2.2 Co spadá do zvláštní kategorie osobních údajů

V celkové množině osobních údajů je nutno vydělit speciální podskupinu – **zvláštní kategorie osobních údajů**. Tyto údaje představují osobní údaje citlivé (respektive citlivější), jimž je potřeba poskytnout **vyšší stupeň ochrany**.

Zvláštní kategorie osobních údajů

V souladu s čl. 9 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR") jsou **zvláštní kategorií osobních údajů** (taxativní výčet):

a) údaje, které vypovídají o rasovém či etnickém původu;
b) údaje, které vypovídají o politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech;
c) genetické údaje;
d) biometrické údaje pořízené za účelem jedinečné identifikace fyzické osoby;
e) údaje o zdravotním stavu;
f) údaje o sexuálním životě nebo sexuální orientaci fyzické osoby.

Vyšší stupeň ochrany

Vyšší ochrana těchto citlivých údajů se projevuje především v požadavku na existenci **speciálních právních titulů** k jejich zpracování dle čl. 9 odst. 2 GDPR, v nutnosti **posouzení vlivu, ustavení pověřence a zohlednění vyššího rizika** pro práva a svo-

body subjektů údajů při zabezpečení těchto údajů.

Dřívější právní úprava

Již před účinností GDPR znala směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a česká právní úprava (zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů) pojem „**citlivé osobní údaje**“, jejichž rozsah se prakticky překrýval s dnešním vymezením zvláštní kategorie osobních údajů. Výjimkou je dřívější „citlivý údaj“ o odsouzení za trestný čin, který dnes dle čl. 10 GDPR spadá do jiné zvláštní kategorie, a to osobní údaje týkající se **rozsudků v trestních věcech a trestných činů**.

Důvody **zvláštní ochrany tohoto typu údajů** vymezila česká judikatura následovně (viz například rozsudek Nejvyššího správního soudu č. j. 9 As 59/2010-58): *„Citlivé údaje nepochybně tvoří zvláštní kategorii osobních údajů ve smyslu zákona o ochraně osobních údajů a smyslem jejich odlišení je především potřeba zaručit těmto údajům speciální, větší ochranu; k tomu srov. obecně využitelná východiska v části IV.1.dl, body 157. a 158. nálezu Ústavního soudu ze dne 15. 11. 2010, sp. zn. I. ÚS 517/10, dostupného z http://nalus.usoud.cz, který v souvislosti s naznačenou zvýšenou ochranou citlivých údajů poukázal mj. na to, že: ‚…tkví v jejich povaze (kterou se odlišují od ostatních osobních údajů). Jde totiž o informace nejvíce soukromé a důvěrné, nejúžeji spjaté s osobní identitou či nejintenzivněji vypovídající o nitru (duchu) lidské bytosti, tedy o aspekty*

identity a existence jednotlivce nanejvýš osobního charakteru. Jedná se tudíž o informace o nejintenzivnějším (detailním) soukromí, o údaje výhradně osobního, soukromého charakteru. Kupříkladu lze uvést údaje o sexuálním životě jednotlivce (kam patří sexuální orientace, sexuální partneři, kvantita sexuálních styků aj.); genetické údaje (které obsahují mnoho osobních informací o jednotlivci a umožňují odhalení genetických vztahů, jež mohou mezi jednotlivci existovat, a odhalení pravděpodobného etnického původu jednotlivce aj.); biometrické údaje (kupř. míry a váhy jednotlivců – velikost poprsí, obvod pasů a boků aj., otisk prstů a dlaně); údaje o zdravotním stavu (měřené hodnoty v relaci k organismu, diagnózy včetně příp. duševních chorob, léčba); údaje o národnostním, rasovém nebo etnickém původu.'"

Širší výklad

Z jazykového výkladu definice zvláštní kategorie osobních údajů – výčet pod písm. a)–f) výše – bychom mohli dospět k závěru, že údaji dle písm. a)–b) nejsou pouze samotné informace o rasovém či etnickém původu nebo údaje o politických názorech a podobně, ale všechny další informace, které **o těchto údajích „vypovídají"**.

Širší výklad je nicméně třeba **volit i v případě dalších osobních údajů**, a to zejména s ohledem na judikát Soudního dvora Evropské unie (dále jen „SDEU") ve věci C-184/20. Zde SDEU hodnotil, „*zda údaje, z nichž lze myšlenkovou asociací nebo dedukcí zjistit sexuální orientaci fyzické osoby, spadají do zvláštní kategorie osobních údajů ve smyslu čl. 8 odst. 1 směrnice 95/46 a čl. 9 odst. 1 GDPR*".

V souladu s jazykovým výkladem nastíněným výše poukázal generální advokát na jazykové **rozdíly mezi užitím slovesa „vypovídají" a předložky „o"**, která implikuje, že je vyžadována přímější a bezprostřednější vazba mezi zpracováním a dotyčnými údaji. SDEU však s tímto názorem nesouhlasil a zvolil **široký výklad ve prospěch posouzení údajů nepřímo směřujících** ke zjištění sexuální orientace dané osoby jako zvláštní kategorie osobních údajů: „*Tato ustanovení proto nemohou být vykládána v tom smyslu, že zpracování osobních údajů, které může nepřímo vést k odhalení citlivých údajů o fyzické osobě, je vyňato z režimu zvýšené ochrany stanoveného uvedenými ustanoveními, jinak by byl narušen užitečný účinek tohoto režimu a ochrana základních práv a svobod fyzických osob, kterou má tento režim zajistit.*"

Častá chyba

Z výše uvedeného je zřejmé, že výskyt osobních údajů spadajících do zvláštní kategorie osobních údajů bude mnohem vyšší, než řada správců předpokládá.

Profilování

Pozor je třeba dát i v souvislosti s profilováním, jak uvádí pokyny pracovní skupiny dle čl. 29 (WP251rev.01) k **automatizovanému individuálnímu rozhodování a profilování** pro účely nařízení 2016/679: „*Profilování může vytvořit zvláštní kategorie údajů prostřednictvím dedukce z údajů, které nejsou samy o sobě zvláštními kategoriemi údajů, ale stávají se jimi, když se zkombinují s jinými údaji. Například může existovat možnost vydedukovat zdravotní stav určité osoby ze záznamů o jejích nákupech jídla ve spojení s údaji o kvalitě a energetickém obsahu potravin.*"

Praktický příklad

Pracovní skupina dle čl. 29 uvádí jako příklad studii, která spojila kliknutí na tlačítko „to se mi líbí" na Facebooku s omezenými informacemi z průzkumu, přičemž bylo zjištěno, že výzkumní pracovníci přesně odhadli sexuální orientaci mužského uživatele v 88 % případů, etnický původ uživatele v 95 % případů a zda je uživatel křesťan nebo muslim v 82 % případů.

Dále se budeme věnovat některým **hraničním případům či údajům**, u nichž došlo v čase ke změně názoru na jejich (citlivou) povahu.

Přístupové a docházkové systémy

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ") se v minulosti vyjádřil k využívání docházkových či přístupových systémů založených na **otisku prstů či dlaně zaměstnanců**. Ve svém stanovisku ÚOOÚ rozlišoval u těchto systémů skutečnost, zda dochází k **uchovávání úplných biometrických údajů**, nebo zda systém vytváří z úplných biometrických údajů šablonu, která není volně čitelná nebo zpětně rekonstruovatelná. V takovém případě nešlo dle názoru ÚOOÚ o zvláštní kategorii osobních údajů (biometrické údaje).

Odkaz:

Stanovisko ÚOOÚ č. 3/2009 si můžete stáhnout na adrese:
www.uoou.cz/files/stanovisko_2009_3.pdf

V tomto ohledu **došlo ovšem s účinností GDPR ke změně**, avizované ÚOOÚ na stránkách dne 8. 6. 2017: *„Dne 25. května 2018 nabývá účinnosti evropský předpis, který nově nastavuje ochranu*

osobních údajů mj. z důvodu proměn a rychlého rozvoje technologií, tzv. obecné nařízení o ochraně osobních údajů (nařízení Evropského parlamentu a Rady, č. 2016/679). Ve svém čl. 9 upravuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Tato úprava přináší podstatnou změnu v právním pohledu na technologie zpracovávající biometrické údaje, mj. také v tom, že uchovávání biometrických šablon (template) a jejich zpracování za účelem identifikace osob považuje za zpracování zvláštní kategorie osobních údajů."

Nadále je tedy třeba i systémy využívající k autentizaci šablony vytvořené z biometrických údajů **považovat za zpracování zvláštní kategorie** osobních údajů – se všemi omezeními, které z toho vyplývají.

Dynamický biometrický podpis

K problematice dynamického biometrického podpisu vydal ÚOOÚ ještě v době platnosti zákona č. 101/2000 Sb. stanovisko č. 2/2014, v němž mimo jiné uvedl, že **klasický i dynamický biometrický podpis** je nositelem biometrických údajů. Oproti klasickému vlastnoručnímu podpisu, který bylo dle ÚOOÚ možné považovat za citlivý údaj až v souvislosti s **aktivním využitím** v něm obsažených citlivých údajů (například podrobení písmoznaleckému zkoumání za účelem ověření jeho pravosti), považoval ÚOOÚ dynamický biometrický podpis za citlivý údaj bez dalšího, neboť u něj již automaticky mělo docházet ke zpracování citlivých údajů.

Odkaz:

Stanovisko ÚOOÚ č. 2/2014 je dostupné na adrese: www.uoou.cz/stanovisko-c-2-2014-dynamicky-biometricky-podpis-z-pohledu-zakona-o-ochrane-osobnich-udaju/d-11298

ÚOOÚ tento výklad během dalších let upřesnil tak, že pokud je biometrický podpis **zpracováván pouze jako běžný podpis** (jeho využití nebude spojeno s dalším automatickým zpracováním biometrických údajů), nejedná se o zpracování citlivých údajů, ale uplatní se právní režim jako při **zpracování klasického podpisu** (dynamický biometrický podpis byl za těchto okolností chápán pouze jako jiný prostředek podpisu).

Posun nastal s platností GDPR, které zařadilo biometrické údaje do zvláštní kategorie osobních údajů, a tedy i ÚOOÚ začal problematiku vnímat tak, že v případě použití jakéhokoliv systému shromažďujícího **biometrické údaje za účelem identifikace osob** (tedy i prostřednictvím dynamického biometrického podpisu) jde o zpracování zvláštní kategorie osobních údajů.

ÚOOÚ zatím **nevydal v uvedené problematice nové stanovisko**, kterým by zrušil citované stanovisko z roku 2014, ale jeho postoj je zřejmý například ze závěru prováděných kontrol.

Při posouzení **vhodnosti a oprávněnosti použití dynamického biometrického podpisu** je v současnosti nutné přihlížet nejen k GDPR, ale například i k nařízení Evropského Parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách

vytvářejících důvěru pro elektronické transakce na vnitřním trhu, (dále jen „nařízení eIDAS“) či zákonu č. 297/2016 Sb., o službách vytvářejících důvěru v elektronických transakcích, ve znění pozdějších předpisů.

Kamerové systémy

Skutečnost, že i v rámci **provozování kamerových systémů** může docházet ke zpracování zvláštní kategorie osobních údajů, vyplývá mimo jiné z vodítka Evropského sboru pro ochranu osobních údajů (dále jen „EBDP“) 3/2019, o zpracování osobních údajů prostřednictvím videozařízení.

Praktický příklad

Jako konkrétní příklady takového zpracování jsou uváděny:

- záběry umožňující identifikovat subjekty údajů **účastnící se demonstrace či stávky** (údaje, které vypovídají o politických názorech nebo členství v odborech);
- **kamery v nemocnici** monitorující pacientův zdravotní stav.

Naproti tomu EBDP neshledává zpracování zvláštní kategorie údajů v tom, vyskytují-li se na kamerovém záznamu **osoby s brýlemi či na invalidním vozíku** nebo je-li pouze monitorován kostel jako takový (samozřejmě je třeba vždy vyhodnotit povahu dat a rizika zachycení dalších citlivých údajů).

Data v platebních systémech

V souvislosti s přijetím druhé směrnice o platebních službách (směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 23. 12. 2015, dále jen

„směrnice PSD2"), která se věnuje **provádění online plateb** a **poskytování informací v platebním styku**, se EBDP vyjadřoval k různým aspektům ochrany údajů z hlediska směrnice PSD2.

EBDP se v Pokynech 06/2020 týkajících se vzájemného působení druhé směrnice o platebních službách a GDPR (Verze 2.0) kladně vyjádřil k možnému **výskytu zvláštní kategorie osobních údajů u finančních transakcí**: „*Například z darů politickým stranám nebo organizacím, církvím nebo farnostem by v závislosti na podrobnostech transakce mohly být odhaleny politické názory a náboženské vyznání. Odečtením ročního členského příspěvku z bankovního účtu by mohlo být odhaleno členství dané osoby v odborech. Analýzou účtů za zdravotní péči, které subjekt údajů uhradil zdravotníkovi (například psychiatrovi), by mohly být získány osobní údaje o zdravotním stavu. A konečně informace o některých nákupech mohou odhalit informace týkající se sexuálního života nebo sexuální orientace dané osoby. Jak dokládají tyto příklady, mohou i jednotlivé transakce obsahovat zvláštní kategorie osobních údajů. Služby informování o účtu by navíc mohly vycházet z profilování, jak je definováno v čl. 4 odst. 4 GDPR. Proto je velká pravděpodobnost, že poskytovatel služeb, který zpracovává informace o finančních transakcích subjektů údajů, zpracovává také zvláštní kategorie osobních údajů.*"

Dle EBDP tak existuje velká pravděpodobnost, že poskytovatel služeb, který zpracovává **informace o finančních transakcích subjektů údajů**, zpracovává také zvláštní kategorie osobních údajů.

Častá chyba

V kontextu výše uvedeného je třeba zmínit e-shopy, které pro pravidelné zákazníky ukládají v jejich uživatelském účtu **údaje o předchozích objednávkách, platbách** a podobně. Půjde-li například o léčiva či doplňky stravy, erotické pomůcky či třeba politické časopisy, bude se pravděpodobně jednat o zvláštní kategorii údajů.

Údaje o zdravotním stavu

Širší pojetí bylo u **údajů o zdravotním stavu** judikaturou zdůrazněno již před rozhodnutím SDEU ve věci C-184/20 – viz rozsudek SDEU ve věci 101/01: *„S ohledem na předmět této směrnice je třeba výraz ‚údaje týkající se zdraví', použitý v jejím čl. 8 odst. 1, vykládat široce, tedy tak, že zahrnuje informace týkající se všech stránek zdraví člověka, ať fyzických či duševních*."

Lze konstatovat, že tato kategorie je širší než pojem „údaje o zdravotním stavu" dle zákona č. 372/2011 Sb., o zdravotních službách. Kromě obsahu zdravotnické dokumentace pacienta sem spadají i **údaje zpracovávané zaměstnavateli**, jako jsou například různé testy na návykové látky, informace o pracovních úrazech a nemocech z povolání.

Otázkou je, **zda je zvláštní kategorií osobních údajů e-neschopenka** obsahující pouze informaci o tom, že zaměstnanec je dočasně práce neschopen. Dřívější odborná literatura i ÚOOÚ se k tomuto problému stavěly tak, že se o zvláštní kategorii osobních údajů nejedná: *„Naopak zpracování citlivých dat zaměstnavatelem nebude nezbytné*

v případě, kdy je posuzována (na základě § 5 odst. 2 zákona č. 372/2011 Sb. a Směrnice Ministerstva zdravotnictví č. 49/1967 Věstníku MZd o posuzování zdravotní způsobilosti k práci) zdravotní způsobilost zaměstnanců pro konkrétní pracovní zařazení. Zde se zaměstnavatel s ohledem na požadavek nezbytnosti uvedený v § 9 písm. d) OchOsÚ musí spokojit se závěrem posudkového lékaře o tom, zda daný zaměstnanec je či není pro výkon konkrétní práce zdravotně způsobilý, aniž by disponoval detaily o jeho zdravotním stavu." (citace z publikace Zákon o ochraně osobních údajů, Kučerová et al., str. 193).

S ohledem na výše uvedené by ale zřejmě i tyto údaje (ve spojení s dalšími údaji, které zaměstnavatel v rámci e-neschopenky obdrží – jméno a adresa ošetřujícího lékaře, údaje, zde existuje podezření na úraz způsobený třetí osobou či požití alkoholu, omamných nebo psychotropních látek) měly být považovány za **údaje o zdravotním stavu v širším smyslu**.

Vedení účetnictví

V souvislosti se zvláštní kategorií osobních údajů týkajících se zdravotního stavu by si poskytovatelé zdravotních služeb měli rovněž dávat pozor při **vystavování daňových dokladů a vedení účetnictví**. Na daňových dokladech by totiž dle ÚOOÚ **neměl být uveden kód diagnózy pacienta**, a to zejména proto, že:

- faktura se zakládá do účetnictví, ke kterému mají přístup i třetí osoby, a tedy dochází k porušení povinnosti mlčenlivosti;
- kód diagnózy pacienta je zpracován za jiným účelem (a to informace o onemocnění pacienta

a provedení vyšetřovacích výkonů), než za jakým byl zpracován (uvedení kódu na faktuře);
- faktura není zdravotnickou dokumentací a i bez uvedení kódu diagnózy pacienta splňuje náležitosti daňového dokladu.

Shodně vyznívá například i **rozhodnutí Městského soudu v Praze** ze dne 6. 6. 2017, č. j. 6 Ad 23/2015–6: *„(...) žalobkyně nebyla potrestána za vystavení faktury podle zákona o účetnictví, ale za to, že v této faktuře uvedla i kód vyšetření, a zejména pak v průvodním dopise honorárnímu konzulovi uváděla osobní údaje, které nejsou pro identifikaci účastníka nezbytné (např. poukazem XXXXXXXX). Celý tento souhrn údajů byl shledán jako porušující povinnost mlčenlivosti, s čímž soud souhlasí – uvádění těchto údajů není nezbytné ani na faktuře, a rozhodně pak dokonce v průvodním dopise, kterým byla tato faktura zaslána. Obecný praktický postup je běžně takový, že tyto údaje se uvádějí (i v soudním řízení) až tehdy, pokud je nějaký spor o příslušné fakturované plnění (jeho rozsah, trvání apod.). Až tehdy se většinou tato informace doplňuje o další skutečnosti, ty však samy o sobě nejsou nutné k tomu, aby příslušné fakturované plnění identifikovaly, a proto jejich uvádění na faktuře nutné není."*

Odhalení zvláštní kategorie OÚ

Jak jsme v této kapitole ukázali, pro správce a potažmo pověřence pro ochranu osobních údajů bude mnohdy nelehkým úkolem **odhalit všechny případy, kdy jsou zpracovávány zvláštní kategorie** osobních údajů. Často se přitom bude jednat o běžně se vyskytující agendu.

Častá chyba

Zejména situace, kdy budou zpracovávané údaje vést ke zjištění údajů citlivých pouze nepřímo, mohou vést k mylnému závěru, že předmětem zpracování jsou „běžné“ osobní údaje.