stížnosti týkající se zpracování, nebo nežádá-li subjekt údajů výmaz z jiného důvodu.

*Compliance: Akční plán*

Správci by měli:

- vytvořit interní postupy pro včasné vyřizování žádostí subjektů údajů, týkajících se zákonnosti zpracování jejich osobních údajů (zejména zákazníků, případně zaměstnanců);
- vyškolit tým zaměstnanců, vyřizujících žádosti subjektů údajů, o jejich právech a povinnostech;
- připravit standardizované vzory odpovědí na žádosti, vytvořit procesy pro dodržování zákonných lhůt pro vyřizování, zajistit, aby subjektům údajů byly poskytnuty všechny informace, na něž mají nárok;
- zajistit, aby způsob vyřizování žádostí splňoval technické požadavky podle Nařízení;
- prověřit, zda v důsledku informační povinnosti nebude porušeno právo na soukromí jiného subjektu údajů a vytvořit procesy k minimalizování těchto rizik;
- zajistit, aby bylo technicky a organizačně možné vyřídit žádost o výmaz nebo omezení zpracování osobních údajů v systémech správce.

**K právům subjektu údajů**

Nařízení rozšiřuje a upřesňuje práva subjektu údajů. Pro úplnost uvádíme seznam všech práv, jak je upravuje Nařízení v Kapitole III s tím, že pro rozsah materie se budeme touto tématikou zabývat ve dvou lekcích.

### *Právo na přístup k údajům*

Na rozdíl od informační povinnosti správce, viz naše Lekce 7, je právo na přístup k údajům koncipováno odlišně. Zatímco informační povinnost se vztahuje na správce, který musí automaticky, t.j. bez zvláštní žádosti subjektu údajů, poskytnout určité údaje, pak právo na přístup k informacím je koncipováno nezávisle na tom, zda správce splnil svou informační povinnost. Toto právo garantuje subjektu údajů právo jednak na přístup k jeho údajům a jednak na doplňující informace, a to na jeho žádost.

Obsahem práva na přístup k údajům je právo subjektu údajů získat od správce potvrzení, zda se zpracovávají osobní údaje, které se ho týkají. Pokud ano, má právo přístupu k nim (t.j. na jejich kopii) a na další informace[52] o zpracování.

Kopii zpracovávaných osobních údajů poskytne správce bezplatně. Za další vyžádané kopie může správce účtovat přiměřený poplatek, odpovídající administrativním nákladům s tím spojeným. Pokud subjekt údajů požádal elektronickými prostředky, budou informace poskytnuty v běžně používané elektronické podobě, pokud subjekt údajů nepožádal o jiný způsob. Uvedený požadavek by mohl způsobit navýšení nákladů pro ty, kteří zpracovávají údaje v listinné formě nebo ve zvláštních formátech, jež bude nutné konvertovat do všeobecně čitelné elektronické formy. V této souvislosti mohou tudíž vzniknout správci další náklady na softwarové a hardwarové vybavení, administrativní personál apod.

Podle recitálu 63 může správce poskytnout dálkový přístup k bezpečnému systému, který by subjektu údajů zajistil přímý přístup k jeho osobním údajům. To znamená, že pokud např. správce předpokládá větší frekvenci žádostí subjektů údajů na přístup k údajům, může tuto povinnost splnit tím, že vytvoří bezpečnou databázi údajů, do níž bude mít subjekt údajů přístup v rozsahu vlastních osobních údajů. Uvedený návrh je však spíše doporučující než závazné povahy.

Právo přístupu subjektu údajů k osobním údajům odpovídá povinnosti správce zavést takové interní postupy a organizační a technická opatření, aby žádostem subjektů údajů byl schopen vyhovět v zákonné lhůtě. Ta je určena jako „bez zbytečného odkladu", vždy však do jednoho měsíce od doručení žádosti s tím, že v odůvodněných případech může být lhůta prodloužena o další dva měsíce.

Správci by proto měli mimo jiné zavést pro dané případy pracovní postupy, zaškolit personál pro vyřizování žádostí, poučit jej o povinnostech souvisejících s ochranou osobních údajů, např. o povinnosti mlčenlivosti, a zajistit odpovídající technické a organizační vybavení k tomu, aby byl schopen vyřizovat žádosti ve všeobecně čitelné elektronické formě.

### *Výjimky z práva na přístup k údajům*

Nařízení dále upravuje určité výjimky z práva přístupu k údajům:

- v prvé řadě, právo získat kopii údajů nesmí mít nepříznivé důsledky pro práva a svobody jiných, ani pro obchodní tajemství nebo právo duševního vlastnictví/autorská práva, týkající se softwaru. Pokud by splněním práva na přístup k údajům měla být dotčena práva jiné osoby, je třeba přijmout taková organizační a technická opatření, aby k porušení nedošlo. Výsledkem zohlednění těchto požadavků by však nemělo být odmítnutí poskytnout jakoukoliv informaci subjektu údajů. Jelikož tu proti sobě stojí minimálně dvě rovnocenná

[52] Tzn.: a./ účely zpracování; b./ kategorie dotčených osobních údajů; c./ příjemci nebo kategorie příjemců, jimž byly nebo budou osobní údaje zpřístupněny, zejména příjemci v třetích zemích anebo mezinárodní organizace; d./ je-li to možné, předpokládaná doba uložení osobních údajů nebo, není-li to možné, kritéria pro její určení; e./ právo požadovat od správce opravu osobních údajů týkajících se subjektu údajů nebo jejich výmaz či omezení jejich zpracování, nebo právo vznést námitku proti takovému zpracování; f./ právo podat stížnost orgánu dohledu; g./ pokud nebyly osobní údaje získány od subjektu údajů, jakékoliv dostupné informace ohledně jejich zdroje; h./ existence automatizovaného rozhodování včetně profilování, informace o použitém postupu, jakož i o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů; i./ pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách.

práva či svobody[53], v případě sporu je oprávněn s konečnou platností rozhodnout příslušný soud;

- pokud správce zpracovává v souvislosti se subjektem údajů velké množství informací, může požadovat, aby před doručením informací subjekt údajů upřesnil, jakých informací nebo zpracovatelských činností se jeho žádost týká; uvedené však neznamená, že pokud by vyřízení žádosti subjektu údajů mělo být časově a rozsahem náročné, že by správce neměl povinnost vyhovět;
- žádost subjektu údajů by měla být motivovaná ověřením zákonnosti zpracování jeho osobních údajů; žádosti podané za jiným účelem než kvůli ochraně osobních údajů by správce nemusel vyhovět.

Správce by měl využít všech přiměřených opatření k ověření totožnosti subjektu údajů, který žádá o přístup, zejména v souvislosti s on-line službami a on-line identifikátory. Správce by však neměl uchovávat osobní údaje jen proto, aby byl schopen reagovat na případné žádosti.

### *Právo na opravu*

Subjekt údajů má právo, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, jež se ho týkají. Se zřetelem k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

### *Právo na výmaz (právo „být zapomenut")*

Právo „být zapomenut" vyvolalo již v době legislativního procesu přípravy Nařízení mnoho emocí, a to především v souvislosti s poskytováním služeb informační společnosti korporacemi jako Google, Facebook atd. Služby, poskytované uvedenými i dalšími společnostmi, jsou specifické v tom, že zpracovávají obrovské množství osobních údajů subjektů údajů, přičemž je ukládají na svých serverech, dále s nimi nakládají a vzhledem k rozsahu údajů a zpracovatelských operací tyto společnosti předvídali značná úskalí související s uvedeným právem. Právo „na zapomnění", dosud upraveno pouze judikatorně,[54] se však do finálního znění Nařízení dostalo, a to v následujícím rozsahu:

Subjekt údajů má právo, za splnění podmínek upravených Nařízením, dosáhnout u správců bez zbytečného odkladu vymazání svých osobních údajů. Tomuto právu odpovídá povinnost správce bez zbytečného odkladu vymazat osobní údaje subjektu údajů, je-li splněn některý z těchto důvodů:

- osobní údaje již nejsou potřeba k účelům, pro něž byly shromážděny nebo jinak zpracovány;

  Podle této premisy, pokud byly osobní údaje shromážděny nebo zpracovány např. k účelu přímého marketingu, avšak správce změnil obchodní činnost a již své marketingové aktivity nezaměřuje vůči subjektu údajů, měl by jeho osobní údaje vymazat.

- subjekt údajů odvolá souhlas, na jehož základě se provádí zpracování[55], a jestliže neexistuje jiný právní základ pro zpracování;

  Odvolání souhlasu nezpůsobuje nezákonnost zpracování, k němuž došlo před odvoláním (více k souhlasu viz Lekce 4).

[53] Právo subjektu údajů na přístup k údajům a právo jiné osoby např. na ochranu osobnosti, na soukromí, listovní tajemství, obchodní tajemství, autorské právo apod.
[54] Na úrovni EU viz zejména rozsudek SDEU (velká komora) z 13. 5. 2014, ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González.
[55] Podle článku 6 odst. 1 písm. a) nebo článku 9 odst. 2 písm. a) Nařízení.

- subjekt údajů vznese námitky vůči zpracování podle článku 21 odst. 1 Nařízení[56] a nepřevažují žádné oprávněné důvody pro zpracování anebo subjekt údajů vznese námitky vůči zpracování podle článku 21 odst. 2 Nařízení[57];

  Právem namítat zpracování se budeme zabývat v další lekci.

- osobní údaje byly zpracovány protiprávně;

  Uvedený důvod je značně obecný a natolik široce koncipovaný, že bude pod něho možné subsumovat velké množství žádostí subjektů údajů na výmaz. Riziko s ním spojené spočívá v tom, že bude na správci, aby prokázal, že údaje zpracovává zákonně (k zákonnosti zpracování viz Lekce 3). To, že subjekt údajů bude tvrdit, že údaje jsou zpracovávány protiprávně, bude stačit k tomu, aby důkazní břemeno prokázání opaku se přesunulo na správce. Ten by si proto měl zajistit, aby nebyl v důkazní nouzi ohledně prokázání zákonnosti a aby o zpracovávání a právních základech, které se na něho vztahují, vedl náležitou evidenci.

  Bude jistě zajímavé sledovat, jak se členské státy postaví k implementaci výjimek[58] do svých právních řádů. Je samozřejmé, že správci, kteří budou zpracovávat údaje na přeshraničním základě, by měli být s těmito místními specifiky seznámeni a mohli zajistit zákonnost zpracování v každém státě Unie.

- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;

  Uvedené by se vztahovalo např. na situaci, kdy dosud zpracované údaje mají být podle právního řádu vymazány po uplynutí určité doby (a zároveň se neaplikuje výjimka opravňující k zpracování např. pro účely archivace ve veřejném zájmu – viz níže).

- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 Nařízení.

  Uvedené právo je relevantní především v situaci, kdy subjekt údajů dal souhlas k zpracování osobních údajů v dětském věku, nebyl si plně vědom rizik spojených se zpracováním a později chce tyto osobní údaje odstranit, zejména z internetu. Subjekt údajů by měl mít možnost toto právo uplatnit bez ohledu na skutečnost, že již není dítě.

### *Specifika související se zveřejněnými údaji*

Jestliže správce zveřejnil osobní údaje a zároveň je povinen je vzhledem na výše uvedená pravidla vymazat, přijme přiměřené kroky, včetně technických opatření, aby informoval další správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje a jejich kopie či replikace. Uvedená opatření se přijmou se zřetelem na dostupnou technologii a náklady.

Uvedené ustanovení odráží snad jednu z nejrevolučnějších změn při zpracování osobních údajů, kterou přináší Nařízení. Toto ustanovení v zásadě ukládá povinnost správci, který zpracoval osobní údaje subjektu údajů a pokud v rámci tohoto zpracování došlo též k jejich zveřejnění, aby v případě, kdy subjekt údajů důvodně požádá o výmaz svých údajů,

- aktivně přijal příslušná opatření, včetně technických opatření, a

[56] Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, proto, že zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo že zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě, včetně námitek proti profilování založeného na uvedených ustanoveních.
[57] Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování jeho osobních údajů, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu.
[58] Článek 23 Nařízení.

- účinně informoval správce, kteří předmětné údaje zpracovávají, že subjekt údajů požaduje vymazání svých údajů, jejich kopií a replik,
- to vše s ohledem na dostupnou technologii a náklady.

Podle recitálu 66 bylo uvedené opatření přijato v neposlední řadě k posílení práva být zapomenut v on-line prostředí internetu. Není však zatím celkem zřejmé, jakým způsobem konkrétní správce vůbec určí okruh dalších správců, kteří zpracovávají osobní údaje, jež se staly veřejnými, tzn. jak identifikuje konkrétní správce, kterým by měl žádost o výmaz údajů notifikovat. Bude tudíž otázkou dalšího testu praktické aplikace tohoto ustanovení, jak a zda vůbec bude toto ustanovení vykonatelné, a do jaké míry bude právo subjektu údajů, odpovídající této povinnosti, skutečně realizovatelné.

### *Výjimky z práva na výmaz*

Výše uvedené povinnosti správce se neuplatní, pokud je zpracování třeba:

- k uplatnění práva na svobodu projevu a na informace;
- pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- z důvodů veřejného zájmu v oblasti veřejného zdraví[59];
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 Nařízení, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování, nebo
- pro prokazování, uplatňování nebo obranu právních nároků[60].

### *Právo na omezení zpracování*

Omezení zpracování[61] znamená, že správce je oprávněn osobní údaje pouze uchovávat, aniž by je jakkoliv zpracovával. Pokud jsou údaje zpracovávány automatizovaně, je k tomu nutné přijmout odpovídající technická opatření (např. stažené z on-line prostředí). Subjekt údajů je oprávněn, aby správce omezil zpracování, pokud jde o některý z těchto případů:

- subjekt údajů popírá přesnost osobních údajů, a to po dobu, umožňující správci ověřit jejich přesnost;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro prokazování, uplatňování nebo obranu právních nároků;
- subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 Nařízení, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Pokud bylo zpracování omezeno podle výše uvedených pravidel, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu založení,

---

[59] V souladu s článkem 9 odst. 2 písm. h) a i) Nařízení, jakož i článkem 9 odst. 3 Nařízení.

[60] Český oficiální překlad, publikovaný EU, zní *„pro určení, výkon nebo obhajobu právních nároků“*; nezdá se však přesný, nevystihuje věcnou podstatu a tuzemskou odbornou terminologii.

[61] Článek 4 odst. 3 Nařízení.

výkonu nebo hájení právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.

Správce předem upozorní subjekt údajů, který dosáhl omezení zpracování, že bude omezení zrušeno.

*Kromě uvedeného*

V souvislosti s právem na opravu, výmaz a omezení je správce povinen oznámit každému příjemci, jemuž osobní údaje poskytl, každou opravu nebo výmaz osobních údajů nebo omezení jejich zpracování. Uvedenou povinnost však nemá, pokud se to ukáže jako nemožné nebo by to vyžadovalo nepřiměřeného úsilí. Správce o uvedených příjemcích informuje subjekt údajů, pokud to tento subjekt požaduje.

*Co dále*

V souvislosti s uvedenými oprávněními má správce rozšířené povinnosti, na něž odkazujeme v části *Compliance: Akční plán* výše. K zajištění souladu s Nařízením se správci doporučuje konzultovat vnitřní procesy zpracování osobních údajů s právními poradci, případně IT odborníky.

*Další informace*

Recitály 63 - 69

Články 15 – 19

*Lekce 9 z 16*

## Práva subjektů údajů (2. část)

**V textu se dozvíte:**

*Důležité změny*

- Právo na přenositelnost údajů rovněž opravňuje subjekt údajů, aby správce předal jeho osobní údaje přímo jinému správci;
- Obsah práva subjektů údajů vznést námitku proti zpracování u správce údajů se mění; o tomto právu musí být subjekty údajů řádně informovány;
- Subjekt údajů má právo, aby se na něj nevztahovalo rozhodnutí, které:
    - je založeno výhradně na automatizovaném zpracování (včetně profilování), a
    - má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

*Compliance: Akční plán*

Správci údajů mají:

- zajistit, aby jimi zpracovávané osobní údaje byly jednoduše přenositelné ve strukturovaném, běžně používaném a strojově čitelném formátu;
- ověřit, že subjekty údajů byly řádně a při první komunikaci informovány o právu vznést námitku proti zpracování;
- prověřit, zda dochází k profilování, a pokud ano, zajistit, aby pro to existoval relevantní právní základ.

**K právům subjektu údajů**

*Právo na přenositelnost údajů*

Právo na přenositelnost údajů Nařízení zakotvuje jako právo subjektu údajů:

- na získání jeho osobních údajů a na jejich následné předání jinému správci[62], a rovněž
- na předání osobních údajů jedním správcem přímo správci druhému.

V prvním případě právo na získání osobních údajů může připomínat spíše dříve zmiňované *právo na přístup k údajům* (viz Lekce 8). Právo získat osobní údaje je však upraveno specifičtěji, s těmito rozdíly:

- zatímco právo na přístup k údajům opravňuje subjekt údajů k přístupu k jeho údajům (tj. také k získání jejich kopie) v běžně používané elektronické podobě,
- právo na přenositelnost je koncipováno úžeji a detailněji v tom smyslu, že opravňuje subjekt k získání údajů ve strukturovaném, běžně používaném a strojově čitelném formátu. Po technické stránce je tedy specifičtější a pro správce náročnější, neboť musí zajistit, aby osobní údaje odevzdal ve strukturovaném, tj. systematickém, organizovaném formátu[63].

Právo na přenositelnost údajů se však může uplatnit pouze tehdy, pokud:

[62] Výkonem tohoto práva není dotčen článek 17 Nařízení. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.
[63] Recitál 68 zmiňuje také „interoperabilní formát", ale jedná se zřejmě spíše o doporučení než o závaznou dikci.

- jde o údaje, které subjekt údajů sám poskytl správci,
- zpracování je založeno na souhlasu nebo výslovném souhlasu (u zvláštních kategorií údajů), případně je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, a
- pokud se zpracování provádí automatizovaně (tj. nikoliv v listinné formě; pro srovnání – právo na přístup k údajům se vztahuje rovněž na údaje zpracované v listinné formě).

Nejsou-li splněny výše uvedené podmínky, subjekt údajů se nemůže tohoto práva domáhat. Pokud by např. správce získal osobní údaje od jiného správce a nikoliv přímo od subjektu údajů, neměl by subjekt právo na přenositelnost, ale pouze na přístup k údajům.[64]

Získá-li subjekt údaje v rámci práva na přenositelnost, je oprávněn je následně sám předat jinému správci. Tím však nesmí být nepříznivě dotčena práva a svobody jiných osob. To znamená, že pokud by právo na přenositelnost údajů mělo negativní vliv na práva a svobody jiných osob, k předání (resp. k poskytnutí údajů subjektu údajů) by nemělo dojít. Tato situace by mohla nastat například v rámci sociálních sítí, kdy se spolu s údaji subjektu údajů zpracovávají osobní údaje jiných osob (např. v rámci vzájemné komunikace). Při uplatnění práva na přenositelnost tak nesmí být dotčena práva jiné osoby.

Podstatná změna, vnesená novým konceptem práva na přenositelnost údajů, spočívá v tom, že subjekt údajů může rovněž žádat po správci, aby osobní údaje nevydal jemu, ale aby je přímo předal jinému správci. V praxi je toto právo využitelné např. tehdy, pokud subjekt údajů mění dodavatele určitých (např. telekomunikačních) služeb. V takovém případě je subjekt zbaven administrativní a technické zátěže spojené s předáním svých osobních údajů jinému správci, neboť tuto povinnost má přímo původní správce, a to ve *„strukturovaném, běžně používaném a strojově čitelném formátu*". Podmínkou je pouze technická realizovatelnost tohoto požadavku.

### *Právo vznést námitku*

Právo vznést námitku proti zpracování osobních údajů přiznává Nařízení subjektu údajů pouze v určitých specifických případech. Subjekt není oprávněn vznést námitku proti jakémukoliv zpracování, ale pouze pokud jde o:

1. zpracování, které je nezbytné:
    a. pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce; nebo
    b. pro účely oprávněných zájmů příslušného správce či třetí strany;

    včetně námitky proti profilování, založenému na uvedených ustanoveních.

    V těchto případech je subjekt údajů oprávněn kdykoliv vznést námitku proti zpracování, ale pouze *„z důvodů týkajících se jeho konkrétní situace*". Břemeno tvrzení, proč by mělo být zpracování zastaveno, je tak na straně subjektu údajů, který musí uvést specifické okolnosti, týkající se konkrétně jeho osoby nebo situace.

    Jestliže subjekt údajů vznesl námitku a uvedl relevantní důvody, nesmí správce osobní údaje dále zpracovávat, pokud neprokáže

    - závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo
    - důvody pro prokazování, uplatňování nebo obranu právních nároků[65].

[64] Pro praktický život však tento formalistický přístup komunitární či jiné normotvorby nemá valného významu a je samoúčelem. Subjekt údajů má a bude mít nárok – přes dikci aktuálního českého zákona v § 12 - na zpracovávané osobní údaje, nikoliv jen na informaci, že je zpracováváno jeho jméno a příjmení, dat. narození, bydliště atp. Nic tedy nebrání, aby subjekt takto získané údaje sám poskytl, „přenesl", jinému správci.

V takovém případě by správce mohl ve zpracování dále pokračovat. To znamená, že pokud subjekt údajů vznese námitku z výše uvedených důvodů, důkazní břemeno se přesouvá na správce, který musí prokázat existenci důvodů, které jej opravňují i nadále zpracovávat osobní údaje k daným účelům.

Na právo vznést námitku z výše uvedených důvodů musí být subjekt údajů výslovně správcem upozorněn, a to nejpozději v okamžiku první komunikace. Toto právo musí být uvedeno zřetelně a odděleně od jakýchkoliv jiných informací správce;

2. zpracovávání pro účely přímého marketingu;

   Subjekt údajů je oprávněn kdykoli vznést námitku proti zpracování svých osobních údajů pro účely přímého marketingu, včetně profilování, pokud souvisí s přímým marketingem.

   Jedná se o absolutní právo subjektu údajů, a to aniž by byl povinen tvrdit nebo dokazovat cokoliv dalšího. Jinak řečeno, pokud si subjekt údajů nepřeje, aby se jeho osobní údaje zpracovávaly k tomuto účelu, postačí, že vznese námitku vůči správci údajů, který je bez dalšího povinen zpracovávání pro tento účel ukončit. Subjekt údajů nemá povinnost uvést důvody nebo závažné důvody jako výše v bodě 1. Zároveň neexistuje způsob, jak by se správce mohl proti této námitce účinně bránit (např. tvrzením, že jeho oprávněný zájem převažuje nad právy a zájmy subjektu údajů). Jakmile tedy subjekt údajů doručí správci námitku proti zpracovávání osobních údajů pro účely přímého marketingu, nesmí správce ve zpracovávání pro tento účel dále pokračovat. Pokud však příslušné údaje zpracovává rovněž pro jiný účel na základě jiného vhodného právního základu, takové zpracování není námitkou dotčeno.

   Podobně jako v bodě 1 správce musí na uvedené právo výslovně upozornit, a to nejpozději v okamžiku první komunikace se subjektem údajů a toto právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací;

3. zpracovávání pro účely vědeckého či historického výzkumu nebo pro statistické účely;

   Jsou-li osobní údaje zpracovávány pro uvedené účely, má subjekt údajů z důvodů svých zvláštních poměrů právo vznést námitku proti zpracování osobních údajů. Toto právo však nemá, je-li zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.

   Podobně jako v bodě 1 musí subjekt údajů uvést relevantní důvody, týkající se jeho konkrétní situace, aby zpracovávání bylo ukončeno.

   Na rozdíl od námitek z důvodů, uvedených v bodech 1 a 2, nemusí být subjekt údajů na právo vznést námitku z tohoto důvodu upozorněn. Námitku je možné vznést také automatizovanými prostředky pomocí technických specifikací.

### *Automatizované individuální rozhodování[66] a profilování[67]*

---

[65] Český oficiální překlad, publikovaný EU, zní *„pro určení, výkon nebo obhajobu právních nároků*"; není však přesný, nevystihuje totiž věcnou podstatu ani tuzemskou odbornou terminologii.

[66] O automatizované individuální rozhodování se jedná tehdy, pokud se o určité skutečnosti rozhoduje automatizovaným způsobem, tj. bez zásahu lidského faktoru, např. na základě určitých dopředu stanovených algoritmů.

[67] Profilování je jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu (čl. 4 odst. 4 Nařízení). Podle recitálu 71 Nařízení by měl správce použít vhodné matematické nebo statistické postupy profilování, zavést technická a organizační opatření, která zejména zajistí opravu faktorů vedoucích k nepřesnosti osobních údajů a minimalizaci rizika chyb, a zabezpečit osobní údaje takovým způsobem, který zohledňuje potenciální rizika pro zájmy a práva subjektu údajů a který mimo jiné předchází diskriminačním účinkům vůči fyzickým osobám na základě rasy nebo etnického původu, politických názorů, náboženského vyznání nebo přesvědčení, členství v odborech,

Nařízení poskytuje subjektům údajů ochranu před rizikem potenciálně nepříznivého rozhodnutí, které bylo přijato bez jakéhokoliv lidského zásahu, tj. výhradně na základě automatizovaného zpracování.[68] Recitál 71 uvádí jako příklad takového rozhodnutí automatické zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru pracovníků bez jakéhokoliv lidského zásahu. Nařízení přiznává subjektu údajů právo, aby nebyl předmětem rozhodnutí

- založeného výhradně na automatizovaném zpracování, včetně profilování; a
- které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

Uvedená ochrana proti automatizovanému individuálnímu rozhodování se neuplatní, pokud je rozhodnutí

a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů,

b) povoleno právem Unie nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů[69], nebo

c) založeno na výslovném souhlasu subjektu údajů.

V případech sub a) a c) provede správce údajů vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. Minimálním standardem je, že zajistí alespoň právo na lidský zásah ze strany správce, tj. aby automatizovaně přijaté rozhodnutí mohl prověřit člověk, právo subjektu údajů vyjádřit svůj názor k okolnostem přijetí rozhodnutí a právo napadnout rozhodnutí.

Automatizované rozhodování však nesmí být založeno na zvláštních kategoriích osobních údajů (tj. vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, o zdravotním stavu, sexuálním životě či orientaci, viz čl. 9 odst. 1 Nařízení), s výjimkou případů, kdy by k němu docházelo na základě

- výslovného souhlasu subjektu údajů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že uvedený zákaz nemůže být subjektem údajů zrušen;
- významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;

a pokud by byla zavedena vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.

### *Co dále*

Správci údajů by se měli – k zajištění souladu s Nařízením v rozsahu práva na přenositelnost, práva vznést námitku a práv spojených s automatizovaným rozhodováním a profilováním - ujistit, nakolik budou této úpravě podléhat (např. do jaké míry využívají profilování) a podle toho nastavit vnitřní procesy týkající se zpracovávání a procesy komunikace se subjekty údajů.

Také bude potřeba sledovat další unijní a vnitrostátní legislativu, neboť rozsah práv a oprávnění subjektů údajů a korespondujících povinností správců může být modifikován v zájmu mj. ochrany subjektu údajů nebo práv druhých či s cílem zajistit vymáhání občanskoprávních nároků.

---

genetických údajů nebo zdravotního stavu či sexuální orientace nebo předchází přijímání opatření, jež mají takové účinky.

[68] Zatím upraveno v čl. 15 Směrnice v podobě zákazu rozhodnutí, přijatého výlučně na automatizovaném zpracování údajů určeném k hodnocení určitých rysů osobnosti subjektu údajů, například pracovního výkonu, důvěryhodnosti, spolehlivost, chování, atd. Výjimka je umožněna pro rozhodnutí v rámci uzavírání nebo plnění smlouvy z podnětu subjektu údajů, anebo je-li to povoleno právním předpisem, který rovněž upřesňuje opatření zajišťující ochranu oprávněných zájmů subjektu údajů.

[69] Např. pro účely monitorování podvodů a daňových úniků a jejich předcházení, které se uskutečňuje v souladu s právními předpisy, normami a doporučeními institucí Unie nebo vnitrostátních orgánů dozoru, a pro zajištění bezpečnosti a spolehlivosti služby poskytované ze strany správce údajů.

*Další informace*

Recitály 68 – 72

Články 4 odst. 4, 20 – 23

*Lekce 10 z 16*

## Bezpečnost osobních údajů a porušení jejich ochrany

**V textu se dozvíte:**

*Důležité změny*

- Správci budou mít v případě porušení ochrany osobních údajů dvojí oznamovací povinnost - jednak vůči dozorovému úřadu, jednak vůči subjektům údajů;
- Správci budou povinni vést evidenci porušení ochrany osobních údajů.

*Compliance: Akční plán*

- Správci a rovněž zpracovatelé musí provést vhodná bezpečnostní opatření na ochranu dat při zpracování;
- Pro tento účel je nezbytné důkladně posoudit okolnosti zpracování, a to ve spolupráci s IT techniky (např. pro účely zavedení šifrování údajů);
- Doporučuje se zavést interní směrnice pro případ zjištění porušení ochrany údajů;
- Doporučuje se zvážit možnost pojištění následků případného porušení ochrany osobních údajů;
- Pokud smlouvy s dodavateli zahrnují zpracování osobních údajů (např. výplatní pásky, účetnictví), měly by obsahovat odpovědnost za bezpečnost osobních údajů[70].

### Bezpečnost osobních údajů

Nařízení stanoví minimální standard ochrany osobních údajů při jejich zpracování prostřednictvím několika institutů, resp. opatření, která je správce povinen přijmout[71]. Z Nařízením sledovaného záměru je zřejmé, že hlavním účelem nové legislativy upravující zpracování osobních údajů je zajištění jejich bezpečnosti při zpracování a minimalizace rizik – nejen před následky lidského jednání (úmyslného či nedbalostního, interního u správce či zpracovatele nebo vnějšího, mimo tyto subjekty), ale i přírodních sil nebo selhání techniky - spojených s různými operacemi zpracování.

Nařízení upravuje povinnosti související s bezpečností osobních údajů tak, že správce (a také zpracovatel) je povinen provést vhodná technická a organizační opatření, aby zajistil náležitou úroveň bezpečnosti, včetně důvěrnosti, odpovídající tomuto riziku. Tato opatření mohou zahrnovat také:

- pseudonymizaci a šifrování osobních údajů;
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

[70] Smlouva o zpracování je brána za součást bezpečnostních opatření.

[71] Jedná se zejména o povinnost vést záznamy o činnostech zpracování, povinnost přijmout přiměřená technická a organizační opatření, oznamovací povinnost v případě porušení ochrany osobních údajů, posouzení vlivu na ochranu osobních údajů, předchozí konzultace s dozorovým úřadem a pod.

- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Nařízení uvádí výše uvedená bezpečnostní opatření pouze jako příklady, tj. správce může stanovit i jiná vhodnější opatření k zajištění bezpečnosti údajů, podle svých specifických podmínek. Nařízení stanoví, jakého stavu musí správci a zpracovatelé docílit, ale nikoliv již jakými prostředky. Tato opatření však musí být zavedena s ohledem na:

- *aktuální stav techniky* – za účelem zjištění, jaké možnosti ochrany osobních údajů v době stanovování bezpečnostních opatření existují, je vhodné, aby správce konzultoval aktuální prostředky ochrany s IT specialisty. Opatření musí vykazovat náležitou odbornou úroveň. Je vhodné je poté v pravidelných intervalech obnovovat; pokud by se totiž v průběhu zpracování osobních údajů úroveň poznatků o způsobech ochrany zlepšila, nemusel by mít správce z důvodu zastaralosti ochranných systémů zajištěn soulad s Nařízením;
- *náklady na provedení opatření* – při přijímání konkrétních opatření zvažuje správce i jejich nákladnost. Argumentem není, že bezpečnostní opatření nebyla přijata vzhledem k jejich finanční, personální či časové náročnosti;
- *povahu, rozsah, kontext a účely zpracování* – při určovaní, jaká bezpečnostní opatření správce přijme, je třeba samozřejmě důkladně zvážit všechny okolnosti zpracování osobních údajů v době, kdy ke zpracování dochází; rovněž tyto okolnosti je potřeba průběžně přehodnocovat vzhledem k měnícím se podmínkám zpracování;
- *různě závažná rizika pro práva a svobody fyzických osob* – jde o důležitý aspekt zpracování, přičemž od správce se vyžaduje, aby provedl vyhodnocení jakýchkoliv možných bezpečnostních rizik spojených se zpracováním, která by mohla mít negativní dopad na práva a svobody fyzických osob. Toto posouzení rizik by mělo být provedeno zejména s ohledem na rizika vyplývající z automatizovaného zpracování (např. hackerské útoky, selhání IT techniky, neoprávněné nebo neodborné zásahy třetích osob do procesu zpracování) a s ohledem na rizika spojená s prostředím, ve kterém se data nacházejí (např. zabezpečení budov a prostor, protipožární ochrana, dostupnost serverů a jiných úložišť dat apod.). Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim[72].

Z uvedeného je zřejmé, že to, jaká konkrétní bezpečnostní opatření správce v konečném důsledku přijme, by mělo být výsledkem důkladného posouzení okolností zpracování v konkrétních podmínkách každého správce nebo zpracovatele.

Účinností Nařízení nastává podstatná změna v tom, že správci již nebudou muset vypracovat bezpečnostní projekty či dokumentaci[73], jak tomu bylo doposud. Místo toho bude potřeba – pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob - provést před zpracováním posouzení vlivu ochrany údajů (*„privacy impact assessment", „PIA"*), případně požádat dozorový úřad o konzultaci podle čl. 35 a 36 Nařízení. Tato povinnost se bude aplikovat ve specifických případech, např. při rozsáhlém systematickém monitorování veřejně přístupných míst, pokud bude správce ve velkém rozsahu zpracovávat citlivé údaje nebo osobní údaje týkající se rozsudků v trestních věcech, při profilování či automatizovaném rozhodování apod.

Pro účely zajištění a prokázání přijetí vhodných bezpečnostních opatření je možné, aby správce přistoupil k dodržování schváleného kodexu chování[74] nebo schváleného mechanismu pro vydávání osvědčení[75]. Správce je rovněž povinen zajistit, aby každá fyzická osoba jednající na základě pověření správce, která má přístup k osobním údajům (momentálně tzv. odpovědná osoba)

[72] Čl. 32 odst. 2 Nařízení.
[73] § 13 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.
[74] Čl. 40 Nařízení.
[75] Čl. 42 Nařízení.

zpracovávala tyto údaje pouze na základě pokynů správce, s výjimkou případů, kdy je po ní zpracování vyžadováno podle unijního práva nebo práva členského státu.

Podstatnou povinností správce a zpracovatele je pak důsledná kontrola plnění přijatých opatření a povinností odpovědných osob. Samotná PIA či konzultace Úřadu a následné přijetí bezpečnostních technických a organizačních opatření tedy nebude postačovat.[76]

### *Oznamování porušení zabezpečení osobních údajů*

Jakkoliv odpovědně přistupuje správce k ochraně osobních údajů, které zpracovává, nebude zřejmě možné zcela vyloučit riziko porušení jejich zabezpečení („*data breach*"). Takovým porušením se rozumí zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim[77].

Nařízení upravuje v souvislosti s porušením ochrany osobních údajů dva druhy oznamovací povinnosti správců:

#### a) *Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu*

V případě porušení zabezpečení osobních údajů je správce povinen v první řadě ohlásit tuto skutečnost dozorovému úřadu příslušnému podle čl. 55 Nařízení. Toto ohlášení je třeba učinit bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl. Pokud není ohlášení učiněno ve stanovené době, musí být současně s ním uvedeny důvody tohoto zpoždění.

Pokud není správce schopen z objektivních příčin poskytnout dozorovému úřadu informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Ohlášení musí obsahovat přinejmenším:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Správce není povinen ohlásit porušení dozorovému úřadu, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

#### b) *Oznamování případů porušení zabezpečení osobních údajů subjektu údajů*

Pokud dojde k porušení zabezpečení osobních údajů, které bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, je správce povinen toto porušení bez zbytečného odkladu oznámit subjektu údajů.

---

[76] Kontrola nemusí být specializovaná na ochranu osobních údajů, může být součástí uplatňování práva a povinnosti vedoucích pracovníků kontrolovat v rámci pracovně-právních vztahů práci podřízených zaměstnanců. Možností je také využití již standardních automatizovaných prostředků, např. tzv. logů (záznamů o přístupu konkrétní osoby do systému).

[77] Čl. 32 odst. 2 Nařízení.

V oznámení správce za použití jasných a jednoduchých jazykových prostředků popíše povahu porušení zabezpečení osobních údajů a uvede přinejmenším tyto informace a opatření:

- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů; a
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Také v tomto případě Nařízení upravuje výjimku, kdy správce není povinen porušení oznámit subjektu údajů. Oznámení se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

- správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
- vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil.

### *Zdokumentování porušení zabezpečení osobních údajů*

Kromě výše uvedené oznamovací povinnosti je správce povinen také interně zdokumentovat každý případ porušení zabezpečení osobních údajů včetně skutečností s porušením zabezpečení osobních údajů spojených, jeho následky a opatření přijatá k nápravě a tyto dokumenty uchovávat.

Mimo to je správce povinen splnit také určitý komunikační (tj. dokumentační standard při ohlašování porušení dozorovému úřadu a oznamování subjektům údajů (náležitosti těchto oznámení viz výše).

### *Co dále*

Správci i zpracovatelé by měli před účinností Nařízení prověřit svá dosavadní interní technická a organizační opatření z hlediska nových požadavků, vyhodnotit znovu míru rizik s ohledem na stávající stav techniky, nákladovost opatření a povahu zpracovávaných osobních údajů, aktualizovat svá dosavadní bezpečnostní opatření a kontrolní a odpovědnostní mechanismy, zajistit řádnou evidenci a postupy pro včasné hlášení případných bezpečnostních incidentů. Shledají-li vysoké riziko pro práva a svobody fyzických osob, měli by provést PIA, příp. konzultovat Úřad. Uvedené kroky by měli také být schopni zpětně doložit a zdůvodnit v zájmu průkaznosti a své liberace z případné odpovědnosti jak soukromoprávní (za újmu subjektů údajů či dotčených osob), tak veřejnoprávní (za správní delikt) či trestněprávní odpovědnosti (např. trestný čin neoprávněného nakládání s osobními údaji).

*Další informace*

Recitály 83 - 94

Články 32 - 34

*Lekce 11 z 16*

## Kodexy chování a vydávání osvědčení

**V textu se dozvíte:**

*Důležité změny*

- Nařízení přináší nové instituty k zajištění a prokázání skutečnosti, že zpracování je v souladu s Nařízením, a to:
    - kodexy chování, a
    - mechanismy pro vydávání osvědčení, pečetí nebo známek;
- Prostřednictvím kodexů chování mají správci a zpracovatelé možnost snáze zajistit a dodržovat soulad s Nařízením;
- Dodržování kodexů chování bude monitorováno akreditovanými subjekty; bude-li zjištěno porušení kodexu, může být správce či zpracovatel vyloučen z účasti na kodexu;
- Mechanismy pro vydávání osvědčení, pečetí nebo známek jsou určeny pro dobrovolnou „samoregulaci" správce nebo zpracovatele;
- Bude-li správce nebo zpracovatel disponovat kodexem nebo osvědčením atd., bude to svědčit o souladu s Nařízením, a to po dobu 3 let (platnost osvědčení bude možné prodloužit).

*Compliance: Akční plán*

Správci a zpracovatelé by měli:

- monitorovat, zda neexistují v jejich odvětví schválené kodexy chování platné v rámci ČR nebo EU;
- zjistit, zda existují mechanismy pro vydávání osvědčení, pečetí nebo známek, které by mohli získat a prokázat tak soulad s Nařízením;
- seznámit se s osvědčeními, pečetěmi nebo známkami, které budou postupně zaváděny, a zohledňovat tyto instituty při výběru svých zpracovatelů nebo subdodavatelů.

### Kodexy chování

Nařízení upravuje kodexy chování jako dokumenty, vypracované sdruženími nebo jinými subjekty zastupujícími různé kategorie správců nebo zpracovatelů. Kodexy upravují zpracování osobních údajů specifické pro tyto skupiny správců nebo zpracovatelů. Mají přispět k řádnému uplatňování Nařízení s ohledem na konkrétní povahu různých odvětví a na konkrétní potřeby mikropodniků a malých a středních podniků.

Kodexy tak budou mít význam pro správce a zpracovatele, kteří budou jejich dodržováním jednodušeji a spolehlivě zajišťovat a prokazovat dozorovým úřadům soulad s Nařízením.

To, že se správce nebo zpracovatel zaváže dodržovat schválený kodex chování, může mít několik pozitivních účinků:

- prostřednictvím kodexů budou zavedeny doporučené postupy, jak v daném odvětví a ve specifickém kontextu zpracovávání nakládat s osobními údaji;
- budou se moci spolehnout, že zpracovávání provozují zákonným způsobem, což může ušetřit např. náklady na odborné poradce;

- účast na schváleném kodexu bude u subjektů údajů vzbuzovat důvěru, že jejich údaje jsou zpracovávány zákonným způsobem;
- spolu se závazkem příjemce údajů, sídlícího mimo EU, přijmout vhodné záruky budou kodexy použitelné při zajišťování zákonnosti přenosu údajů mimo EU, podobně jako standardní smluvní doložky a závazná vnitropodniková pravidla; a
- dozorovému úřadu bude snadno prokazatelný soulad s Nařízením.

Sdružení nebo jiný subjekt zastupující různé kategorie správců nebo zpracovatelů může tudíž vypracovat kodex chování relevantní pro daný sektor nebo odvětví. Kodex má sloužit jako „návod" pro společnosti působící v daném odvětví, jak správně zpracovávat osobní údaje pro jejich odvětví specifické, např. subjekty působící v oblasti bankovnictví, zdravotnictví, školství, farmaceutického průmyslu, maloobchodu, IT a cloudových služeb atd.

Kodexy mohou upravovat doporučené postupy například v souvislosti se spravedlivým a transparentním zpracováním, oprávněnými zájmy, jež správci v konkrétních situacích sledují, shromažďováním osobních údajů, pseudonymizací osobních údajů, informacemi poskytovanými veřejnosti a subjektům údajů, výkonem práv subjektů údajů, informacemi poskytovanými dětem a jejich ochraně a způsobem získávání souhlasu nositele rodičovské zodpovědnosti nad dítětem, opatřeními a postupy účelnými pro přijetí vhodných technických a organizačních opatření a specificky navržené a standardní ochrany údajů, opatřeními k zajištění bezpečnosti zpracování, ohlašováním případů porušení zabezpečení osobních údajů dozorovým úřadům a oznamováním těchto případů porušení subjektům údajů, předáváním osobních údajů do třetích zemí nebo mezinárodním organizacím a mimosoudním vyrovnáním a jinými postupy pro řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním.

### *Schvalování kodexů*

K tomu, aby měl kodex chování vyšší právní účinky, je třeba schválení příslušným dozorovým úřadem. Proces schválení se odvíjí od toho, zda se jedná o kodex s vnitrostátní platností, nebo zda má mít kodex všeobecnou platnost v rámci Unie.

Pokud jde o kodex, který se netýká činností zpracování mimo určitý stát (např. ČR), je třeba jeho návrh předložit příslušnému dozorovému úřadu (v tomto případě Úřadu pro ochranu osobních údajů ČR). Úřad vydá stanovisko, zda je daný návrh kodexu v souladu s Nařízením, a pokud shledá, že poskytuje dostatečné vhodné záruky, návrh schválí. Dozorový úřad také daný kodex zaregistruje a zveřejní.

Jedná-li se naopak o kodex, který se týká činností zpracování v několika členských státech, předloží příslušný dozorový úřad návrh kodexu v rámci spolupráce dozorových úřadů států Unie a Komise Evropskému sboru pro ochranu osobních údajů („Sbor"), který vydá stanovisko, zda je návrh kodexu v souladu s Nařízením nebo zda poskytuje vhodné záruky. Pokud Sbor potvrdí, že návrh kodexu je v souladu s Nařízením či poskytuje vhodné záruky, předloží své stanovisko Komisi. Komise může svým prováděcím aktem rozhodnout, že schválený kodex chování, který jí byl předložen, má všeobecnou platnost v rámci Unie. Komise zajistí odpovídající zveřejnění těchto kodexů s všeobecnou platností. Sbor schválené kodexy chování shromáždí a vhodným způsobem je zpřístupní veřejnosti.

### *Monitorování dodržování kodexů*

Kromě příslušného dozorového úřadu může monitorování souladu s kodexem chování provádět subjekt, který má o předmětu kodexu odpovídající odborné znalosti a je pro tento účel akreditován příslušným dozorovým úřadem. Tento subjekt musí:

- prokázat nezávislost a odborné znalosti o předmětu kodexu;

- stanovit postupy, které mu umožňují posoudit způsobilost dotčených správců a zpracovatelů, pokud jde o uplatňování kodexu, monitorovat, zda jeho ustanovení dodržují, a pravidelně přezkoumávat jeho činnost;
- stanovit postupy a struktury pro řešení stížností na porušování kodexu nebo na způsob, jak správce nebo zpracovatel kodex uplatňoval nebo uplatňuje, a zajistit transparentnost těchto postupů a struktur pro subjekty údajů a pro veřejnost; a
- prokázat, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

Kritéria pro akreditaci určí příslušný dozorový úřad po konzultaci s Evropským sborem pro ochranu osobních údajů. Pokud akreditovaný subjekt zjistí porušení kodexu, může správci nebo zpracovateli uložit sankci v podobě vhodných opatření, včetně pozastavení jejich účasti na kodexu nebo vyloučení z této účasti.

**Vydávání osvědčení**

Mechanismy pro vydávání osvědčení a zavedení pečetí a známek upravuje Nařízení jako další nové instituty ochrany osobních údajů. Tyto mechanismy mají sloužit zejména k zvýšení transparentnosti zpracování a mají pomoci subjektům údajů při rychlém posouzení úrovně ochrany osobních údajů v případě relevantních produktů a služeb. Jako příklad je možno uvést situaci, kdy se pro určitou službu, např. poskytování cloudových služeb, zavedou pečetě nebo známky, které budou znamenat, že subjekt, který je získá, splňuje požadavky Nařízení pro zákonné zpracování[78].

Vydávání osvědčení pro zpracování osobních údajů je důležitým mezníkem pro vytvoření spolehlivého a transparentního rámce zpracování. Tyto mechanismy mohou být zavedeny členskými státy, ale i dozorovými úřady, Sborem či Komisí. Měly by být použitelné především na úrovni Unie, ale není vyloučena ani vnitrostátní platnost. Zohledněny by měly být specifické potřeby mikropodniků a malých a středních podniků.

Vydání osvědčení je dobrovolné, ale nesnižuje odpovědnost správce nebo zpracovatele za soulad s Nařízením. Jinak řečeno, pokud např. správce získá osvědčení, ale navzdory tomu zpracováním poruší Nařízení, osvědčení ho nezbavuje odpovědnosti. Osvědčení se vydává na dobu nejvýše tří let a lze je obnovit za stejných podmínek, pokud jsou i nadále plněny příslušné požadavky. Obdobně, nejsou-li požadavky na osvědčení plněny, může být osvědčení subjektu odebráno.

Osvědčení může mít pro správce a zpracovatele následující výhody:

- správci a zpracovatelé budou moci snáze prokázat soulad s Nařízením, a to především v souvislosti s přijetím vhodných technických a organizačních opatření;
- subjekty údajů, případně zákazníci, kteří se budou rozhodovat pro dodavatele služeb, mohou k osvědčení přihlížet jako k důkazu věrohodnosti a profesionality poskytovatele (např. cloudových) služeb; a
- obdobně jako v případě kodexů, spolu se závazkem příjemce údajů sídlícího mimo EU přijmout vhodné záruky budou osvědčení použitelná při zajišťování zákonnosti přenosu údajů mimo EU, podobně jako standardní smluvní doložky a závazná vnitropodniková pravidla

Nařízení přiznává pravomoc vydávat osvědčení kromě dozorových úřadů také subjektům pro vydávání osvědčení, které získají pro tuto činnost akreditaci. V českých podmínkách bude Úřad pro ochranu osobních údajů oprávněn udělit akreditaci subjektům pro vydávání osvědčení. Pro získání akreditace musí subjekt pro vydávání osvědčení splnit kritéria stanovená Nařízením, mimo jiné:

- prokázat nezávislost a odborné znalosti o předmětu osvědčení;
- zavázat se respektovat kritéria schválená Sborem nebo příslušným dozorovým úřadem;

[78] Pro porozumění je možno uvést např. značku ISO, která dokazuje, že subjekt v dané oblasti dosahuje kvalit požadovaných tímto certifikátem.

- stanovit postupy pro vydávání, pravidelný přezkum a odebírání osvědčení, pečetí a známek dokládajících ochranu údajů;
- stanovit postupy a struktury pro řešení stížností týkajících se porušování osvědčení nebo způsobu, jak správce nebo zpracovatel osvědčení uplatňoval nebo uplatňuje, a zajistit transparentnost těchto postupů a struktur pro subjekty údajů a pro veřejnost; a
- doložit, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

Akreditace se vydává na období nejvýše pěti let a lze ji obnovit.

*Co dále*

Správci a zpracovatelé mohou významně těžit z účasti na schválených kodexech chování (platných vnitrostátně nebo v rámci Unie), nebo z vydávání osvědčení nebo zavedení pečetí a známek, které budou průběžně zaváděny po nabytí účinnosti Nařízení. Z uvedeného důvodu lze doporučit, aby správci a zpracovatelé monitorovali zavádění těchto institutů, aby se mohli včas rozhodnout, zda se jich budou chtít účastnit nebo je získat.

*Další informace*

Recitály 77, 81, 98 – 100, 148, 166, 168,

Články 40 – 43, 57 odst. 1 písm. p), q), odst. 3 písm. e), 64 odst. 1 písm. c), 70 odst. 1 písm. o), p)

*Lekce 12 z 16*

## Předávání osobních údajů mimo EU/EHS

**V textu se dozvíte:**

*Důležité změny*

- Požadavky Nařízení pro předávání údajů se budou týkat zejména nadnárodních společností nebo společností, které využívají služby zahrnující předávání údajů do třetích zemí (např. cloudové služby);
- V porovnání s předchozí právní úpravou se zavádějí nové možnosti, jak zajistit zákonnost předávání údajů mimo EU/EHS;

*Compliance: Akční plán*

Správci a zpracovatelé by měli:

- prověřit toky osobních údajů, které zpracovávají;
- pokud se údaje předávají mimo EU/EHS, prověřit, zda jsou přijaty mechanismy k zajištění zákonnosti předání (např. standardní smluvní doložky, závazná vnitropodniková pravidla apod.);
- prověřit, zda a kam předávají osobní údaje dodavatelé služeb, jimž správci nebo zpracovatelé poskytují údaje;
- pokud se předávání uskutečňovalo na základě „Bezpečného přístavu", určit jiný právní základ předávání, neboť Bezpečný přístav byl zrušen.

### Předávání osobních údajů mimo EU/EHS

Podobně jako předchozí právní úprava, také Nařízení upravuje podmínky předávání osobních údajů do třetích zemí (mimo EU/EHS) a do mezinárodních organizací[79]. Důvodem je skutečnost, že jakmile osobní údaje opustí území, kde se uplatňuje právní řád EU, stanou se předmětem právní úpravy cizích právních předpisů, které nemusí zaručovat ochranu osobních údajů na úrovni srovnatelné s právem EU. Tato problematika se proto bude týkat zejména nadnárodních společností, nebo společností, které využívají služby dodavatelů působících mimo Unii (např. pokud využívají cloudové služby serverů umístěných ve třetích zemích). Tato problematika se naopak nebude týkat společností, které údaje nepředávají, anebo je předávají pouze v rámci EU/EHS.

Východisko pro porozumění potřebnosti úpravy předávání údajů mimo EU uvádí recitál 101 Nařízení, podle něhož jsou toky osobních údajů se státy mimo Unii a s mezinárodními organizacemi potřebné pro rozvoj mezinárodního obchodu a spolupráce. Nárůst těchto toků s sebou přinesl nové výzvy a potřeby týkající se ochrany osobních údajů. Úroveň ochrany údajů fyzických osob, zaručovaná Unií na základě Nařízení, by neměla být ohrožena, ani pokud jsou osobní údaje předávány z Unie správcem, zpracovatelem nebo jiným příjemcem v třetích zemích nebo mezinárodním organizacím, a to ani v případech následného předání osobních údajů z třetí země anebo mezinárodní organizace správcem, zpracovatelem v téže nebo v jiné třetí zemi anebo mezinárodní organizaci.

Předávání osobních údajů do třetích zemí bude možné za splnění některé z následujících podmínek:

*Předání založené na rozhodnutí o odpovídající ochraně*

[79] Čl. 4 odst. 26 Nařízení: *„organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě."*

Evropská komise („Komise") může rozhodnout, že určitá třetí země, území nebo jeden či více určených sektorů v dané třetí zemi nebo mezinárodní organizace zaručují odpovídající úroveň ochrany.[80] K předání do takové země pak není nutné žádné zvláštní povolení. Přezkum okolností, na základě nichž Komise rozhodnutí vydala, se provádí nejméně jednou za čtyři roky.

Pokud Komise zjistí, že podmínky mající dopad na ochranu osobních údajů v třetí zemi (příp. mezinárodní organizaci) se zhoršily, rozhodne, že takový stát již nezaručuje odpovídající úroveň ochrany. Uvedené rozhodnutí však nemá retroaktivní účinek, tzn. je účinné nejdříve v den jeho přijetí. Proto zůstává otázkou bezpečnost již předaných údajů.

Seznam třetích zemí a mezinárodních organizací, které podle rozhodnutí Komise zaručují odpovídající úroveň ochrany anebo ji už přestaly zaručovat, Komise uveřejní v Úředním věstníku Evropské unie a na svém webovém portálu.[81] Aktuálně jsou zeměmi, které zaručují odpovídající úroveň ochrany údajů, Andora, Argentina, Kanada, Švýcarsko, Faerské ostrovy, ostrovy Guernsey, Man a Jersey, Izrael, Nový Zéland a Uruguay.

Předání údajů do Spojených států amerických má určitá specifika. Do roku 2015 bylo předání do USA možné mimo jiné i prostřednictvím schématu tzv. Bezpečného přístavu[82], který umožňoval předávat osobní údaje subjektům nacházejícím se v USA a registrovaným v Bezpečném přístavu bez dalších opatření a formalit. Dne 6. října 2015 však vydal Velký senát SD EU rozhodnutí[83], jímž zrušil rozhodnutí Komise upravující Bezpečný přístav, a předávání osobních údajů do USA na základě tohoto legislativního aktu není proto považováno za zákonné.[84]

Uvedené schéma bylo proto následně nahrazeno schématem tzv. „Privacy shield" – Štít soukromí [85], jež Komise schválila dne 12. června 2016. Seznam společností, které se zavázaly dodržovat zásady ochrany osobních údajů zavedené prostřednictvím Privacy shield, je zveřejněný na stránce Ministerstva obchodu (Department of Commerce) USA [86].

### *Předávání založené na vhodných zárukách*

Jestliže neexistuje výše uvedené rozhodnutí Komise, může se předávání osobních údajů do třetí země nebo mezinárodní organizace uskutečnit pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva a účinné právní prostředky ochrany subjektů údajů. Vhodné záruky mohou být stanoveny aniž by bylo potřeba žádat dozorový úřad o nějaké zvláštní povolení, prostřednictvím:

- právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnoprávními subjekty;

---

[80] Při posuzování odpovídající úrovně ochrany Komise zohledňuje takové skutečnosti, jako např. právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, jakož i aplikaci těchto právních předpisů, pravidel ochrany údajů, profesních pravidel a bezpečnostních opatření včetně pravidel pro následné předání osobních údajů do dalšího třetího státu nebo mezinárodní organizace, účinné správní a soudní prostředky nápravy, existenci a účinné působení nezávislých dozorových orgánů, mezinárodní závazky apod.

[81] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[82] Rozhodnutí Komise 2000/520/EC z 26. července 2000, které obsahovalo zásady a požadavky, týkající se ochrany osobních údajů, jimž se společnosti registrované v USA mohly dobrovolně podřídit a být tak ohledně nakládání s osobními údaji považovány za spolehlivé.

[83] http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=sk&lang2=EN&type=TXT&ancre=

[84] Stalo se tak na základě podnětu rakouského občana Maxe Schremse, který byl od roku 2008 uživatelem služeb Facebook. Facebook přitom předával osobní údaje svých uživatelů na servery nacházející se v USA, kde se dále zpracovávaly. P. Schrems podal stížnost dozorovému orgánu v Irsku, jehož smyslem bylo, že podle informací zveřejněných Edwardem Snowdenem v roce 2013 ohledně způsobu, jakým americké bezpečnostní složky (zejména NSA – National Security Agency) nakládají s osobními údaji v jejich jurisdikci (t.j. rovněž evropských uživatelů Facebooku), Spojené státy americké nezaručují ochranu před sledováním ze strany amerických orgánů. Dozorový orgán v Irsku stížnost odmítl s odvoláním se na záruky, které se subjekt USA zavázaly poskytnout prostřednictvím Bezpečného přístavu. Po přezkoumání merita věci SD EU schéma Bezpečného přístavu zrušil.

[85] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

[86] https://www.privacyshield.gov/welcome

- závazných vnitropodnikových pravidel (viz níže);

  Jestliže se jedná o holdingovou společnost, která má pobočky v Unii a ve třetích státech, může se předání údajů v rámci tohoto holdingu provádět i na základě závazných vnitropodnikových pravidel. V takovém případě musí být schváleny příslušným dozorovým úřadem, na základě něhož se stanou závaznými nejen v jurisdikci dozorového úřadu, který je schválil, ale ve všech dalších jurisdikcích, v nichž má holding pobočky. Dozorový úřad pravidla schválí, pokud:

  - jsou právně závazná a vztahují se na každý subjekt údajů skupiny podniků nebo podniků zapojených do společné hospodářské činnosti včetně jejich zaměstnanců, a tito členové je prosazují;
  - pokud se jimi výslovně přiznávají vymahatelná práva subjektům údajů, jde-li o zpracování jejich osobních údajů; a
  - upravují Nařízením určené náležitosti, mezi jiným např. strukturu a kontaktní údaje skupiny podniků anebo podniků zapojených do společné hospodářské činnosti a každého z jejích členů, předání údajů nebo soubor předání včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo zemí, jejich právní závaznost, a to uvnitř i navenek, práva subjektů údajů v souvislosti se zpracováním a prostředky k uplatnění těchto práv, postupy týkající se vyřizování stížností, mechanismus spolupráce s dozorovým úřadem k zajištění dodržování pravidel ze strany všech členů skupiny apod.;

- standardních doložek o ochraně údajů, které přijala Komise nebo které přijal dozorový úřad a které následně schválila Komise; doložky, které existovaly před přijetím Nařízení, zůstávají v platnosti[87];

  I když správci či zpracovatelé použijí k předání mimo Unii standardní smluvní doložky, mohou je zahrnout do širší smlouvy, jako například smlouvy mezi zpracovatelem a dalším zpracovatelem, nebo doplnit jiné doložky či další záruky, pokud tyto nejsou v přímém nebo nepřímém rozporu se standardními smluvními doložkami nebo pokud se nedotýkají základních práv či svobod subjektů údajů;

- schváleného kodexu chování (jde o nový institut – viz Lekce 11) spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele v třetí zemi spočívajícími v uplatňování vhodných záruk, a to i pokud jde o práva subjektů údajů, anebo

- schváleného mechanismu pro vydávání osvědčení (jde o nový institut – viz Lekce 11) spolu se závazným a vymahatelným závazkem správce nebo zpracovatele v třetí zemi, spočívajícím v uplatňování vhodných záruk, a to i pokud jde o práva subjektů údajů.

*Výjimky*

Jestliže neexistuje rozhodnutí o odpovídající ochraně nebo pokud neexistují vhodné záruky, předání osobních údajů do třetí země nebo mezinárodní organizaci se může uskutečnit, pokud je splněna některá z těchto podmínek:

- subjekt údajů vyjádřil výslovný souhlas s navrhovaným předáním;
- předání je nezbytné k plnění smlouvy mezi subjektem údajů a správcem nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů;
- předání je nezbytné pro uzavření nebo splnění smlouvy, uzavřené v zájmu subjektu údajů mezi správcem a jinou fyzickou nebo právnickou osobou;
- předání je nezbytné z důležitých důvodů veřejného zájmu;
- předání je nezbytné pro určení, výkon nebo obhajobu právních nároků;

[87] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

- předání je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiných osob, pokud je subjekt údajů fyzicky nebo právně nezpůsobilý souhlas udělit;
- k předání dochází z rejstříku, který je podle práva Unie nebo práva členského státu určený k poskytování informací veřejnosti a který je přístupný k nahlížení veřejnosti nebo jakékoliv osobě, která prokáže oprávněný zájem, ale jen pokud jsou v tomto konkrétním případě splněny podmínky pro nahlížení stanovené právem Unie nebo právem členského státu.

Předání do třetí země nebo mezinárodní organizace se může uskutečnit rovněž tehdy, nemá-li předání opakující se povahu, týká se jen omezeného počtu subjektů údajů, je nezbytné pro účely závažných oprávněných zájmů správce, nad nimiž nepřevažují zájmy nebo práva a svobody subjektu údajů, a správce posoudil všechny okolnosti provázející předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů. V takovém případě však správce musí informovat o předání dozorový úřad.

*Co dále*

Správci a zpracovatelé musí prověřit, zda předávají osobní údaje mimo EU/EHS, případně zda taková předání realizují jejich dodavatelé služeb anebo zboží. Následně je také třeba předávání založit na některém z platných právních základů, a to zejména na základě rozhodnutí o odpovídající ochraně anebo na základě vhodných záruk. Pokud není možné předání odůvodnit některým z uvedených právních základů, je třeba prověřit, zda se na předání může aplikovat některá výjimka z této povinnosti.

*Další informace*

Recitály 6, 23, 101 - 116

Články 44 – 49

*Lekce 13 z 16*

## Dozor nad zpracováním osobních údajů

**V textu se dozvíte:**

*Důležité změny*

- Správci a zpracovatelé budou v určených případech podléhat nejen dozorovému úřadu na ochranu osobních údajů „vlastního" státu, ale mohou podléhat i orgánu dozoru jiného státu Unie, který bude mít postavení vedoucího dozorového úřadu;
- Zřizuje se nový orgán EU – Evropský sbor pro ochranu osobních údajů.

*Compliance: Akční plán*

Správci a zpracovatelé by se měli:

- seznámit s rozsáhlými kompetencemi dozorových úřadů;
- pokud provádějí přeshraniční zpracování, doporučuje se seznámit se se způsobem fungování a spolupráce vedoucího dozorového úřadu a lokálních dozorových úřadů.

**Dozor nad zpracováním osobních údajů**

Dozor nad zpracováním osobních údajů je další velkou kapitolou problematiky osobních údajů. Podle recitálu 117 Nařízení je zřízení dozorových úřadů v členských státech *„(...) zásadním prvkem ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů*". Úkolem dozorových úřadů je tedy vykonávat dohled a případně autoritativně zajišťovat soulad s Nařízením za účelem ochrany práv a základních svobod subjektů údajů, jejichž údaje se zpracovávají.

V oblasti dohledu nad zpracováním osobních údajů zavádí Nařízení několik nových konceptů a dokonce též jednu novou instituci, v níž budou mít zastoupení všechny státy Unie. Pro správce a zpracovatele bude důležité se zorientovat, kterým úřadům budou podléhat v rozsahu jakých zpracovatelských operací, a případně jaké povinnosti budou mít vůči těmto úřadům.

*Vnitrostátní dozorové úřady*

V první řadě budou správci a zpracovatelé podléhat vnitrostátnímu úřadu dozoru nad ochranou osobních údajů. V podmínkách ČR jde o Úřad na ochranu osobních údajů.[88]

Vnitrostátní dozorový úřad bude příslušný provádět zejména dozor nad zpracováním:

- v souvislosti s činnostmi provozovny správce nebo zpracovatele na území jejich členského státu.

  Vnitrostátní dozorový úřad tudíž nebude bez dalšího příslušný vykonávat dozor nad přeshraničním zpracováním osobních údajů v rámci dvou a více států Unie (pro takové zpracování viz část *„Vedoucí dozorový úřad*" níže), ale pouze nad zpracovatelskými operacemi prováděnými v rámci jednoho státu (a to i tehdy, jde-li o správce nebo zpracovatele, který jinak provádí i přeshraniční zpracování);
- které provádějí orgány veřejné moci nebo soukromé subjekty jednající ve veřejném zájmu.

[88] Web: https://www.uoou.cz/.

Standardně půjde např. o zpracovatelské operace orgánů státní správy a samosprávy. Dozorové úřady však nebudou příslušné k dozoru nad zpracovatelskými operacemi soudů při výkonu soudní pravomoci;

- které se dotýká subjektů údajů na jejich území.

  Pravomoc vnitrostátního dozorového úřadu bude daná vždy, půjde-li o práva subjektu údajů nacházejícího se na jeho území, tj. bez ohledu na to, zda jde o vnitrostátní anebo přeshraniční zpracování (výjimka z pravidla uvedeného v prvním bodě výše). Každý dozorový úřad bude příslušný zabývat se u něho podanými stížnostmi nebo případným porušením Nařízení, pokud se daná záležitost týká pouze provozovny v jeho členském státě nebo jsou podstatným způsobem dotčeny subjekty údajů pouze v jeho členském státě;

- prováděným správcem nebo zpracovatelem neusazeným v Unii, pokud cílí na subjekty údajů s pobytem na území Unie.

  Tento druh kontrolní pravomoci se týká rozšířené teritoriální působnosti Nařízení (viz Lekce 1). To znamená, že vnitrostátní orgán bude mít pravomoc např. nad čínským správcem neusazeným v EU, který však v některém státě Unie nabízí zboží nebo služby.

### *Vedoucí dozorový úřad*

Jestliže správce nebo zpracovatel zpracovává osobní údaje přeshraničně (ať již prostřednictvím jedné nebo několika poboček v rámci Unie), bude podléhat též vedoucímu dozorovému úřadu, který je příslušný jako vedoucí dozorový úřad pro přeshraniční zpracování. Zpracovatelské operace, které nezahrnují přeshraniční prvek, budou nadále podléhat vnitrostátnímu dozorovému úřadu; pokud však půjde o přeshraniční zpracování, bude příslušným vedoucí dozorový úřad.

Každý (a rovněž jiný než vedoucí) dozorový úřad bude však příslušný zabývat se u něho podanou stížností nebo případným porušením Nařízení, pokud se daná záležitost týká pouze provozovny v jeho členském státě anebo jsou tam podstatným způsobem dotčeny subjekty údajů. To znamená, že i když půjde o přeshraniční zpracování, každý dozorový úřad může za uvedených podmínek jednat. Dozorový úřad však o této skutečnosti nejprve bezodkladně informuje vedoucí dozorový úřad, který rozhodne, zda se bude nebo nebude případem zabývat.

Rozhodne-li se vedoucí dozorový úřad že se případem nebude zabývat, příslušným bude vnitrostátní dozorový úřad. Jakmile však vedoucí dozorový úřad rozhodne, že se případem bude zabývat, dozorový úřad, který jej informoval, mu může předložit návrh rozhodnutí, a vedoucí dozorový úřad bude postupovat následujícím způsobem:

### *Spolupráce mezi vedoucím dozorovým úřadem a jinými dotčenými dozorovými úřady*

- *Spolupráce a výměna informací*: vedoucí dozorový úřad spolupracuje s jinými dotčenými dozorovými úřady s cílem dosažení shody. Vedoucí dozorový úřad a dotčené dozorové úřady si navzájem vyměňují všechny relevantní informace.

- *Předložení návrhu rozhodnutí k vyjádření dotčeným dozorovým úřadům*: vedoucí dozorový úřad bezodkladně sdělí informace o věci jiným dotčeným dozorovým úřadům. Bezodkladně předloží jiným dotčeným dozorovým úřadům návrh rozhodnutí k vyjádření a pro náležité zohlednění jejich stanovisek.

    - *Předložení věci Sboru*: jestliže kterýkoliv z jiných dotčených dozorových úřadů podá ve lhůtě čtyř týdnů relevantní a odůvodněnou námitku vůči návrhu rozhodnutí, vedoucí dozorový úřad, pokud s takovou námitkou nesouhlasí nebo má za to, že je irelevantní nebo neodůvodněná, předloží záležitost Evropskému sboru pro ochranu osobních údajů („Sbor").

    - *Předložení revidovaného návrhu k vyjádření dotčeným dozorovým úřadům:* Pokud vedoucí dozorový úřad bude chtít podané relevantní a odůvodněné námitce

vyhovět, předloží dalším dotčeným dozorovým úřadům revidovaný návrh rozhodnutí k zaujetí stanoviska.

- *Vydání rozhodnutí: v*edoucí dozorový úřad vydá rozhodnutí a sdělí je hlavní provozovně nebo jediné provozovně správce, případně zpracovatele, a o daném rozhodnutí včetně shrnutí relevantních skutečností a důvodů informuje další dotčené dozorové úřady a Sbor. Dozorový úřad, u něhož byla podána stížnost, informuje o daném rozhodnutí stěžovatele. Bude-li stížnost odmítnuta nebo zamítnuta, dozorový úřad, u něhož byla stížnost podána, vydá rozhodnutí, oznámí ho stěžovateli a informuje o něm správce.

- *Zajištění souladu:* vedoucí dozorový úřad dohlédne, aby správce nebo zpracovatel přijali potřebná opatření k zajištění souladu s rozhodnutím, pokud jde o zpracovatelské činnosti v souvislosti se *všemi* jeho provozovnami v Unii. Správce nebo zpracovatel sdělí opatření, přijatá k splnění rozhodnutí vedoucímu dozorovému úřadu, který o tom informuje jiné dotčené dozorové úřady.

Pravidla pro určení vedoucího dozorového úřadu správců nebo zpracovatelů, včetně širšího pojednání o problematice s příklady, obsahuje dokument, připravený WP 29.[89]

### *Evropský sbor pro ochranu osobních údajů*

Nařízení upravuje postavení nového nezávislého orgánu s vlastní právní subjektivitou – Evropského sboru pro ochranu osobních údajů („Sbor"). Sbor má postavení orgánu Unie a je tvořen zástupci dozorových úřadů jednotlivých států Unie a evropským inspektorem ochrany údajů[90].

I když správci a zpracovatelé nebudou přímo podléhat dozoru Sboru, může mít Sbor vliv na zpracování osobních údajů, které vykonávají. Sbor má řadu úkolů, především však zajišťuje konzistentní provádění Nařízení. K tomuto účelu v rámci mechanismu konzistentnosti spolupracuje s dozorovými úřady členských států při vydávání rozhodnutí napříč Unií.

### *Co dále*

Pro správce i zpracovatele, kteří zpracovávají osobní údaje pouze v rámci jednoho členského státu, bude relevantní pouze dohled ze strany dozorového úřadu v tomto státě.

Bude-li docházet k přeshraničnímu zpracování údajů, je důležité si uvědomit, že tyto zpracovatelské operace mohou rovněž podléhat dozoru vedoucího dozorového úřadu. Správci a zpracovatelé by měli být v tomto případě připraveni komunikovat též s jiným než místním dozorovým úřadem.

### *Další informace*

Recitály 117 – 140

Články kapitol VI a VII

[89] Guidelines for identifying a controller or processor´s lead supervisory authority; přijato Article 29 Data Protection Working Party 13. 12. 2016, revidováno 5. 4. 2017, WP 244 rev. 01.
[90] "European Data Protection Supervisor"

*Lekce 14 z 16*

# Právní ochrana

**V textu se dozvíte:**

*Důležité změny*

Subjekty údajů (v některých případech také jiné osoby, např. správci) mají k dispozici následující prostředky právní ochrany:

- právo podat stížnost u dozorového úřadu;
- právo podat žalobu vůči rozhodnutí dozorového úřadu;
- právo podat žalobu vůči správci nebo zpracovateli;
- právo na náhradu majetkové i nemajetkové újmy.

*Compliance: Akční plán*

- Správci a zpracovatelé by si měli účinnými smluvními prostředky podrobně mezi sebou vymezit rozsah povinností, sankce za jejich porušení, způsob řešení sporů a vztahy odpovědnosti vůči subjektům údajů.
- Společní správci by si měli dohodnout rozsah svých povinností k dosažení souladu s Nařízením, rozsah odpovědnosti za porušení Nařízení, způsob řešení sporů a způsob náhrady odpovědnosti za škodu (újmu).

**K právní ochraně**

*Právo podat stížnost u dozorového úřadu*

V první řadě Nařízení přiznává subjektu údajů právo podat stížnost u dozorového úřadu, pokud se domnívá, že zpracování jeho osobních údajů je v rozporu s Nařízením. Účelem tohoto právního prostředku je ochránit práva, která Nařízení přiznává subjektům údajů, před porušováním správci nebo zpracovateli.

Jak jsme uvedli v Lekci 13, mohou zpracovatelské operace správce podléhat minimálně dvěma dozorovým úřadům, a to úřadu příslušnému podle místa sídla správce, nebo vedoucímu dozorovému úřadu, příslušnému k dohledu nad zpracovatelskými operacemi správce nebo skupiny správců v rámci Unie.

Pro usnadnění přístupu subjektů údajů k dozorovému úřadu, Nařízení stanoví, že subjekt údajů může podat stížnost u dozorového úřadu především v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení.

Dozorový úřad je povinen prověřit událost, která je předmětem stížnosti, tj. zjistit, zda k porušení skutečně došlo, a pokud ano, zajistit nápravu. Dozorový úřad, u něhož byla stížnost podána, je následně povinen informovat stěžovatele o postupu v řešení stížnosti a o jeho výsledku, jakož i o možnosti soudní ochrany (viz níže).

Je-li v dané věci zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem, měl by být subjekt údajů informován průběžně. S cílem usnadnit podávání stížností by měl každý dozorový úřad přijmout určitá opatření, například poskytnout formulář pro podání stížnosti, který lze vyplnit i elektronicky, bez vyloučení dalších komunikačních prostředků.

### *Právo na účinnou soudní ochranu vůči dozorovému úřadu*

#### *Fyzické nebo právnické osoby*

Nařízení přiznává každé fyzické a právnické osobě (tj. také správcům a zpracovatelům) právo na účinnou soudní ochranu (tj. podání žaloby) vůči právně závaznému rozhodnutí dozorového úřadu, které se jí týká. Účelem tohoto prostředku právní ochrany je soudní přezkum pravomocného rozhodnutí dozorového úřadu, pokud se dotčená osoba domnívá, že je nesprávné.

Osoba dotčená pravomocným rozhodnutím dozorového úřadu jej může napadnout žalobou u příslušného soudu. Rozhodnutí se může týkat také výkonu vyšetřovacích, nápravných a povolovacích pravomocí dozorovým úřadem nebo odmítnutí či zamítnutí stížností. Napadnout však nelze opatření dozorových úřadů, která nejsou právně závazná, jako jsou stanoviska dozorového úřadu nebo jím poskytované poradenství. Řízení proti dozorovému úřadu by mělo být zahájeno u soudů toho členského státu, v němž je daný dozorový úřad zřízen.

Má-li daný soud informaci, že před příslušným soudem v jiném členském státě je vedeno řízení týkající se stejného zpracování,[91] soud jej kontaktuje pro ověření informací. Pokud se v jiném členském státě či státech taková soudní řízení konají, mohou všechny soudy, u nichž nebylo řízení zahájeno jako první, svá řízení přerušit, a to zřejmě až do pravomocného skončení takového řízení.[92] Dané soudy se také mohou na návrh některé zúčastněné strany prohlásit za nepříslušné, a to ve prospěch soudu, u něhož bylo řízení zahájeno jako první a za předpokladu, že spojení takových řízení je podle právního řádu posledně uvedeného soudu možné.[93]

Podle recitálu 143 má také každá fyzická nebo právnická osoba, případně i dotčený dozorový úřad, který je adresátem těchto rozhodnutí, právo podat žalobu na neplatnost rozhodnutí Sboru u Soudního dvora EU.

### *Subjekty údajů*

Podle Nařízení má každý subjekt údajů právo na účinnou soudní ochranu, tj. na podání žaloby proti dozorovému úřadu u příslušného soudu, pokud se dozorový úřad nezabývá stížností nebo pokud neinformuje subjekt údajů do tří měsíců o postupu v řešení stížnosti či o jeho výsledku. Účelem tohoto prostředku právní ochrany je poskytnout možnost nápravy proti nečinnosti příslušného dozorového úřadu.

Návrh na zahájení řízení se podává u soudu členského státu, v němž je daný úřad zřízen.

Pokud je zahájeno řízení proti rozhodnutí dozorového úřadu, kterému předcházelo stanovisko nebo rozhodnutí Sboru v rámci mechanismu jednotnosti, dozorový úřad toto stanovisko nebo rozhodnutí předloží soudu.

### *Právo na účinnou soudní ochranu vůči správci nebo zpracovateli*

Podle Nařízení má každý subjekt údajů také právo podat žalobu u příslušného soudu, pokud se domnívá, že zpracováním jeho osobních údajů v rozporu s Nařízením byla porušena jeho práva.

Návrh na zahájení řízení proti správci či zpracovateli se podává u soudu členského státu, v němž má daný správce nebo zpracovatel provozovnu. Návrh je možno podat také u soudů členského státu, kde má subjekt údajů své obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.

---

[91] Například řízení se stejným předmětem týkajícím se zpracování stejným správcem nebo zpracovatelem, nebo se stejným důvodem žaloby.

[92] Viz čl. 11 odst. 2 Nařízení; zásada zabraňující konat souběžně tatáž soudní řízení v různých členských státech a popř. je skončit protikladnými rozhodnutími.

[93] Viz čl. 81 odst. 3 Nařízení.

### *Právo na náhradu újmy a odpovědnost*

Nařízení dále přiznává každému (nejen subjektu údajů), kdo v důsledku porušení Nařízení utrpěl hmotnou či nehmotnou újmu, právo obdržet od správce nebo zpracovatele náhradu způsobené újmy. Subjektem povinným k náhradě bude správce nebo zpracovatel, a to podle skutkových okolností případu.

Odpovědnost správce a zpracovatele za způsobenou újmu je vymezena následovně:

- Každý *správce* zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním v rozporu s Nařízením.
- Na druhé straně *zpracovatel* je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené Nařízením konkrétně pro zpracovatele, nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.
- Pokud je do téhož zpracování zapojen více než jeden správce nebo zpracovatel, nebo správce i zpracovatel společně, a pokud nesou odpovědnost za jakoukoliv škodu způsobenou daným zpracováním, je každý správce nebo zpracovatel odpovědný za celou újmu, společně a nerozdílně. To znamená, že subjekt údajů je oprávněn uplatnit nárok na náhradu újmy u kteréhokoliv subjektu. Správce nebo zpracovatel, který nahradil způsobenou újmu v celé výši, má právo žádat od ostatních správců nebo zpracovatelů zapojených do téhož zpracování vrácení části náhrady, která odpovídá jejich podílu na způsobené újmě.

Správce nebo zpracovatel se mohou odpovědnosti za újmu zprostit, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Soudní řízení na náhradu újmy se zahajují u soudů příslušných podle práva členského státu, v němž má správce nebo zpracovatel provozovnu. Návrh na zahájení řízení je možno podat také u soudů členského státu, kde má subjekt údajů své obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.

### *Co dále*

Kromě samozřejmého dodržování povinností, které Nařízení správcům a zpracovatelům ukládá v souvislosti se zpracováním osobních údajů, by měli správci i zpracovatelé důsledně a podrobně smluvně upravit svá vzájemná práva a povinnosti a z toho vyplývající odpovědnostní vztahy.

Vzhledem k solidární odpovědnosti za celou újmu vůči poškozenému subjektu a vzhledem k mezinárodní povaze právních vztahů je důležité věnovat pozornost monitorování právní existence a ekonomického postavení zúčastněných subjektů, signalizaci vůči nim zahájených řízení a zajištění a efektivní náhradě poměrné části uhrazené újmy ostatními správci či zpracovateli.

### *Další informace*

Recitály 141 - 147

Články kapitoly VIII

*Lekce 15 z 16*

## Sankce a odchylky

**V textu se dozvíte:**

*Důležité změny*

- Nařízení přináší podstatné zvýšení maximálních možných pokut za porušení povinností souvisejících s ochranou osobních údajů:
    - v případech závažnějšího porušení Nařízení je maximální výše pokuty 20.000.000 EUR nebo 4 % celkového světového ročního obratu společnosti za předchozí účetní období (podle toho, která suma je vyšší); dosud pokuta činí max. 10 mil Kč;
    - v ostatních případech je maximální výše pokuty 10.000.000 EUR nebo 2 % celkového světového ročního obratu společnosti za předchozí účetní období (podle toho, která suma je vyšší); dosud pokuta činí max. 5 mil Kč.
- Za porušení Nařízení není dozorový úřad povinen uložit pokutu; je-li to však vzhledem k okolnostem případu vhodné a účelné, může uložit i jiný druh sankce (zároveň s pokutou nebo namísto ní).

*Compliance: Akční plán*

- Provedení auditu zpracování osobních údajů k zjištění, které zpracovatelské operace nejsou v souladu s Nařízením;
- Identifikace nejvíce rizikových oblastí a provedení opatření ke zmírnění rizika uložení pokut;
- Zvážení možnosti uzavřít pojistné smlouvy na pojištění rizik spojených se zpracováním osobních údajů.

**K sankcím**

*Správní pokuty*

Dozorové úřady jsou při rozhodování o uložení pokuty a její výši povinny zohlednit skutečnosti, jako jsou např. povaha, závažnost a délka trvání porušení (přičemž přihlédnou k povaze, rozsahu nebo účelu dotčeného zpracování a k počtu dotčených subjektů údajů a míře škody, která jim byla způsobena), úmyslný nebo nedbalostní charakter porušení, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, míra spolupráce s dozorovým úřadem, kategorie osobních údajů dotčených daným porušením atd.

Pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací zpracování poruší více ustanovení Nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení.

V každém jednotlivém případě musí být uložení pokuty účinné, přiměřené a odrazující.

Nařízení kategorizuje různé druhy porušení do dvou hlavních skupin, a to podle závažnosti porušení, kterým odpovídá různá maximální výše správní pokuty:

*Správní pokuta do výše 10.000.000 EUR nebo 2 % obratu*

Do první kategorie řadí Nařízení druhy porušení, kterým odpovídá sankce v maximální výši 10.000.000 EUR nebo v případě společnosti do výše 2 % celkového světového ročního obratu za předchozí účetní období, podle toho, která suma je vyšší. Patří sem následující delikty:

- zpracování osobních údajů dítěte v souvislosti se službami informační společnosti (čl. 8);

- zpracování, které nevyžaduje identifikaci (čl. 11);
- přijetí technických a organizačních opatření za účelem zajištění specificky navržené a standardní ochrany údajů (čl. 25);
- povinnost společných správců dohodnout si vzájemnou odpovědnost za plnění povinností podle Nařízení (čl. 26);
- povinnost jmenovat zástupce správců nebo zpracovatelů neusazených v Unii (čl. 27);
- povinnosti spojené s ustanovením zpracovatelů a povinnosti zpracovatelů (čl. 28 a 29);
- povinnost uchovávat záznamy o činnostech zpracování (čl. 30);
- povinnost spolupracovat s dozorovými úřady (čl. 31);
- povinnost zajistit bezpečnost údajů a ohlašovat porušení (čl. 32 - 36);
- povinnosti související se jmenováním pověřence (čl. 37 - 39);
- povinnosti subjektu pro vydávání osvědčení (čl. 42 a 43); a
- povinnosti monitorujícího subjektu (čl. 41 odst. 4).

*Správní pokuta do výše 20.000.000 EUR nebo 4 % obratu*

Do druhé kategorie spadají delikty, za které Nařízení umožňuje uložit sankci do výše 20.000.000 EUR nebo v případě společnosti až do výše 4 % celkového světového ročního obratu za předchozí účetní období, podle toho, která suma je vyšší. Patří sem následující delikty:

- povinnosti související se zásadami zpracování údajů včetně souhlasu (čl. 5 – 7 a 9);
- porušení práv subjektů údajů (čl. 12 - 22);
- porušení povinností při předání údajů do třetí země nebo mezinárodní organizace (čl. 44 - 49);
- jakékoli porušení povinností podle práva členského státu přijatého podle kapitoly IX; a
- nesplnění příkazu souvisejícího s tokem osobních údajů nařízeného dozorovým úřadem a jiné související delikty (čl. 58).

Zatím ještě platná Směrnice zmocňuje členské státy, aby přijaly vhodná opatření pro zajištění jejího uplatňování a zejména aby stanovily sankce za porušení vnitrostátních předpisů, přijatých na jejím základě.[94]

Český zákonodárce tak učinil v hlavě VII „Správní delikty", §§ 44 až 46 zákona o ochraně osobních údajů. Fyzické osobě v postavení správce či zpracovatele mohla být uložena pokuta až do 1 mil Kč za stanovené přestupky resp. až do 5 mil Kč v případě přitěžujících okolností. Jakákoliv fyzická osoba pak za porušení zákazu zveřejnění osobních údajů stanovený jiným předpisem[95] může být postižena pokutou do 1 mil Kč; za takový přestupek spáchaný tiskem, rozhlasem, TV a jiným obdobně účinným způsobem pokutou do 5 mil. Kč. U právnických osob je možné uložit za uvedené protiprávní jednání pokutu do výše 5 mil Kč resp. 10 mil Kč.

[94] Viz čl. 24 Směrnice.
[95] Viz zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a např. jeho ustanovení o zákazu zveřejňování údajů o osobách zúčastněných na trestním řízení, které přímo nesouvisejí s trestnou činností; zákaz zveřejnění informací o nařízení či provedení odposlechu a záznamu telekom. provozu; zákaz sdělování informací, které porušují princip presumpce neviny; zákaz zveřejnění informací umožňujících zjištění totožnosti poškozeného, mladšího 18 let. Dále též zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění pozdějších předpisů, a obdobný zákaz o sdělování informací o mladistvých.

### *Jiné sankce*

Dozorový úřad má kromě pravomoci uložit pokutu podle výše uvedených zásad k dispozici také možnost uložení jiných druhů sankcí, a to:

- upozornění správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují Nařízení;
- udělení napomenutí správci či zpracovateli, jehož operace zpracování porušily Nařízení;
- nařízení správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle Nařízení;
- nařízení správci či zpracovateli, aby uvedl operace zpracování do souladu s Nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
- nařízení správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
- uložení dočasného nebo trvalého omezení zpracování, včetně jeho zákazu;
- nařízení opravy či výmazu osobních údajů nebo omezení zpracování a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny;
- odebrání osvědčení nebo nařízení, aby subjekt pro vydávání osvědčení odebral osvědčení, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;
- nařízení přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

### *Trestní postih*

Nařízení v čl. 84 a Recitálu 149 ukládá členským státům stanovit pravidla pro jiné i trestní sankce za porušení Nařízení,[96] včetně sankce odebrání zisků, získaných porušením Nařízení. Respektována by však vždy měla být zásada zákazu uložení dvou a více sankcí za totéž jednání porušující Nařízení.

Český trestní zákoník[97] již nyní zakotvuje skutkovou podstatu neoprávněného nakládání s osobními údaji s tresty odnětí svobody, peněžitým trestem či trestem zákazu činnosti.[98] Trestně odpovědné za neoprávněné nakládání s osobními údaji nejsou jen fyzické osoby, ale podle zákona o trestní odpovědnosti právnických osob a řízení proti nim[99] rovněž osoby právnické.

### *Odchýlení se a zvláštní případy zpracování*

Nařízení přiznává členským státům právo odchýlit se od jeho znění, resp. (kde Nařízení příslušná ustanovení neobsahuje) přijmout vlastní právní úpravu ohledně následujících záležitostí:

- oblast veřejné bezpečnosti, prevence a odhalování trestných činů;
- oblast svobody projevu a práva na informace;
- oblast přístupu veřejnosti k úředním dokumentům;
- zpracování národního identifikačního čísla (rodné číslo);
- zpracování osobních údajů v pracovněprávních vztazích;

---

[96] Viz čl. 84 Nařízení
[97] Zákon č. 40/2009 sb., trestní zákoník
[98] Viz § 180 tr. zákoníku:"*(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.(2) ….*".
[99] Zákon č. 418/2011 Sb., ve znění pozdějších předpisů.

- účely archivace ve veřejném zájmu, vědeckého nebo historického výzkumu nebo statistické účely; a
- mlčenlivost související s profesním tajemstvím.

*Co dále*

Správcům a zpracovatelům doporučujeme provést audit k identifikaci nejvíce rizikových oblastí zpracovatelských operací a následně stanovit prioritu kroků vedoucích ke zmírnění rizika uložení správních pokut nebo jiných sankcí. Za tímto účelem je též vhodné posoudit povinnost k náhradě škody v souvislosti se smlouvami s obchodními partnery, zákazníky nebo dodavateli, jejichž jsou správci či zpracovatelé smluvními stranami, a případně upravit odpovědnostní vztahy mezi stranami.

Pro přenesení rizik je možné zvážit pojištění odpovědnosti za škodu způsobenou zpracovatelskou činností.

*Další informace*

Recitály 148 - 165

Články 83 – 84 a články kapitoly IX

*Lekce 16 z 16*

## Praktické kroky k zajištění souladu a minimalizace rizika sankcí

### *Shrnutí Školy ochrany osobních údajů*

V průběhu uplynulých měsíců jsme Vám přinášeli pravidelné informace o nové právní úpravě zpracování osobních údajů, která zásadně mění podmínky zákonnosti zpracování. Nařízení mimo jiné rozšiřuje teritoriální dosah evropského standardu ochrany osobních údajů, přičemž ambicí nové právní úpravy je zajistit, aby se ochrana osobních údajů vztahovala na subjekty údajů nacházející se v Unii i v případě, kdy se jejich údaje zpracovávají mimo Unii subjekty neusazenými v Unii.

Nařízení dále zejména:

- ukládá správcům, aby proaktivně přistupovali k zajištění zákonnosti zpracování a byli schopni dozorovým úřadům prokázat, že provedli všechny potřebné kroky k zajištění souladu s Nařízením;
- upravuje zásady, kterými se mají správci řídit při zpracování osobních údajů, při zahájení zpracování a kdykoliv v jeho průběhu;
- mění podmínky pro platné udělení souhlasu subjektu údajů se zpracováním osobních údajů;
- podstatně rozšiřuje práva subjektů údajů (např. o právo na odstranění údajů z on-line prostředí nebo o právo na přenositelnost údajů);
- ukládá správcům rozšířenou informační povinnost vůči subjektům údajů a povinnost s nimi v odůvodněných případech aktivně komunikovat;
- zvyšuje standard bezpečnostních opatření na ochranu údajů a ukládá správcům i zpracovatelům povinnost oznámit dozorovému úřadu a případně subjektům údajů porušení Nařízení;
- přináší nové instituty, kterými mohou správci zajistit a prokázat soulad s Nařízením, a to kodexy chování a vydávání osvědčení;
- upravuje povinnost uchovávat záznamy o zpracovatelských operacích, provést posouzení vlivu na ochranu údajů a předem konzultovat zpracovávání s dozorovým úřadem;
- upravuje podmínky předávání údajů do třetích zemí a rozšiřuje možnosti pro zajištění souladu předávání;
- zavádí systém jednotného kontaktního dozorového úřadu pro přeshraniční zpracování, které správce provádí v rámci Unie;
- zakotvuje podstatně vyšší sankce za porušení Nařízení oproti stávající právní úpravě.

### *Časový harmonogram praktických kroků k dosažení souladu*

Nařízení nabyde účinnost za necelých 12 měsíců, přesněji 25. května 2018. S ohledem na závažnost změn, rozsáhlost problematiky a výši hrozících sankcí se doporučuje správcům, kteří osobní údaje zpracovávají (tj. např. kteří zaměstnávají fyzické osoby), bezodkladně přistoupit k praktickým krokům, které jsou nezbytné pro implementaci požadavků Nařízení do interních zpracovatelských procesů.

Seznam nezbytných kroků a realistický návrh časového harmonogramu uvádíme níže. Doporučuje se řádně zdokumentovat průběh celého projektu zajišťování souladu s Nařízením pro účely případné potřeby prokazování odborné péče dozorovému úřadu.

- ✓ Co: **Určení týmu zaměstnanců a finančních a technických prostředků pro účely projektu**

  Kdy: červenec - srpen 2017

  Jak: Nejdříve je nutné pověřit zaměstnance, který bude odpovědný / kteří budou odpovědní za (a bude / budou mít v náplni práce) zajištění souladu zpracovatelských operací správce s Nařízením. Uvedené platí také tehdy, pokud správce plánuje pověřit vypracováním projektu souladu externího dodavatele; v takovém případě bude tento odpovědný zaměstnanec za správce komunikovat s dodavatelem služeb. Typicky se může jednat o pracovníka právního nebo HR oddělení a pro technickou podporu bude účelné zajistit součinnost a informovanost IT specialisty.

  Tomuto projektovému týmu bude potřeba zajistit veškeré potřebné informace a školení, aby byl schopen se v problematice zorientovat a znát své úkoly.

  Nadnárodní organizace nebo společnosti určí, zda budou soulad s Nařízením řešit na lokální (národní) úrovni, nebo bude lokální tým spolupracovat s centrálou.

- ✓ Co: **Zjištění zpracovatelských operací**

  Kdy: srpen – říjen 2017

  Jak: Správce musí zmapovat (i) jaké osobní údaje zpracovává, (ii) jaké kategorie subjektů údajů jsou pro něj relevantní a (iii) jaké zpracovatelské operace s osobními údaji provádí. Tyto vstupní informace je nezbytné zjistit s důrazem na detail, přesnost, aktuálnost a úplnost a je potřeba tyto výstupy zachytit písemně, neboť poslouží jako východisko pro další aktivity.

- ✓ Co: **Analýza nedostatků ve světle nové legislativy**

  Kdy: říjen – prosinec 2017

  Jak: Správce by měl provést důkladnou analýzu stávajících interních postupů všech svých zainteresovaných oddělení (např. HR oddělení, IT oddělení znalé softwarových řešení ve společnosti, oddělení styku se zákazníky, recepční, ztotožňující návštěvy, oddělení vnitřní bezpečnosti, správci kamerových systémů CCTV a jiných monitorovacích zařízení apod.) – pokud se dostávají do kontaktu s osobními údaji. Rovněž je potřebná analýza dokumentů upravujících tyto vnitřní postupy, pokud je správce implementoval.

  Ze zjištění je potřeba vypracovat písemnou zprávu s uvedením nedostatků a rizik a s uvedením návrhů na jejich zmírnění. S touto zprávou by se mělo seznámit nejvyšší vedení správce.

- ✓ Co: **Pověřenec pro ochranu osobních údajů a zpracovatelé**

  Kdy: říjen – prosinec 2017

Jak: Správce musí dále prověřit, zda bude potřebné k datu účinnosti Nařízení jmenovat pověřence pro ochranu osobních údajů.

Je potřeba provést revizi smluv se zpracovateli a případnými jinými subjekty pro zajištění souladu smluvních ustanovení s Nařízením. Doporučuje se zanalyzovat také odpovědnostní vztahy s těmito subjekty, týkající se oblasti ochrany osobních údajů, a z nich plynoucí rizika vzniku nároků na náhradu škody a případných sankcí.

✓ Co: **Vytvoření nebo aktualizace interních směrnic o ochraně osobních údajů**

Kdy: leden – březen 2018

Jak: Je potřeba, aby měl správce ke dni účinnosti Nařízení připravenou zrevidovanou, případně nově vytvořenou interní dokumentaci, kterou požaduje Nařízení. Ta bude zahrnovat např. oznámení o zpracování osobních údajů určené subjektům údajů, spisovými plány s uvedením doby uchovávání jednotlivých dokumentů obsahujících osobní údaje, souhlasy se zpracováním osobních údajů, postupy pro případ žádostí o přístup k údajům, zásady ochrany osobních údajů, postupy pro výmaz či blokování údajů apod.

✓ Co: **Implementace vnitřních procesů**

Kdy: březen – květen 2018

Jak: Správce musí implementovat vnitřní procesy závazné pro zaměstnance nakládající s osobními údaji a řádně je vyškolit o úkolech, které se od nich budou ode dne účinnosti Nařízení vyžadovat. Tyto postupy by se měly týkat všech možností, které se mohou v průběhu zpracování vyskytnout, např. pro případ porušení Nařízení, v případě žádosti subjektu údajů o přístup k údajům, o vymazání údajů nebo jejich blokování apod.

Zaměstnance nakládající s osobními údaji je třeba detailně a prokazatelně seznámit s povinností mlčenlivosti a s přijatými interními dokumenty v oblasti zpracování a poučit je, jak se který dokument používá, poučit je o způsobu komunikace se subjekty údajů apod.

Samozřejmostí je, že všechny potřebné zpracovatelské operace by měly být technicky realizovatelné, k čemuž je třeba zajistit služby IT specialisty.

✓ Co: **Školení zaměstnanců**

Kdy: únor – květen 2018

Jak: Správce musí pro zvýšení povědomí o ochraně osobních údajů zajistit potřebná školení zaměstnanců nakládajících s osobními údaji. Na jejich odbornosti bude přímo záviset míra rizika případných sankcí, které za porušení Nařízení hrozí a které mohou být v určitých případech uloženy správci až do výše 20 mil. EUR nebo 4 % celkového ročního obratu, podle toho, která suma je vyšší.

*Kde začít*

Tým odborníků advokátní kanceláře Balcar, Polanský & Spol. s.r.o. je připraven Vám poskytnout bližší informace o výše uvedených povinnostech nebo jakýchkoliv jiných aspektech blížící se účinnosti Nařízení. Neváhejte se proto obrátit na některého z níže uvedených advokátů nebo na Vaši obvyklou kontaktní osobu v naší advokátní kanceláři.

Naši odbornost, včetně mezinárodní certifikace v oblasti ochrany osobních údajů, si můžete ověřit zde:

http://www.balcarpolansky.cz/files/251/Focussed%20on%20DP_CZ.pdf

## Kontaktní osoby

Pro další informace prosím kontaktujte:

Česká republika:

**JUDr. Jaroslav Srb**
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz

Slovensko:

**JUDr. Helga Maďarová, CIPP/E, CIPM**
Advokátka | Certified Intl. Privacy Professional/Europe | Certified Intl. Privacy Manager

Tel.: +421 220 251 311
Mobil: +421 917 092 076

helga.madarova@bapol.sk