**Zaměstnávání osob s trestní minulostí v souvislosti se zpracováním jejich údajů**

**Expertní skupina zástupci zaměstnanců**

Alice Čamková

Bc. Petr Weisser

Tomáš Kasalický

# PRAHA

# 2018

# Představení cílů

Předkládaná studie si klade za cíl navázat na dřívější studie expertní skupiny zástupců zaměstnanců, které se týkaly především zaměstnávání osob s trestní minulostí, a zároveň protnout tato témata stále aktuální problematikou ochrany osobních údajů vzhledem k přijetí nařízení GDPR a postupně legislativním procesem přijímaným zákonem o zpracování osobních údajů.

Studie bude zaměřená na v prvé řadě na vzájemnou korelaci zpracování osobních údajů souvisejících s trestnou činností se zaměstnáváním osob s trestní minulostí. Dále se bude studie týkat práv zaměstnanců, které jim jako jiným subjektům v pracovněprávních vztazích nařízení GDPR přiznává, způsoby jeho výkonu a možnosti ochrany před zaměstnavatelem z hlediska nadbytečného sbírání údajů, monitoringu a diskriminačních závěrů z neoprávněně získaných údajů. Současně by studie měla představit zákonný rámec pro zaměstnavatele, kteří by na jejím základě měli být schopni nastavit počet standardně dějících se zpracování, aby bylo dosaženo souladu s nastávající právní úpravou. Studie by tak měla reflektovat proces náboru, zaměstnávání včetně zpracování pro mzdové, daňové a účetní účely, problematické aspekty monitoringu zaměstnanců a způsoby obrany zaměstnanců, aspekty neoprávněných ukončení pracovního poměru a zpracování dokladů po ukončení pracovněprávního vztahu. Vzhledem k výše uvedenému a také k předchozím tématům expertní skupiny bude speciálně reflektováno téma zpracování osobních údajů trestněprávní tematiky, především rozsudků v trestních věcech a trestných činů ve smyslu čl. 10 nařízení GDPR.

Studií si autoři kladou za cíl představit právní úpravu a její východiska nikoliv teoreticko-právní, ale maximálně praktickou cestou: záměrem je ve studii vytvořit komplexní příručku, dle které bude moci být přímo postupováno při implementaci nařízení GDPR a zohledňování ochrany osobních údajů, s maximálním důrazem na zpracovávání údajů související s trestnou činností v průběhu celého trvání pracovněprávního vztahu. V jejím průběhu budou dotazováni zaměstnavatelé i zaměstnanci z hlediska připravenosti na GDPR, znalosti faktů ohledně údajů a práv zaměstnance a v návaznosti na předchozí studie jejich limity při zpracování údajů v trestněprávních záležitostech.

Studie bude vycházet ze znalostí a zkušeností, získaných autory při implementaci nařízení GDPR v soukromé i veřejné sféře v rámci jejich praxe, dále ze znalostí a faktů získaných při přípravě předchozích odborných studií, zejména při zaměstnávání osob po výkonu trestu, a z informací získaných od zaměstnavatelů a zaměstnanců prostřednictvím dotazníků a dalších neformalizovaných postupů.

# Osnova studie

1. Úvod
   1. představení problematiky ochrany osobních údajů
   2. posun v právní úpravě
   3. hledisko pracovněprávních vztahů v oboru ochrany osobních údajů
   4. zpracovávání údajů souvisejících s trestní minulostí
2. Teoretická část
   1. rozdělení procesu pracovněprávních vztahů a typických zpracování
      1. náborový proces
      2. přijmutí do zaměstnání
      3. evidence neúspěšných uchazečů
      4. průběh zaměstnání
      5. právní povinnosti zaměstnavatele
      6. osobní spis
      7. ukončení pracovněprávního vztahu
      8. evidence listin a dokumentace zaměstnavatelem
   2. práva zaměstnance a způsob jejich výkonu
      1. právo na přístup
      2. právo na opravu
      3. právo na výmaz
      4. právo na omezení zpracování
      5. právo podat námitku
      6. právo na přenositelnost
   3. problematické aspekty zpracování, právní základy zpracování
   4. plnění informační povinnosti zaměstnavatele
3. Praktická část
   1. představení úpravy zaměstnavatelům
   2. nastavení právních základů pro zpracování údajů o trestněprávní činnosti
   3. nastavování procesů, spojování účelů, právních titulů a dob zpracování
4. Závěr
   1. shrnutí dosažení cílů
   2. shrnutí povědomí o právech subjektů
   3. vycházející doporučení pro zaměstnance i zaměstnavatele

# Úvod

### Představení problematiky ochrany osobních údajů

1. Nástup nových technologií na začátku 70. let 20. století zcela proměnil celé oblasti lidského konání. Nastaly změny v oblasti komunikace, přístupu a zisku k informacím, jejich vyhodnocování a mnoho dalšího. Tato nová éra započala také zvýšené nebezpečí zásahů do práva na soukromí. Lidé se začali obávat trvalého sledování ze strany státních autorit, možností umělé inteligence a trvalé ztráty soukromí. Za cílem ochránit lidské soukromí za začaly tvořit normy, které by toto především na mezinárodní úrovni uzákonily. Poprvé se o to pokusila OECD v roce 1980, když připravila nezávaznou směrnici se základními principy ochrany soukromí v digitálním věku. Ve směrnici OECD byly poprvé definovány pojmy, jako je osobní údaj, správce osobních údajů či subjekt údajů, byly zde stanoveny základní zásady ochrany osobních údajů, které jsou téměř totožné s těmi, které jsou zakotveny v čl. 5 Nařízení, a objevila se zde také práva jedinců, jejichž osobní údaje jsou zpracovány, jako je právo na informace o zpracování a právo podávat námitky proti zpracování. Vzhledem k tomu, že členskými státy OECD je také velké množství států mimo území Evropy, měla tato směrnice celosvětový dopad. Směrnice však není právně závazná a původně měla sloužit zejména jako návod pro vytvoření legislativy na ochranu osobních údajů v zemích, které doposud žádnou takovou právní úpravu neměly.

Jako první opravdu závazný nástroj pro nadnárodní legislativu v oblasti ochrany osobních údajů se objevuje tzv. Úmluva č. 108, kterou v roce 1981 přijala Radou Evropy. Vychází přitom ze směrnice OECD: principy a mechanismy dříve označené jsou zde zachovány a dále rozvíjeny. Poprvé se také objevuje možnost jejími signatáři omezit a upravit některá práva a povinnosti. Omezení probíhá skrze opatření, u kterých jednotlivé státy odůvodní jejich nezbytnost pro dosažení určitého veřejného zájmu v demokratické společnosti. Jejich limity jsou pak otázkou, kterou evropské soudy včetně Soudního dvora a lucemburského Soudu pro lidská práva dovozují do dnešního dne. Hranice, kterou již není státy možné překročit, je přitom poměrně subtilní: obecně však je možné legálně omezovat lidské právo na soukromí. Právě tento obecný klíč je kritériem, které si nakonec našlo cestu až do Nařízení GDPR.

Úmluvu č. 108 k dnešnímu dni podepsalo 53 států (ratifikovalo 50), z nichž 44 bylo v době podepsání členem Rady Evropy. Úmluvu podepsalo jen devět států mimo evropský prostor: Kapverdy, Mauritius, Mexiko, Senegal, Tunisko, Uruguay, Argentina, Burkina Faso a Maroko, z nichž tři poslední Úmluvu k dnešnímu dni ani neratifikovaly.

Úmluva č. 108 kromě výše uvedeného také obsahuje úpravu pro některé přeshraniční kanály pro předávání osobních údajů, jejichž omezení se by se jevilo jako porušující smysl Úmluvy – technologický postup nutně vede k předávání údajů mezi státy a omezovat toto předávání by další technologický rozvoj paralyzovalo. Pravidlo má jedinou výjimku: tou je situace, kdy ve státu, ze které jsou osobní údaje předávány, požívají předávané osobní údaje vyšší úrovně ochrany, než ve státu, ve kterém jsou osobní údaje přijaty. V takovém případě lze obecné pravidlo pro konkrétní předávání upravit.

Příkladem kategorie osobních údajů, jejichž úprava pro předávání může být dle předchozího odstavce odchýlena a které Úmluva č. 108 na rozdíl od unijního práva nepřiznává žádnou zvláštní ochranu, je kategorie údajů o odborové činnosti, v rámci Nařízení GDPR uvedena jako zvláštní kategorie osobního údaje, podléhající ochraně dle čl. 9. Pokud by tedy signatář Úmluvy č. 108 a současně země, která by nebyla vázaná unijní právem, neměla pro takové údaje vlastní sektorovou úpravu, mohou předávající země předávání takových údajů do této země zvlášť upravit, a to včetně omezení nebo úplného zákazu.

Úmluva doznávala v průběhu let určitých změn. Poslední modernizace právě s přihlédnutím k Nařízení GDPR proběhla k 18. květnu 2018. V rámci této modernizace byly upraveny oblasti výjimek z aplikace Úmluvy, kdy již nebude možné z její působnosti vyjmout některé oblasti zpracování. Rovněž byly doplněny nové procesní nástroje pro zajištění či dokumentování souladu ochrany osobních údajů s platnou právní úpravou. Tímto nástrojem je především dle čl. 7 Úmluvy povinnost oznamovat bezpečnostní incidenty, které mohou vážně zasáhnout do práv dotčených osob. Druhým nástrojem je pak dle čl. 10 Úmluvy nutnost dbát na ochranu osobních údajů již při zavádění konkrétních procesů, v jejichž rámci dochází ke zpracování osobních údajů. Tento princip, který dle Nařízení GDPR, nese název *privacy-by-design*, je klíčovým i při přístupu ke zpracování údajů o trestněprávní činnosti a dalším přístupu správce k těmto údajům.

Současně znění Úmluvy současně dostalo interpretačních změn ze strany Úřadu na ochranu osobních údajů. V často kladených otázkách k předávání osobních údajů do třetích zemí Úřad totiž 10. října uvedl, že o zemích, které Úmluvu ratifikovaly, nebude uvažovat jako o zemích splňujících odpovídající úroveň ochrany osobních údajů. K ratifikaci Úmluvy bude pouze při takovém posuzování o odpovídající ochraně údajů přihlíženo.

Národní úpravou České republiky, které se týká ochrany osobních údajů, je právo na soukromí, primárně uvedené v čl. 7 v Listině základních práv a svobod, kde se nachází jeho definice. V souladu s čl. 7 se stanoví nedotknutelnost osoby a jejího soukromí, přičemž omezení nedotknutelnosti povoluje pouze v případech stanovených zákonem.

Toto právo se však prolíná větším počtem ustanovení Listiny a není obsaženo pouze v jediném článku. Jako příklad lze uvést čl. 10 odst. 1 Listiny, dle kterého má člověk právo na zachování jeho důstojnosti, osobní cti a dobré pověsti a dle kterého je chráněno jeho jméno. Odst. 2 stejného článku následně přiznává právo na ochranu před neoprávněným zasahováním do jejich soukromého a rodinného života. Podobně i odst. 3 dává člověku přímo právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o jeho osobě.

Jedním z ustanovení, které chrání soukromí a nedotknutelnost člověka, je i ochrana listovního tajemství v čl. 13 Listiny. Toto ustanovení, půvedně zamýšlené jako ochrana před násilnou ingerencí do papírových dopisů, telegramů a příjímaných signálů skrze telegrafické vedení, je v dnešní době klíčovým ustanovením pro soukromí v elektronické komunikaci. Over-the-top služby v podobě Skype, Messenger, Viber, WhatsApp a mnoho dalších, které umožnují přímo komunikaci osob za využití elektronického zařízení, rovněž podléhají listovnímu tajemství. V České republice je tato komunikace chráněn zákonem o elektronických komunikacích: vzhledem k zastaralé úpravě a nástupu nových technologií se tedy, analogicky jako v případě Nařízení GDPR, uvažuje o nové, celoevropské úpravě v podobě směrnice e-Privacy. Ta je v době přípravy této studie stále v legislativním procesu.

Ač má právo na soukromí mnoho podob, klíčovým však stále zůstává v kontextu ochrany osobních údajů. To však neznamená, že by legislativa na jejich ochranu měla zůstat osamocena a na ostatní oblasti soukromí by neměl být brán zřetel. Soukromí je vedle Nařízení GDPR chráněno také prostřednictvím jiných předpisů, jako jsou např. zmíněný zákon o elektronických komunikacích, zákon o některých službách informační společnosti nebo tiskový zákon. Pro účely této studie je nezbytné dodat, že soukromí včetně osobních údajů jsou chráněny i trestním zákoníkem a především zákoníkem práce.

Vedle uvedených primárně veřejnoprávních předpisů podléhá ochrana osobních údajů jakožto právo na soukromí ochraně osobnosti. Práva na ochranu osobnosti se objevují především v novém občanském zákoníku. Jejich úprava a systematické zařazení v zákoně naznačuje, že jde o práva absolutní, působící *erga omnes*, tzn. vůči všem. Každému subjektu údajů má tak být poskytnuta možnost, aby zakázal jakékoliv zásahy do jeho soukromí. V oblasti technologického rozvoje jde o velmi složitě naplnitelný předpoklad, který ovšem zatím nedošel jiné doktrinální úpravy. Pokud tedy k takovému zásahu má dojít, může subjekt údajů po rušiteli nejen požadovat, aby bylo od zásahu upuštěno, ale může i žádat náhradu vzniklé újmy. Zásahy do soukromí budou přitom vyvolávat primárně újmu nemajetkovou, lze však v historii Soudního dvora Evropské unii najít i případy, kdy v důsledku zásahu do soukromí došlo k majetkové újmě. Tyto případy mívají velmi těsnou vazbu na pracovní právo.

U úpravy ochrany soukromí a zprostředkovaně ochrany osobních údajů je nezbytné hledět na zásadu proporcionality jakožto nástroj ústavního práva. Právo na ochranu soukromí není právem absolutním: oproti ostatním základním právům působí poměrně a je nutno jej vzájemně vyvažovat pro dosažení veřejného zájmu. Dalšími možnostmi, které se pravidelně v souvislosti s proporcionalitou práva na ochranu soukromí objevují, je s právem na svobodu projevu, právem na svobodný přístup k informacím. Pro účely této studie je nezbytné zmínit i jistou proporcionalitu s majetkovým právem, ochrany vlastnictví a z nich vyplývajících práv na ochranu zájmů zaměstnavatele.

### Posun v právní úpravě

Od 25. května 2018 je způsobilé vyvolávat právní účinky tzv. Nařízení GDPR, které napříč EU nahradí předchozí směrnici 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tato směrnice se stala v době digitální ekonomiky a rozvoji technologie již značně zastaralou, zejména pokud jde o prostředky, které jsou ke zpracování využívány a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami let (např. v oblasti profilování, automatizace zpracování osobních údajů atd.) a tudíž je i rizikovější pro práva a svobody fyzických osob. Zároveň v jednotlivých zemích Evropské unie nebyla Směrnicí 95/46/ES dosažena požadovaná míra sjednocení právní úpravy, což správcům působícím ve více zemích činilo problémy.

Cílem tedy bylo přizpůsobit právního rámce ochrany osobních údajů dnešní době a dosáhnout větší jednoty právního rámce ve všech zemích, na které dopadá. Dále se jednalo o posílení práv subjektů údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady, které jsou za oblast ochrany osobních údajů v jednotlivých zemích zodpovědné.

V základních bodech Nařízení GDPR není revolucí, jelikož jde o kontinuitu se zmíněnou Směrnicí 95/46/ES, která jím bude zrušena. Je nutné si uvědomit, že od roku 2000 upravuje zpracování osobních údajů v České republice zákon č. 101/2000 Sb., o ochraně osobních údajů, který vychází ze zmíněné směrnice. Každá organizace by již tedy měla zpracovávat osobní údaje podle tohoto zákona. Nařízení ovšem z hlediska unijního práva a jeho dlouhodobé judikatury je přímo použitelné: tato skutečnost vyplývá z charakteru nařízení Evropské unie.

Obecné nařízení nemění základní zásady zpracování osobních údajů či základní pojmy jako jsou např. osobní údaj, subjekt údajů, správce, zpracovatel či zpracování. Nerozšiřuje ani svoji působnost oproti současné právní úpravě. Pro některá zpracování, resp. subjekty, však klade vyšší nároky při zpracování osobních údajů a to jak z hlediska výkonu jejich činnosti, tak ve vztahu k pracovněprávním vztahům. Typicky jde o velké správce osobních údajů typu bank, telekomunikačních operátorů atd., tj. pro správce, kteří zpracovávají rozsáhlé množství osobních údajů a které je současně ze své podstaty rizikové pro práva a svobody subjektů údajů, tedy fyzických osob, o nichž jsou osobní údaje zpracovávány.

Na druhou stranu pro drobné živnostníky apod., kteří de facto zpracovávají osobní údaje svých zákazníků pouze pro účely poskytnutí služby či výrobku, nepřináší nařízení GDPR zásadní změny oproti stávající úpravě a v takových případech je nutné zejména sledovat dodržování základních zásad zpracování.

Pokud jde o stanovení práv a povinností, není mezi nařízením a zákonem rozdíl, oba dva právní předpisy přímo adresátům stanovují práva a povinnosti. Jistou zvláštností nařízení GDPR je jeho preambule, která obsahuje tzv. recitály, což jsou ustanovení předcházející vlastnímu textu nařízení a jsou v některých případech výkladem či do jisté míry důvodovou zprávou k vlastnímu textu nařízení. Je tak vhodné při práci s nařízením sledovat i příslušné recitály. Dále je nutné vzít v potaz, že celý právní rámec bude dotvářet adaptační zákon, který bude obsahovat i drobné (povolené) odchylky či zvláštní úpravy k obecnému nařízení.  Kompletní právní rámec ochrany osobních údajů tak bude tvořen obecným nařízením a adaptačním zákonem.

Jelikož obecné nařízení stanovuje práva a povinnosti při zpracování osobních údajů, v tomto rozsahu zákon č. 101/2000 Sb., o ochraně osobních údajů nahrazuje. Práva a povinnosti v současném zákoně o ochraně osobních údajů budou nahrazeny právy a povinnostmi přímo vyplývajícími z nařízení GDPR a zákon o ochraně osobních údajů bude účinností adaptačního zákona zrušen.

Jak bylo uvedeno výše, vyvstává nutnost přijmout tzv. adaptační zákon, který bude přijat v souvislosti s přímou použitelností obecného nařízení. Tento zákon, jež nese název zákon o zpracování osobních údajů a v době přípravy této studie stále leží v legislativním procesu, bude upravovat např. aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho opětovné zákonné ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou obecným nařízením upraveny nebo které obecné nařízení umožňuje upravit na vnitrostátní úrovni. U některých aspektů obecné nařízení výslovně předpokládá vnitrostátní úpravu. Mezi ně patří například aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby. Právě tento adaptační zákon bude klást důraz i na zpracování údajů o trestněprávní činnosti osob, respektive další zpracování, které se týkají trestní minulosti osob.

Adaptační zákon je důležitý ještě z jednoho důvodu: z působnosti nařízení GDPR je vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. To je předmětem úpravy Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Jelikož jde o směrnici, je nutné její provedení, které bude vesměs v adaptačním zákoně. I v tomto případě tak lze vysledovat určité prvky ochrany údajů souvisejících s trestnou činností, kterou jsou postaveny částečně mimo standardní předpis.

### Hledisko pracovněprávních vztahů v oboru ochrany osobních údajů

Ochrana osobnosti a osobních údajů se promítá i do pracovněprávní roviny, kde je celkovým cílem ochrana slabší strany: zaměstnance. V souvislosti se zákoníkem práce a pracovněprávními vztahy má pro praktické účely zastoupení zejména v ustanovení § 30 a zejména pak v podobě ustanovení § 316, nadepsaného „Majetek zaměstnavatele; soukromí zaměstnavatele; nesouvisející informace“. Ustanovení se tak přímo dotýká hned několika tematických okruhů: nejdůležitějším z nich je ochrana soukromí zaměstnance ve vzájemném vztahu s ochranou majetku zaměstnavatele. Na místě ustanovení je nejprve upraven výkon práva kontroly, resp. práva zavést sledovací opatření, a ve čtvrtém odstavci je následně upraven obecný rámec pro získávání informací týkajících se zaměstnance. Právě tento rámec je klíčovým pro zpracovávání osobních údajů souvisejících s trestnou činností osob.

Zaměstnanec je povinen zaměstnavateli buď sdělovat, nebo umožnit sběr informací a údajů, které s ním souvisejí a tato data jsou relevantní pro výkon práce, kterou má zaměstnanec v rámci své činnosti u zaměstnavatele vykonávat. Zaměstnanec je současně povinen poskytnout zaměstnavateli údaje, které on potřebuje ke splnění svých právních povinností. Zaměstnavatel tedy zcela jistě bude zpracovávat údaje zaměstnance: kritickou otázkou je rozsah těchto údajů. Právo kontrolovat zaměstnance, vyplývající z práva na ochranu majetku zaměstnavatele, je v tomto případě v kontrastu s právem na ochranu soukromí a důstojnosti člověka.

Ustanovení § 316 nepředstavuje právní základ právní povinnosti pro zpracování osobních údajů: není zde totiž naplnit prvek obligatornosti, který by zaměstnavatele zavazoval zpracování provádět. Zaměstnavatel je nicméně na základě tohoto ustanovení oprávněn provádět kontrolu zaměstnance za účelem předejití možným škodám. Ustanovení pak usilují o omezení zaměstnavatele, aby tak nečinil zvlášť intenzivně a systematicky, ať už se děje otevřeně či skrytě. Za účelem ochrany majetku je tak za určitých okolností a splnění předpokladů, které jinak stanoví zákoník práce, je zaměstnavatel oprávněn provádět kontrolu zaměstnance zejména formou (i) otevřeného sledování, (ii) odposlechu a záznamu zaměstnancových telefonických hovorů, (iii) přístupu na internet (monitorování pohybu na internetu), (iv) užívání aplikačního vybavení přiděleném počítači, přiděleným zaměstnavatelem, (v) sledování služebního vozidla prostřednictvím lokačních systémů, a (vi) kontrolou elektronické pošty nebo listovních zásilek adresovaných zaměstnanci. Vždy však musí ověřit, zda má pro zpracování závažný důvod, jakož i další požadavky dle Nařízení GDPR.

Kontrola musí provedena přiměřeným způsobem. Současně je třeba splnit podmínku dostatečného (nikoliv úplného, viz dále) informování všech dotčených zaměstnanců o rozsahu monitoringu a o způsobech jeho provádění. Prováděním sledovacích opatření nesmí dojít k nepřiměřenému zásahu do soukromí zaměstnance. V případě, že zaměstnavatel využije některé své vlastní zaměstnance k provedení sledovacích opatření v rámci výkonu jejich práce, nepůjde z hlediska právní úpravy o třetí osoby, které by vstupovaly do vztahu, nýbrž za zosobnění zaměstnavatele samotného.

Tato úprava monitoringu zaměstnance ze zákoníku práce je však pouze částí relevantní právní úpravy. Další omezení vyplývají z obecných povinností Nařízení GDPR. Tyto povinnosti se na zaměstnavatele aplikují také tehdy, jestliže bude zaměstnavatel využívat sledovacího systému, který bude uchovávat záznam pořizovaných záběrů či informací, a zároveň účelem takto pořizovaných záznamů (informací) je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Takovým systémem je např. kamerový systém, různé systémy sledující práci na počítači, monitorující e-mailovou korespondenci či telefonní komunikaci. V případě kamerového systému je nutno zdůraznit, že musí jít o systém, který bude sledovat uzavřené prostory, kde se předpokládá pohyb osob. Sledovací systém, který pouze zprostředkuje aktuální snímek sledovaného děje bez následné archivace, dle současné právní doktríny nezpracovává osobní údaje: avšak stále jde o zásah do práva na soukromí, které je nutno posuzovat proporcionalitou práv a ze kterého pro zaměstnavatele vyplývá splnění právních povinností. Zaměstnanec může udělit platný souhlas se zásahem do jeho práva na soukromí pouze tehdy, kdy by jeho nesouhlas nezavdal omezení či postihu ze strany zaměstnavatele. Z takového důvodu lze vidět titul souhlasu v pracovněprávních vztazích jako částečně obsolentní.

Účelem monitoringu zaměstnance bude primárně ochrana majetku zaměstnavatele, spoluzaměstnanců a jiných osob. Nemusí to však být výlučný důvod: lze si představit situace, kdy může být legitimním účelem ochrana života a zdraví zaměstnance, spoluzaměstnanců a jiných osob – typicky půjde o využití lokalizačních systémů při výkonu práce zaměstnance v terénu, kdy hrozí riziko úrazu vyplývající z povahy práce. Dalšími důvody pro monitoring může být kontrola pracovní výkonnosti zaměstnance. Důvod, pro který zaměstnavatel zahájí sledovací opatření, určuje a do značné míry limituje způsob provedení kontroly. Tomuto důvodu musí být přizpůsobeny organizační a technické parametry prováděného monitoringu a nastavení monitorovacích zařízení, včetně jejich rozsahu. Nejvíce omezujícím je v tomto směru sledování pracovní výkonnosti zaměstnance: zde se objevuje dělení na činnost v širším a užším smyslu.

Rozsah sledovaných a zaznamenávaných informací je ovlivněn důvodem, pro který se sledovací opatření zavádějí. Ze stávající judikatury evropských a českých soudů a rozhodnutí Úřadu pro ochranu osobních údajů vyplývá, že zaměstnavatel nesmí sledovat, monitorovat a zpracovávat obsah telefonické, e-mailové a listinné korespondence svých zaměstnanců. Bez dalšího lze sledovat počet došlých a odeslaných e-mailových zpráv, a to včetně adresy odesílatele. Pokud jde o telefonický hovor, pak je podstatně snížena nebezpečnost jednání včasným upozorněním dotčených osob o zavedení sledovacích opatření (rozhodnutí NS 21 Cdo 1009/98). V případě sledování pohybu zaměstnance na internetu je přípustné monitorovat (nahodile) datum, hodinu a čas strávený prohlížením určité webové stránky. V tomto případě se tak jako daleko vhodnější efektivnější metoda ochrany majetku zaměstnavatele jeví nikoliv monitoring a zpracování osobních údajů z něj vyplývající, nýbrž právně bezvadná je předchozí blokace určitých pro výkon práce nepoužitelných www stránek, domén a přístupu do sociálních sítí.

Zaměstnavatel je obvykle oprávněn provádět pouze otevřené sledování: je proto povinen předem informovat zaměstnance o rozsahu monitoringu (jaké údaje budou shromažďovány) a o způsobech jejího provádění (kde a po jakou dobu budou shromážděné údaje uschovány, kdo k nim má přístup, kdo bude provádět kontrolu, které údaje se budou dlouhodobě archivovat, jaká jsou bezpečnostní opatření na zabránění neoprávněného přístupu atd.). Měl by tak ve smyslu stanoviska WP 29 k transparentnosti učinit rozmístěním informativních cedulí a dále podrobnou úpravou ve vnitřním předpise (či kolektivní smlouvě. Sledování je možno provádět pouze namátkově, zaměstnanec musí mít šanci „uniknout“ (tzv. princip „fair play“). Sledovat lze prostory, kde došlo k protiprávnímu jednání (např. opakované krádeže) nebo jde o plnění povinností stanovených obecně závaznými právními předpisy (např. zajištění bezpečnosti a ochrany zdraví při práci).

K invazivnosti sledovacích opatření je třeba uvést, že sledování výkonnosti zaměstnanců je především povinností vedoucího zaměstnance. Především tento zaměstnanec by měl být přítomen na pracovišti a soustavně sledovat výkonnost podřízených zaměstnanců. Ihned po zjištění protiprávního jednání pak musí zaměstnavatel učinit oznámení na policii, případně jiných příslušných orgánech. Dlouhodobě lze archivovat pouze pozitivní záznamy (důkaz o protiprávním jednání, dochází ke změně důchodu evidence a archivace těchto osobních údajů). Pokud je předmětem kontroly výkonnost zaměstnance či na záznamu mohou být obsaženy záznamy zaměstnance, je vhodné takovému zaměstnanci umožnit zhlédnutí pořízeného záznamu (princip transparence).

Zaměstnavatel je povinen přijmout taková technická a organizační opatření, která zamezí neoprávněnému přístupu k archivovaným záznamům (např. přístup k elektronickým datům je umožněn po zadání hesla, jsou archivovány údaje o osobě prohlížející údaje, uschovávají se záznamy o učiněných změnách, data jsou chráněna šifrováním, kódováním dat v případě přenosu dat jinému subjektu, sjednávají se zpracovatelské smlouvy atd.). V případě využití dodavatelského subjektu, který bude konat zpracování za účely zaměstnavatele a pouze podle jeho pokynů, musí současně zaměstnavatel uzavřít písemnou zpracovatelskou smlouvu, ve které vymezí rozsah, účelem a dobu, na jakou se sjednává, a záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

Vedle obecných doporučení uvedených v předchozím bodě lze učinit několik poznatků k monitorování e-mailové korespondence. ÚOOÚ ve stanovisku č. 2/2009 rozlišuje mezi soukromou a úřední e-mailovou adresou a mezi soukromým a pracovním e-mailem. Pokud je e-mailová adresa složena ze jména a příjmení zaměstnance, např. Jan.Svoboda@doména.cz, je dle ÚOOÚ e-mail na ni doručený soukromou elektronickou poštou. Naopak věcně konstruovaná e-mailová adresa, např. info@doména.cz, je dle ÚOOÚ úřední elektronickou adresou, a to i v případě, že ji spravuje pouze jeden zaměstnanec (stanovisko č. 2/2009). Předmětné stanovisko je nutno vzhledem ke způsobu jeho vzniku brát s rezervou. Přesto by neměl zapadnout poznatek o soukromé a úřední e-mailové adrese. Není-li v názvu e-mailové adresy použito jméno zaměstnance a e-mailový účet je obhospodařován více zaměstnanci současně či postupně, je zaměstnancovo očekávání míry soukromí při e-mailové korespondenci nutně minimální. Nejnižší (tj. nulové) očekávání soukromí mohou mít zaměstnanci obhospodařující datovou schránku zaměstnavatele, resp. elektronickou podatelnu orgánu veřejné správy. Ne zcela lze souhlasit s existencí soukromé e-mailové adresy v případech, kdy je e-mailový účet zřízen zaměstnavatelem na pracovní počítačové stanici v majetku či užívání zaměstnavatele za účelem využití při výkonu práce. Identifikace e-mailové adresy jménem zaměstnance však na druhou stranu bezesporu zvyšuje míru očekávání soukromí ze strany tohoto zaměstnance. ÚOOÚ dále uvádí, že e-mailovou poštu doručenou na „soukromou“ e-mailovou adresu smí zaměstnavatel otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail (čímž je ale popřeno předchozí rozlišení na soukromý e-mail). Povaha e-mailu je pro jeho rozlišení jistě rozhodující. O jaký e-mail se jedná, lze usoudit z tzv. identifikačních znaků, jako jsou odesílatel, předmět a oslovení příjemce. V případě, že se jedná o e-mail pracovní, který byl doručen na pracovní e-mail, pak je způsob jeho vyřízení obdobný vyřizování neosobní (úřední) listinné korespondence. Bude-li pracovní e-mail doručen na soukromou e-mailovou adresu, pak lze tento vyřídit bez účasti zaměstnance, kterému byl předmětný e-mailový účet zřízen, jestliže daný zaměstnanec není neočekávaně dlouhodobě schopný došlou e-mailovou korespondenci vyřizovat (např. pro nemoc). I zde se však nanejvýš doporučuje předchozí úprava v dohodě se zaměstnancem a ve vnitřním předpisu. Pro situace, kdy lze předvídat nepřítomnost zaměstnance, by měl zaměstnavatel dohodnout pravidla vyřizování takové korespondence.

Jedná-li se o e-mail soukromý, který byl doručen na pracovní či soukromou e-mailovou adresu, pak zaměstnavatel není bez dalšího oprávněn k přečtení (dočtení) či vyřízení této korespondence. Může však požadovat po zaměstnanci, aby tuto korespondenci odstranil, resp. vyzvedl a zpracoval mimo pracoviště v době svého odpočinku. Vyřizování soukromé korespondence v pracovní době je porušením pracovních povinností.

Dle čtvrtého odstavce ustanovení § 316 smí zaměstnavatel vyžadovat od zaměstnance informace, které bezprostředně souvisejí s výkonem práce a se vznikem, změnou, existencí či zánikem pracovněprávního vztahu. Zvláštní režim platí pro informace týkající se sexuální orientace zaměstnance, jeho původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, a příslušnosti k církvi nebo náboženské společnosti. Na tyto informace se zaměstnavatel dle předmětného ustanovení nesmí ptát vůbec. Informace týkající se těhotenství, rodinných a majetkových poměrů a trestněprávní bezúhonnosti může zaměstnavatel vyžadovat pouze tehdy, pokud mu to ukládá tento zákon či zvláštní předpis nebo existuje přiměřený a ospravedlnitelný důvod vztahující se k povaze práce (např. práce zakázána těhotným ženám, nemožnost zabezpečit neprodleně náhradníka v případě náhlé nepřítomnosti zaměstnance atd.).

### D. Zpracovávání údajů souvisejících s trestní minulostí

Na rozdíl od dřívější úpravy ochrany osobních údajů Nařízení GDPR neoznačuje osobní údaje týkající se rozsudků v trestních věcech a trestných činů za součást citlivých údajů: namísto toho stanoví speciální (nikoliv zvláštní) kategorii a definuje pro jejich zpracování odlišné podmínky. Ve směrnici 95/46/ES je tato kategorie osobních údajů vymezena samostatně, podobným způsobem jako v Nařízení, přičemž čl. 8 odst. 5 uvedené směrnice do této kategorie řadí osobní údaje „týkající se protiprávního jednání, rozsudků v trestních věcech nebo bezpečnostních opatření“. Česká republika toto ustanovení do původního zákona o ochraně osobních údajů implementovala s poněkud restriktivnějším výčtem a ochranu omezuje pouze na osobní údaje o odsouzení za trestný čin.

Dle výše uvedeného tak současný výklad ustanovení do této speciální kategorie nezařazuje např. informace o podmíněném zastavení trestního stíhání podle § 307 tr. řádu, o narovnání podle § 309 tr. řádu apod., jelikož se o údaj o odsouzení nejedná. Zároveň se ochrana nevztahuje ani na údaje o bezúhonnosti, jelikož taková ochrana by byla zjevně v rozporu se smyslem tohoto ustanovení. Naopak údaje získané z opisu z rejstříku trestů dle § 10 odst. 5 zák. o Rejstříku trestů do této kategorie spadají, jelikož ten obsahuje údaje o každém odsouzení fyzické osoby, které se opis týká, a všechny údaje o průběhu výkonu trestů a ochranných opatření i o zahlazení odsouzení, tedy i informace o zahlazených odsouzeních dané osoby. Nařízení tuto kategorii osobních údajů oproti zákonu o ochraně osobních údajů značně rozšiřuje, jelikož se tento přísnější režim nově vztahuje na zpracování jakýchkoliv osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření (dále jen „údaje o trestných činech“). Lze proto předpokládat, že se ochrana dle Nařízení vztáhne také na výše uváděné údaje o podmíněném zastavení trestního stíhání, narovnání apod.

V souladu s dřívější právní úpravou by do této kategorie ani dle Nařízení GDPR neměly patřit údaje o bezúhonnosti osoby. Vzhledem k povaze takového údaje lze jen těžko mít za to, že by při kontinuitě znění , jelikož povaha ustanovení se v Nařízení nemění a i zde by byla ochrana takového ustanovení v rozporu s cílem přiznat zvýšenou míru ochrany práv a svobod subjektů údajů. Lze si totiž jen těžko představit, že by údaj o bezúhonnosti mohl znamenat riziko pro práva a svobody subjektu údajů. Stejně jako citlivé údaje požívají i údaje o trestných činech v různých institutech Nařízení zvýšenou ochranu. Kromě zvláštních požadavků na zpracování stanovených v tomto článku obsahuje Nařízení v řadě ustanovení přísnější úpravu pro případy, v nichž bude docházet ke zpracování údajů o trestných činech.

Dle znění Nařízení GDPR musí zpracování údajů o trestných činech (i) probíhat pod dozorem orgánu veřejné moci nebo (ii) být oprávněné podle práva EU či členského státu, přičemž toto oprávnění musí poskytovat vhodné záruky, pokud jde o práva a svobody subjektů údajů. Pro údaje o trestných činech se tak výrazně zužuje šíře právních základů, na jejichž základě je možné údaje zpracovávat.

První případ, kdy je údaje o trestných činech možné zpracovávat, je situace, kdy zpracování probíhá pod dozorem orgánu veřejné moci. Pod takovýmto dozorem probíhá např. zpracování rejstříku trestů orgány veřejné moci, které mohou osobní údaje z rejstříku trestů zpracovávat v souladu s § 15a a násl. zák. o Rejstříku trestů. Údaje o trestných činech lze zpracovávat také tehdy, je-li zpracování oprávněné podle práva EU či členského státu, přičemž toto oprávnění musí poskytovat vhodné záruky, pokud jde o práva a svobody subjektů údajů. Příkladem oprávněného zpracování může být např. zpracování údajů o trestněprávní bezúhonnosti či výpisu z rejstříků trestů zaměstnavatelem při výběru uchazečů o zaměstnání.

Jak bylo uvedeno v odstavci 24 studie, údaj o tom, že osoba v minulosti nebyla odsouzena za trestný čin, do této kategorie nejspíše nespadne. Zaměstnavatel však nemůže automaticky předpokládat, že všichni uchazeči o zaměstnání předloží výpis bez údajů o trestných činech, a pokud předložení výpisu požaduje, musí být připraven s nimi jako s údaji o trestných činech zacházet. Požadování údajů o bezúhonnosti zaměstnavatelem je dle ustanovení § 316 odst. 4 zákoníku práce dovoleno jen v případě, že je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví tento zákon nebo zvláštní právní předpis. Tyto informace nesmí zaměstnavatel získávat ani prostřednictvím třetích osob. Právní úprava poskytuje poměrně vysokou míru ochrany práv a svobod subjektů údajů, nicméně s účinností Nařízení nemusí tato úroveň postačovat. Kromě zvláštních požadavků na zpracování stanovených v tomto článku obsahuje Nařízení v řadě ustanovení přísnější úpravu pro případy, v nichž bude docházet ke zpracování údajů o trestných činech. Konkrétní pravidla pro zpracování údajů o bezúhonnosti uchazečů o zaměstnání budou tedy nejspíše ještě upřesněna legislativou ČR.

Vedle podmínek pro zpracování údajů o trestných činech uvedených v čl. 6 a 8 Nařízení GDPR nelze zapomínat ani na další veřejnoprávní předpisy, které takovým údajům přiznávají ochranu. V první řadě se jedná o úpravu v trestním řádu, která v § 8a–8d upravuje způsob, jakým orgány činné v trestním řízení informují o své činnosti, dále pak zákaz omezení zveřejňování údajů o nezletilých a údajů o poškozeném a omezení zveřejňování pravomocného rozsudku ve veřejných sdělovacích prostředcích. Ochrana údajů mladistvých je pak zakotvena v zákoně č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů.

Na základě výše uvedeného bychom tedy mohli shrnout, že výpis z rejstříku trestů může zaměstnavatel vyžadovat a uchazeč o zaměstnání ho musí předložit pouze ve dvou případech. První je případ, kdy přímo z povahy práce vyplývá, že k jejímu výkonu je nezbytná bezúhonnost, přičemž je právní povinností zaměstnavatele tento fakt ověřit: tuto právní povinnost nalezneme např. v zákoně č. 109/2002 Sb., v platném znění, který vyžaduje bezúhonnost pedagogických i nepedagogických pracovníků zajišťujících výkon ústavní a ochranné výchovy ve školských zařízeních. Současně u pracovních místech ve školství lze dodat, že požadavek na předložení výpisu z rejstříku trestů u nepedagogických zaměstnanců může být někdy rovněž přiměřený a odůvodnitelný. Veřejný ochránce práv ve svém stanovisku z roku 2011 uvádí: "*Bude tedy zajisté namístě, pokud na pozici vychovatele dětského domova, jakož i na jiná pracovní místa v takovém či obdobném zařízení, nebude přijata osoba odsouzená např. za pohlavní zneužívání či týrání svěřené osoby*." Takovéto nebezpečí hrozí nejen u pedagogů, ale i nepedagogických pracovníků, kteří během výkonu své práce přicházejí do kontaktu s dětmi, žáky, studenty. V každém případě by měl zaměstnavatel zaměstnance informovat, na základě kterého zákonného předpisu výpis z trestního rejstříku jako doklad o bezúhonnosti požaduje.

Druhým případem bude situace, kdy požadavek bezúhonnosti sice nevyplývá přímo z právního předpisu, avšak z logiky věci musí zaměstnavatel v případě konkrétního pracovního místa hledat zaměstnance, u kterého lze předpokládat určitou důvěryhodnost v souvislosti s nabídkou pracovního místa. Typicky půjde o pracovní místa, ve kterých bude mít zaměstnanec hmotnou odpovědnost: zde si lze jen těžko představit přijetí osoby, která byla odsouzena za majetkovou trestnou činnost. Vždy je však nutné posoudit povahu trestné činnosti uchazeče vzhledem k charakteru práce, kterou by měl vykonávat. Pokud je zaměstnavateli výpis z Rejstříku trestů zaměstnancem dobrovolně předložen, měla by být vždy zvažována závažnost a povaha spáchaného trestného činu ve vztahu k charakteru nabízeného pracovního místa.

Pro naprostou většinu nekvalifikovaných manuálních prací přitom vyžadovat bezúhonnost uchazeče o zaměstnání není adekvátní, přičemž právě u nabídek těchto prací se setkáváme nejčastěji s požadavkem zaměstnavatele na předložení důkazu o bezúhonnosti. Ověření tohoto bodu za využití analyticko-deskriptivní metodologie je jedním z cílů této studie.

# Teoretická část

### Náborový proces

Zaměstnavatel smí v souvislosti s jednáním před vznikem pracovního poměru nebo před uzavřením dohody o provedení práce nebo dohody o pracovní činnosti vyžadovat od fyzické osoby, která se u něho uchází o zaměstnání, nebo od jiných osob jen ty údaje, které bezprostředně souvisejí s přijetím do zaměstnání. V souladu s Nařízením GDPR se tak ještě před vznikem pracovněprávního vztahu u zaměstnavatele zamezuje nadbytečnému shromažďování údajů o budoucím zaměstnanci a tím i jejich možnému zneužití.

Výběrové řízení, v němž se „hledá“ vhodný zaměstnanec, musí zaměstnavatel vést neutrálně a nesmí odrazovat fyzické osoby z hlediska pohlaví, rasy, víry, věku apod. Rovněž výběr zaměstnanců musí provádět tak, aby nedocházelo k diskriminaci zaměstnanců nebo k porušování zásady rovnosti, která se uplatňuje v pracovněprávních vztazích. Je proto zakázán takový postup zaměstnavatelů při výběru zaměstnanců, v němž by zjišťovali další a jiné údaje, které nesouvisejí s pracovním uplatněním (např. informace o příbuzných, vyznamenáních, rodinný stav). V rozporu se zákonem jsou tzv. diskriminační dotazníky, které mnozí zaměstnavatelé dávají zaměstnancům k vyplnění při přijímacích rozhovorech. Výjimka platí pouze pro případy, kdy vyžadování těchto údajů je odůvodněno podstatným a rozhodujícím požadavkem pro výkon zaměstnání, které má občan vykonávat a který je pro výkon tohoto zaměstnání nezbytný. Např. pro výkon zaměstnání, který je spojen s hmotnou zainteresovaností a vyžadují se k němu určité bezúhonnostín předpoklady, je zřejmě správným požadavkem zaměstnavatele výpis z rejstříku trestu zaměstnance. U některých profesí, např. u pedagogických pracovníků, musí zaměstnavatel vyžadovat výpis z rejstříku trestů ve všech případech. Nelze však obecně tvrdit, že některé údaje musí zaměstnavatelé vyžadovat vždy. Záleží na charakteru a druhu práce.

Pro náborový proces je klíčové ustanovení § 316 odst. 4 lze zákoníku práce, které částečně odchyluje a upřesňuje úpravu Nařízení GDPR . Zaměstnavatel smí vyžadovat od zaměstnance informace, které bezprostředně souvisejí s výkonem práce a se vznikem, změnou, existencí či zánikem pracovněprávního vztahu. Zvláštní režim platí dle § 316 odst. 4 pro informace týkající se sexuální orientace zaměstnance, jeho původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, a příslušnosti k církvi nebo náboženské společnosti. Na tyto informace se zaměstnavatel dle předmětného ustanovení nesmí ptát vůbec. Toto pravidlo však bylo nepřímo novelizováno § 6 Antidiskrimačního zákona, který umožňuje zaměstnavateli za stanovených podmínek znevýhodnit uchazeče o zaměstnání, resp. zaměstnance z důvodu příliš vysokého nebo příliš nízkého věku. Konkrétní úpravu přinesl § 6 odst. 4 též pro církve a náboženské společnosti, které se tak (po právu) mohou ptát na náboženské vyznání, víru či světový názor uchazeče o zaměstnání, resp. zaměstnance. Z rozumného uspořádání věcí plyne, že církev či náboženské společnosti se mohou ptát (v rozporu s § 316 odst. 4) též na příslušnost k církvi nebo náboženské společnosti. Informace týkající se těhotenství, rodinných a majetkových poměrů a trestněprávní bezúhonnosti může zaměstnavatel vyžadovat pouze tehdy, pokud mu to ukládá tento zákon či zvláštní předpis nebo existuje přiměřený a ospravedlnitelný důvod vztahující se k povaze práce (např. práce zakázána těhotným ženám, nemožnost zabezpečit neprodleně náhradníka v případě náhlé nepřítomnosti zaměstnance atd.). Odbornou obcí do značné míry otřásl SD EU rozhodnutím ve věci *Galina Meister*. Zde (zjednodušeně řečeno) bylo potvrzeno, že zaměstnavatele nesdělujícího či nevysvětlujícího důvody odmítnutí uchazeče o zaměstnání je téměř nemožné usvědčit z diskriminace.

### Přijmutí do zaměstnání

Po přijmutí do zaměstnaná se mění účel zpracování údajů: zaměstnavatel tudíž smí shromažďovat pouze takové osobní údaje, které jsou nezbytné pro naplnění stanoveného účelu, v daném případě plnění povinnosti zaměstnavatele. Tyto povinnosti spočívají ve výpočtu mzdy, hlášení na sociálním úřadě a odvodu sociálního a zdravotního pojištění. V případě, že zaměstnanec pobírá slevu na daních na své děti, musí zaměstnavatel dodat, a tudíž zpracovávat, rodná čísla dětí zaměstnanců. V případě, že zaměstnavatel svým zaměstnancům také vyplňuje daňová přiznání, potřebuje navíc mít informace o manželovi / manželce. Pro výpočet mzdy bývá často potřebné znát předchozí zaměstnání. Otázku, zda je zaměstnanec kuřák či nekuřák je rozumné vyřešit při přijímání: např. v provozovně společnosti není dovoleno kouřit. Další dovednosti, ke kterým se zaměstnanec sám hlásí, lze brát jako jeho přednosti pro případ hledání jeho lepšího využití zaměstnavatelem.

Při nástupu do zaměstnání uzavírá zaměstnavatel s budoucím zaměstnancem pracovní smlouvu, která podle zákoníku práce obsahuje identifikační údaje zaměstnance (podle správního řádu jméno, příjmení, datum, místo narození a místo trvalého pobytu).

Zaměstnavatel má právo zpracovávat tyto osobní údaje:

* **Pro evidenční listy důchodového pojištění zasílaných na OSSZ** (podle § 37 zákona o organizaci a provádění sociálního zabezpečení): datum a místo narození, všechna dřívější příjmení, rodné číslo, místo trvalého pobytu. Byl-li občan účasten důchodového pojištění v cizině a zaměstnavatel je jeho prvním zaměstnavatelem po ukončení důchodového pojištění v cizině, rovněž údaj o názvu a adrese cizozemského nositele pojištění a cizozemském čísle pojištění).
* **Pro správný výpočet mzdy**: vzdělání, předchozí praxe
* **Pro správný výpočet měsíčních záloh na daně** (podle zákona o správě daní a poplatků): druh pobíraného důchodu
* **Pro zjištění přesného data nároku na odchod do starobního důchodu** (podle zákona o organizaci a provádění sociálního zabezpečení): počet dětí (u žen)
* **Pro plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců** (podle § 83 zákona o zaměstnanosti): zdravotní znevýhodnění
* **Pro placení zdravotního pojištění** (podle § 10 zákona o veřejném zdravotním pojištění): zdravotní pojišťovna
* **Za účelem hlášení zaměstnávání cizinců**: státní občanství
* **Prohlášení poplatníka daně z příjmu** (podle zákona o správě daní poplatků):
* **pokud zaměstnanec uplatňuje daňové zvýhodnění a manžel/ka je zaměstnán/a**: příjmení a jméno manžela/ky, název a adresa zaměstnavatele
* **pokud zaměstnanec uplatňuje zvýhodnění na vyživované dítě**: jméno, příjmení a rodné číslo dítěte

Zaměstnavatel ovšem k osobním údajům zaměstnanců musí přistupovat jako k vlastnictví zaměstnanců, které má pouze propůjčené k určitým, předem daným a zákonem stanoveným účelům (viz výše) a používat je výhradně pro tyto své účely: výpočet mzdy, komunikace se zaměstnancem, možnost povýšení. Neoprávněnou osobou je každý, kdo nemá ze zákona povinnost s osobními údaji pracovat. Tudíž je třeba mít personální spisy např. v uzamčených skříních, dostupné pouze oprávněným osobám. Možnost přistupovat do jejich elektronického zpracování musí být omezeno pouze na úzký počet zaměstnanců a je nutné všechna zpracování osobních údajů logovat (vést záznam), přičemž zpracováním se rozumí i nahlížení. Týká se to obzvláště velkých podniků, které zpracovávají statisíce osobních údajů (a často velmi citlivých) a přesto není nijak zaznamenáno, kdo z možných, třeba 25 osob, do nich nahlížel.

U menších podniků, zvláště závodů, je problémem předávání výplatních listů zaměstnancům, což se často děje způsobem, při kterém si ostatní zaměstnanci mohou přečíst mzdu i odměny ostatních. Informace o mzdě a o odměnách jsou osobní údaje, které mohou souviset i se závistí ostatních, tudíž je nelze zpřístupňovat ostatním.

### Evidence neúspěšných uchazečů

Po ukončení výběrového řízení je třeba pečlivě zvážit, zda, k jakému účelu a po jakou dobu hodlá zaměstnavatel dále osobní údaje neúspěšných uchazečů uchovávat a buď je o tom informovat již předem při zahájení zpracování, nebo po ukončení výběrového řízení. Jako dobrou praxi je možné hodnotit uchování těchto údajů pro eventuální budoucí nabídku zaměstnání, což je zpracování z důvodu oprávněného zájmu zaměstnavatele, proti kterému může subjekt údajů, není-li s ním srozuměn, podat námitku. K uchovávání údajů by rozhodně nemělo dojít na dobu delší, než je několik málo let.

Evidence neúspěšných uchazečů je také jednou z mála vhodných příležitostí pro titul souhlasu v pracovněprávním procesu. V případě, že zaměstnavatel řádně informuje a současně souhlas má veškeré kvality GDPR požadované, je možné vytvořit evidenci neúspěšných uchazečů a zpracovávat zde údaje s jejich souhlasem. Pořád bude ale nezbytné myslet na možnost výkonu práv neúspěšného uchazeče, včetně potenciální přenositelnosti údajů pro jiného zaměstnavatele.

### Osobní spis

Nařízení ani vnitrostátní úprava neobsahuje konkrétní výčet údajů, jež mohou být vedeny v osobním spise (shromažďovány).

Písemnosti, které jsou nezbytné pro výkon práce v pracovněprávním vztahu a které je tak zaměstnavatel oprávněn vést v osobním spise, budou především ty, které potvrzují kvalifikaci a obecnou způsobilost zaměstnance k výkonu práce [např. profesní životopis, potvrzení o zaměstnání (§ 313) a pracovní posudek (§ 314) od předchozího zaměstnavatele, osobní dotazník, doklady (opisy) o dosaženém vzdělání a kvalifikaci], ty, které se týkají uzavřeného pracovního vztahu (např. pracovní smlouva, platový výměr, pracovní náplň a jejich změny, podání informace podle § 37, seznámení s pracovním řádem a jinými předpisy vztahujícími se k vykonávané práci, s kolektivní smlouvou a vnitřními předpisy), a ty, které se týkají průběhu a skončení pracovního poměru [např. o absolvovaných školeních a jiných kvalifikačních kurzech, o uzavření dohody o odpovědnosti k ochraně hodnot svěřených zaměstnanci k vyúčtování podle § 252, o uzavřených dohodách nebo rozhodnutí o srážkách ze mzdy nebo platu (§ 147 odst. 2), souhlas zaměstnavatele s výkonem výdělečné činnosti zaměstnance (§ 303 odst. 4, § 304 odst. 1), přehled o fakticky vykonávané práci zaměstnancem, úkon, jímž byl rozvázán pracovní poměr a doklady s tím související (podklady pro rozvázání pracovního poměru, ale i případné rozhodnutí soudu o žalobě podle § 72)].

Písemnostmi, které jsou nezbytné pro výkon práce v pracovněprávním vztahu, nemohou být různá podání a stížnosti (zejména anonymní), kterými se třetí osoby obracejí na zaměstnavatele, a doklady o způsobu jejich vyřízení. Takové dokumenty se týkají toliko vztahu mezi zaměstnavatelem a třetí osobou. Jestliže je zaměstnavatel nepojal jako podklad pro vyvození pracovněprávních důsledků vůči zaměstnanci, nemohou být součástí osobního spisu.

Zákoník práce v § 316 odst. 4 uvádí příkladmý výčet toho, které informace nesmí zaměstnavatel od zaměstnance vyžadovat (o těhotenství, rodinných a majetkových poměrech, sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnosti k církvi nebo náboženské společnosti a trestněprávní bezúhonnosti). Zároveň však stanoví výjimku spočívající v tom, že je-li pro to dán věcný důvod, spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví tento zákon nebo zvláštní právní předpis, tento zákaz neplatí ve vztahu k informacím o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnosti; údaje o sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnosti k církvi nebo náboženské společnosti tak nesmí zaměstnavatel vyžadovat nikdy. Nesmí-li zaměstnavatel uvedené informace vyžadovat, nesmí být ani obsahem osobního spisu, i kdyby se tyto informace dověděl jinak. Stejně tak, pomine-li důvod, pro který mohl zaměstnavatel takový údaj výjimečně evidovat (zaměstnanec přešel na jiné místo, kde takový požadavek není, změnila se právní úprava apod.), musí přistoupit k jeho likvidaci.

Další okruh zakázaných údajů je vymezen v § 12 odst. 2 ZamZ. Týká se sice informací, které zaměstnavatel nesmí vyžadovat v souvislosti s výběrem zaměstnanců a do jisté míry se překrývá se zákazem, uvedeným v § 316 odst. 4, ale ani tyto (nad rámec § 316 odst. 4) zakázané informace nesmí být logicky součástí osobního spisu. Jde zejména o údaje týkající se národnosti, rasového nebo etnického původu, politických postojů, filozofického přesvědčení a odporující dobrým mravům (srov. komentář k § 30).

Údaje o zdravotním stavu zaměstnance podléhají režimu čl. 9 Nařízení GDPR. I když jsou tyto údaje na jedné straně nezbytné pro splnění povinnosti zaměstnavatele přidělovat zaměstnanci práci, která odpovídá jeho schopnostem a zdravotní způsobilosti [§ 103 odst. 1 písm. a) Zákoníku práce], jde zároveň o zvláštní kategorii osobního údaje. Zdravotním údajem odpovídajícím tomuto požadavku tak bude při uzavírání pracovního poměru posudek (lékařské vyjádření), který se vyjadřuje pouze ke vhodnosti sjednávané práce pro zaměstnance (způsobilý – nezpůsobilý, případně s omezením a jakým, nebo typové označení prací, které je s ohledem na svoji zdravotní způsobilost zaměstnanec schopen nebo neschopen vykonávat), aniž by obsahoval konkrétní údaje o zdravotním stavu. Stejné platí o zdravotních potvrzeních z preventivních lékařských prohlídek, případně o posudcích o změně zdravotní způsobilosti. Ve všech těchto případech lze zprávy o zdravotním stavu zakládat do osobního spisu za podmínky, že neobsahují jiné údaje než konstatování zdravotní způsobilosti zaměstnance.

Zákoník práce nestanoví, odkdy může zaměstnavatel údaje o zaměstnanci shromažďovat. Protože osobní spis se týká zaměstnance, počátkem oprávnění zaměstnavatele vést osobní spis (a shromažďovat informace o zaměstnanci) bude vznik pracovního poměru; tímto okamžikem se fyzická osoba stává zaměstnancem. Nic ale nebude bránit zaměstnavateli, aby součástí osobního spisu učinil také podklady, které v souladu s § 30 odst. 2 získal před vznikem pracovního poměru (při respektování zákazu uvedeného v § 12 odst. 2 ZamZ). I takové písemnosti však musí splňovat podmínky shora uvedené.

Mimo to, že výslovně nestanoví, od jakého okamžiku může zaměstnavatel údaje o zaměstnanci shromažďovat, nestanoví zákoník práce, ani dokdy je zaměstnavatel oprávněn osobní spis zaměstnance vést. I zde tedy platí úprava, dle které správce (zaměstnavatel) nebo na základě jeho pokynu zpracovatel (zaměstnanec pověřený vedením osobního spisu) je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů (zaměstnance) Převedeno do poměrů zákoníku práce to znamená, že oprávnění zaměstnavatele vést osobní spis zaměstnance bude zpravidla zanikat se skončením pracovního poměru (účel shromažďování informací pominul). To však nebude platit v případech, kdy i po skončení pracovního poměru budou trvat některé právní vztahy z pracovního poměru vyplývající (např. bude veden spor o náhradu mzdy nebo zaměstnavatel bude hradit náhradu za ztrátu na výdělku apod.). V takových situacích bude pro zaměstnavatele nezbytné (pro plnění jeho povinností) některé shromážděné informace mít stále k dispozici. I v těchto případech bude však platit shora uvedené, že takto lze uchovávat jen ty informace, kterých je potřeba, a jen po dobu, dokud taková potřeba nepomine.

Technologii „likvidaci osobních údajů“ zákoník práce ani Nařízení GDPR podrobně nestanoví (s výjimkou fyzického zničení jejich nosiče nebo jejich fyzické vymazání). Protože „nosičem informací“ rozumí tento zákon nosič, na kterém jsou informace ukládány, nikoli jednotlivé dokumenty, a protože v ostatních případech požaduje jejich trvalé vyloučení z dalšího zpracování, bude to prakticky znamenat především vrácení evidovaných dokumentů jejich předkladatelům (zejména bývalému zaměstnanci). Není-li to možné, je nezbytné jejich fyzické zničení. Je nepřípustné obcházet znění zákona tím, že jsou pořizovány a nadále uchovávány kopie všech informací (nebo jejich části) tvořících osobní spis; takový postup je stejným porušením zákona jako porušení povinnosti provést likvidaci osobních údajů.

Samotné vedení osobního spisu zaměstnance by nemělo žádný význam, pokud by zaměstnavatel údaje v něm shromážděné nemohl také používat. V zájmu zachování ochrany osobních údajů stanoví zákoník práce okruh osob, které mají právo do osobního spisu zaměstnance nahlížet. Pojem „nahlížet do osobního spisu“ nelze vnímat jen úzce jako oprávnění vzít fyzicky spis, v něm listovat a takto se s osobními údaji o zaměstnanci seznamovat. Je-li např. osobní spis veden v elektronické podobě, půjde o sledování elektronického záznamu apod. Jinak řečeno, způsob (technologie) „nahlížení do osobního spisu“ se bude odvíjet vždy od toho, v jaké formě je osobní spis veden. Smyslem ochrany osobních údajů je zajistit, aby se s takovými údaji nemohly seznamovat osoby, kterým to ze zákona není dovoleno. Proto je nutno pod pojem „nahlížet do osobního spisu“ zahrnout všechny způsoby seznamování se s údaji vedenými v osobním spise (včetně jejich zasílání).

Právo zaměstnance na náklady zaměstnavatele nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených zajišťuje, aby zaměstnanec, jehož práv na ochranu osobních údajů se vedení osobních údajů týká, mohl kontrolovat, jaké údaje o něm zaměstnavatel shromažďuje a případně se domáhat svých práv v souladu s právem na vysvětlení (požádat správce nebo zpracovatele o vysvětlení, případně odstranění takto vzniklého stavu; zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů) nebo [§ 78](https://www.beck-online.cz/bo/document-view.seam?documentId=onrf6mrqgezf6obzfzygmnzy), [82](https://www.beck-online.cz/bo/document-view.seam?documentId=onrf6mrqgezf6obzfzygmobs), [2956](https://www.beck-online.cz/bo/document-view.seam?documentId=onrf6mrqgezf6obzfzygmmrzgu3a), [2957 ObčZ](https://www.beck-online.cz/bo/document-view.seam?documentId=onrf6mrqgezf6obzfzygmmrzgu3q) (aby bylo upuštěno od neoprávněných zásahů do jeho práv, aby byly odstraněny následky těchto zásahů a aby bylo dáno přiměřené zadostiučinění, případně též náhrady nemajetkové újmy v penězích). Vedle práva nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, vyplývajícího ze [zákoníku práce](https://www.beck-online.cz/bo/document-view.seam?documentId=onrf6mrqga3f6mrwgi), zůstává zaměstnanci zachováno právo požadovat od správce (zaměstnavatele) informaci o zpracování svých osobních údajů zakotvené v čl. 13 Nařízení GDPR. Právo bude mít i k tomu pověřený zástupce zaměstnance.

### Ukončení pracovněprávního vztahu

Každý správce osobních údajů je povinen přestat osobní údaje zpracovávat v okamžiku, kdy uplyne poslední účel, který má pro jejich zpracování.

V pracovněprávních vztazích je účelem zpracování osobních údajů ze strany zaměstnavatele zpravidla nezbytnost plnit uzavřenou pracovní smlouvu a související právní povinnosti (vést účetní a mzdovou agendu). Jakmile dojde k ukončení pracovního poměru a uzavření související agendy, měl by zaměstnavatel zvážit, zda existuje jiný účel, pro který má nebo může osobní údaje nadále uchovávat, nebo jestli a v jakém rozsahu by měly být vymazány.

Osobní údaje by měly být odstraněny bez možnosti následné obnovy dat. Řada správců osobních údajů však v současné době naráží na skutečnost, že jejich stávající systémy výmaz neumožňují. Provizorním řešením může být alespoň přestat zobrazovat dané údaje uživatelům ve front-endu. Nově zaváděné systémy by však s ohledem na princip privacy by design již podporovat mazání vždy.

Nejprve je nutné vymazat ty dokumenty (údaje), které se nearchivují ze zákona a které by zaměstnavatel pro případný pracovněprávní spor se zaměstnancem nepotřeboval. Jedná se např. o kopie osobních dokladů, profesní životopis, různá osvědčení či jiné obdobné dokumenty (přesný výčet neexistuje). Uchovávat lze pouze nezbytně nutné dokumenty pro plnění těchto účelů zpracování osobních údajů.

### Evidence listin a dokumentace zaměstnavatelem

Zaměstnavatel by měl ideálně posoudit existenci jakýchkoliv navazujících účelů pro zpracování pro každý jednotlivý dokument zvlášť. Některé dokumenty by tedy měly být zlikvidovány ihned po ukončení pracovněprávního vztahu, jiné až po uplynutí zákonné archivační doby či oprávněného zájmu zaměstnavatele. V praxi však nepochybně bude docházet k určité paušalizaci a hledání kompromisů, v jaké míře je přiměřené dokumenty v souladu s tímto požadavkem rozlišovat a postupně vyřazovat ze zpracování. Vhodným řešením může být nastavení archivační doby na procesní a systémové úrovni již od počátku zpracování a členit například v tomto smyslu osobní složky zaměstnanců.

Zaměstnavatel je povinen pro plnění archivačních dob vyplývajících ze zákona určité dokumenty archivovat po pevně stanovenou dobu. Dalším navazujícím účelem může být uchování určitých dokumentů pro účely obhajoby právních nároků pro případ budoucího sporu se zaměstnancem, kdy má zaměstnavatel oprávněný zájem uchovat nezbytné informace a dokumenty po dobu trvání promlčecích lhůt, ve kterých by ho mohl bývalý zaměstnanec zažalovat u soudu například na náhradu újmy. S ohledem na tříletou promlčecí lhůtu se obvykle doporučuje uchování pracovněprávních dokumentů za tímto účelem po dobu až 4 let (s ohledem na fakt, že žaloba může být žalovanému zaměstnavateli doručena i několik měsíců po uplynutí promlčecí lhůty).

Archivační doby jsou v případě pracovněprávních dokumentů upraveny v několika právních předpisech. Podle zákona o účetnictví je stanovena doba 5 let pro uchování účetních záznamů, počínající koncem účetního období, kterého se týkají.

Konkrétní lhůty pro archivaci jednotlivých dokumentů mohou být následující:

* **stejnopisy evidenčních listů důchodového pojištění:** po dobu 3 kalendářních roků po roce, kterého se týkají,
* **záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti:** po dobu 6 kalendářních roků následujících po měsíci, kterého se záznam týká; vždy však po dobu 3 kalendářních roků následujících po měsíci, v němž bylo dlužné pojistné za tento měsíc zaplaceno,
* **záznamy o údajích potřebných pro účely důchodového pojištění (konkrétně identifikační údaje, vznik a skončení pracovního poměru, vyměřovací základ pojištěnce, dobu dočasné pracovní neschopnosti, dobu pracovního volna bez náhrady příjmu, záznam o pobírání starobního důchodu a dobu vojenské služby)**: 10 let, po roce, kterého se týkají,
* **mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění**: 30 let, po roce, kterého se týkají (pokud jde o poživatele starobního nebo invalidního důchodu 10 let),
* **doklady z oblasti nemocenského pojištění:** 10 let, po roce, kterého se týkají. Mezi tyto záznamy patří zejména identifikační údaje zaměstnance, výše sjednaného započitatelného příjmu, výši započitatelného příjmu za jednotlivá mzdová období, dobu dočasné pracovní neschopnosti, mateřské a rodičovské dovolené, neomluvené pracovní dny, záznam o pobírání důchodu, výši vyměřovacího základu pro pojistné či název zdravotní pojišťovny,
* **doklady daňové:** prohlášení k dani, žádost o roční zúčtování, vyúčtování – 10 kalendářních roků následujících po roce, kterého se týkají,
* **písemnosti týkající se prováděných srážek ze mzdy** – po dobu 30 roků následujících po roce, kterého se týkají.

Co se pracovnělékařských posudků týče, doba není výslovně stanovena. Obecně je možné vycházet ze zákona o účetnictví, který stanoví lhůtu 5–10 let pro uchování účetních záznamů. V případě zaměstnavatele se mezi tyto účetní záznamy řadí například mzdové listy, mzdové a platové výměry, daňové doklady a další dokumentace. V rámci GDPR bude potřeba vždy stanovit účel, pro který se příslušné dokumenty archivují.

Poté, co je pracovněprávní vztah se zaměstnancem ukončen, bude účelem uchování posudků k pracovnělékařským prohlídkám případný nárok zaměstnance na náhradu škody (při úrazu nebo nemoci z povolání), který může uplatnit po dobu deseti let ode dne, kdy škoda nebo újma vznikla. V případě těchto dokumentů lze doporučit lhůtu pro archivaci pracovnělékařských prohlídek minimálně dobu 10 let od ukončení pracovního poměru, právě z důvodu případného uplatnění nároku na náhradu škody. Z tohoto důvodu je vhodné uchovat všechny posudky, které byly provedeny.

### Práva zaměstnanců

Jednou z oblastí, kterou GDPR upřesňuje poměrně zásadním způsobem, je úprava práv subjektů údajů, kterými jsou z povahy věci i zaměstnanci či uchazeči o zaměstnání, a výjimek z těchto práv. Pojednání o těchto změnách uvádíme v rámci rozboru jednotlivých práv subjektů níže.

Konkrétně se jedná o následující práva:

a) právo na informace o zpracování (čl. 13 a 14 nařízení GDPR);

b) právo na přístup k osobním údajům (čl. 15 nařízení GDPR);

c) právo na opravu (čl. 16 nařízení GDPR);

d) právo na výmaz (čl. 17 nařízení GDPR);

e) právo na omezení zpracování (čl. 18 nařízení GDPR);

f) právo na přenositelnost údajů (čl. 20 nařízení GDPR);

g) právo vznést námitku (čl. 21 nařízení GDPR); a

h) právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování (čl. 22 nařízení GDPR).

Aby zaměstnavatel mohl adekvátně a za řádného splnění všech zákonných povinností reagovat na žádosti subjektů, je nutné, aby měl přehled zpracování včetně jejich titulů a funkční komunikační kanály pro jejich vyřizování. Při nesplnění tohoto předpokladu bude prakticky nemožné vyhovět právům subjektu v plném rozsahu (např. bez evidence, k jakým zpracováním, na základě jakých účelů a v jakém rozsahu dochází, nebude možno vyhovět žádosti o přístup). Z těchto důvodů je nutné vést evidenci o prováděných zpracování a předem stanovit, jak řešit vznesené nároky týkající se práv subjektu údajů.

Čl. 12 nařízení GDPR stanoví obecné podmínky pro uplatňování těchto práv, když definuje způsob vyřizování žádostí subjektů údajů, lhůtu pro jejich vyřízení, požadavky na identifikaci subjektu údajů apod. Podstatnou je též skutečnost, že sdělení informací či jiné úkony dle čl. 13-22 subjektu údajů se na rozdíl od § 12 odst. 3 ZOOÚ, dle kterého byl správce oprávněn požadovat přiměřenou náhradu, nově činí již bezplatně, pokud se nejedná o zjevně nedůvodné, nepřiměřené nebo opakující se požadavky subjektu – v takových případech může správce uložit přiměřený poplatek zohledňující administrativní náklady nebo odmítnout žádosti vyhovět.

Čl. 12 nařízení GDPR stanovuje požadavky na formu komunikace se subjektem údajů. Veškerá sdělení subjektům údajů musí být činěna stručným, transparentním, srozumitelným a snadno přístupným způsobem a musí být použito jasných a jednoduchých jazykových prostředků, ideálně za použití metody otázky a odpovědi, včetně doplňujících vizualizací a grafik, z nichž budou zjevné postupy a dopady zpracování osobních údajů. Správce údajů musí subjektům výkon práv usnadňovat. To znamená, že by měl definovat způsoby, jakými mohou subjekty práva uplatnit, a neměl by při uplatňování subjektům údajů klást překážky. Pokud subjekt údajů podá žádost v elektronické formě, musí mu správce odpovědět a sdělit potřebné informace také v elektronické formě, je-li to možné. Pokud subjekt údajů požádá o jiný způsob, správce mu v elektronické podobě informace zasílat nemusí. Nařízení GDPR stanoví také možnost poskytnout informace ústně, pokud si to subjekt údajů vyžádá, a to za předpokladu, že je prokázána identita subjektu údajů, aby bylo zabráněno neoprávněnému přístupu k osobním údajům a zneužívání těchto práv ze strany třetích osob.

V případě uplatňování práv subjektů uvedených v odst. 2 písm. b) až h) předešlého článku poskytuje správce subjektu údajů, je-li o to požádán, informaci o tom, jaká přijal opatření, a to bez zbytečného odkladu, maximálně však do jednoho měsíce od podání žádosti. V případě potřeby s ohledem na složitost a počet žádostí může být tato lhůta o dva měsíce prodloužena, o čemž však musí být subjekt údajů v původní lhůtě vyrozuměn. Dle názoru WP 29 však může být důvodem pro prodloužení lhůty pouze počet žádostí obdržených od jednoho žadatele. Nebude tedy možné lhůtu prodloužit s odůvodněním, že správce aktuálně vyřizuje velké množství žádostí různých subjektů, popř. s poukazem na kapacitní omezení správce. Prodloužení lhůty správcem o dva měsíce je však možné pouze v případech, kdy se chystá žádosti subjektu vyhovět.

Uvedená lhůta doběhne na konci číslem shodně označeného dne následujícího měsíce – pro vyřízení žádosti doručené 28. 2. 2019 uplyne lhůta pro vyřízení 28. 3. 2019. Pokud by byla žádost doručena v den v měsíci, který v následujícím měsíci není, připadne konec lhůty na poslední den měsíce – pro vyřízení žádosti doručené 31. 1. 2019 uplyne lhůta pro vyřízení 28. 2. 2019.

V případě, že správce žádosti nevyhoví, musí do jednoho měsíce subjekt údajů informovat o důvodech odmítnutí a poučit o možnosti podat stížnost u ÚOOÚ. Označení žádosti subjektu údajů za nedůvodnou má však správce dle stanoviska WP 29 využívat je v minimální míře.

Co se týče práva subjektu na informace o zpracování, toto je zakotveno v čl. 13 a 14 nařízení GDPR. Čl. 13 nařízení GDPR řeší poskytování informací v případě, kdy jsou osobní údaje získány od subjektu údajů, čl. 14 nařízení GDPR pak řeší poskytování informací v případě, kdy osobní údaje od subjektu údajů získány nejsou.

Rozsah informací, které lze subjektu poskytnout, je určen odst. 1 čl. 13 a 14 nařízení GDPR. Dále je definován též rozsah informací, které je nezbytné subjektu poskytnout spolu s informacemi, o které subjekt žádá, a to v odst. 2 čl. 13 a 14 nařízení GDPR.

Pokud byly osobní údaje získány od subjektu údajů (čl. 13 GDPR):

a) totožnost a kontaktní údaje správce a jeho případného zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na titulu oprávněného zájmu;

e) případné příjemce nebo kategorie příjemců osobních údajů; a

f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně.

Rozsah informací, jejichž poskytnutí subjektům je nutné pro spravedlivé a transparentní zpracování, je:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

d) existence práva podat stížnost u dozorového úřadu;

e) zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů; a

f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Informace dle čl. 13 nařízení GDPR, tedy v případě, kdy jsou osobní údaje získány od subjektu údajů, není nutno poskytovat v případech, pokud již subjekt údajů uvedené informace má, a to v rozsahu, ve kterém tyto informace již má (srov. čl. 13 odst. 4). Za případy, kdy subjekt údajů uvedené informace má, však nelze považovat případy, kdy je získávání či zpřístupnění těchto údajů pouze stanoveno právem Unie či členského státu (srov. níže).

Současně na správce dopadne povinnost formulovat tyto informace, totožně jako informace dle článku 14 GDPR (viz níže), prostým jazykem a natolik jasně, aby bylo informování srozumitelné, zejména pro případy, kdy je subjektem údajů dítě.

V souvislosti s problematikou informování je nutné uvést, že subjekt údajů musí být dle GDPR výslovně upozorněn na své právo podat námitku proti zpracování osobních údajů z důvodu oprávněného či veřejného zájmu (viz čl. 31 níže).

Co se týče informací poskytovaných dle čl. 14 nařízení GDPR, tedy v případě, kdy osobní údaje získány od subjektu údajů nejsou, tyto informace není nutno poskytovat v případech, pokud již subjekt údajů uvedené informace má, pokud jejich poskytnutí není možné nebo by vyžadovalo nepřiměřené úsilí, pokud je získávání či zpřístupnění těchto údajů stanoveno právem Unie či členského státu nebo pokud se jedná o osobní údaje, které musí zůstat důvěrné (srov. čl. 14 odst. 5 nařízení GDPR).

Oproti informacím poskytovaným subjektu údajů v případě, že byly údaje získány od něj samotného, musí správce poskytnout informaci o kategorii dotčených osobních údajů a informaci o zdroji, ze kterého osobní údaje pocházejí.

Dalším z práv subjektů údajů je právo na přístup k osobním údajům. Na základě žádostí subjektů bude nutno vydat potvrzení, že osobní údaje týkající se subjektu údajů jsou či nejsou zpracovávány, resp. v případě kdy zpracovávány jsou, poskytnout subjektu kopii těchto údajů a související informace. Tato kopie je, oproti dřívější úpravě v ZOOÚ, poskytována bezplatně, a to za předpokladu, že nejde o šikanózní či jinak nepřiměřené a neodůvodněné žádosti. Za každé další kopie, které jsou subjektem vyžádány (tj. např. pokud by chtěl subjekt údaje vydat ve 3 vyhotoveních), již správce může účtovat administrativní poplatek, který zohledňuje vynaložené náklady na tvorbu a poskytnutí této kopie. Zpravidla se tedy bude jednat o náklady na práci zaměstnance, náklady na nosič informací a případné náklady na zaslání této kopie.

Související informace jsou vymezeny v čl. 15 nařízení GDPR, konkrétně je nutno sdělit následující:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) přehled příjemců nebo kategorií příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovanou dobu, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

e) existenci práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů; a

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Na žádosti subjektu odpovídá správce způsobem komunikace zvoleným subjektem. Jestliže subjekt toto blíže neurčil, odpovídá správce na elektronické žádosti elektronicky, jinak dle vlastní volby. Jestliže odpovídá elektronicky, využívá správce běžně využívaný formát, tedy zpravidla dokumenty typu .xlsx či .docx. Správce není povinen převádět informace do formátu, který si subjektu údajů zvolí, jestliže tento formát nesplňuje podmínky obvyklého formátu. Oproti právu na přenositelnost navíc nemusí být údaje poskytovány ve strukturovaném a strojově čitelném formátu.

Co se týče práva na opravu osobních údajů, dle tohoto práva má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají, popř. neúplné osobní údaje doplnil. Toto právo bude pravidelně realizováno v návaznosti na výše uvedená práva na informace o zpracování a na přístup k osobním údajům.

Povinnost opravit nepřesné osobní údaje má přitom správce i v případě, když se o nepřesnostech těchto údajů dozví z vlastní činnosti (není však povinen proaktivně nepřesnosti vyhledávat).

V případě, že je podána žádost o opravu, správce zablokuje zpracovávání předmětných údajů do rozhodnutí, zda tyto údaje opraví, či nikoliv. V případě nesouhlasu s rozhodnutím správce má subjekt následně možnost si stěžovat u dozorového orgánu, nemůže však zabránit negativnímu rozhodnutí správce. Správce tedy není povinen vyhovět žádosti na opravu osobních údajů, jestliže nalezne nesrovnalosti v žádosti subjektu nebo v údajích získaných jinak než od subjektu.

V případech, kdy správce údaje zveřejnil a je povinen je opravit, musí přijmout přiměřené kroky, aby informoval další správce, kteří tyto údaje zpracovávají, o nutnosti opravy těchto údajů.

Co se dále týče práva na výmaz, označovaného též jako „právo být zapomenut“, toto vychází z úpravy uvedené ZOOÚ a značně ji v návaznosti na rozhodovací praxi Soudního dvora Evropské unie rozšiřuje. Postup v případě žádosti o výmaz je analogický jako v případě žádosti o opravu (vizte výše), i zde musí správce nejprve zablokovat zpracovávání a následně činí rozhodnutí, zda skutečnosti uvedené v žádosti odpovídají realitě. Jestliže správce uzná důvodnost žádosti, údaje vymaže. V případě, že důvodnost neuzná, zasílá subjektu vyjádření, doplněné o doložení této nedůvodnosti a zároveň informace o možnosti subjektu obrátit se na dozorový úřad, respektive žádat o soudní ochranu dle čl. 77 a 79 nařízení GDPR. V případech, kdy správce údaje zveřejnil a je povinen je vymazat, musí i zde přijmout přiměřené kroky, aby informoval další správce, kteří tyto údaje zpracovávají, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

Právo na výmaz má však i své limity a neuplatní se například v případě, pokud je zpracování nezbytné pro splnění právní povinnosti dle práva Unie nebo členského státu či pro určení, výrok nebo obhajobu právních nároků apod. (srov. čl. 17 odst. 3 nařízení GDPR). Lze tedy shrnout, že v případě uplatnění tohoto práva bude předcházet posouzení rozsahu, v jakém bude možné žádosti vyhovět. Nelze vymazat informace, které zvláštní právní předpis ukládá uchovat.

V případě zpracování na základě souhlasu, který je svobodným a jednoznačným projevem vůle, bude právo na výmaz aktuální v zásadě vždy, kdy o něj bude subjektem zažádáno. Tuto žádost může správce aktivně vyhodnocovat a posuzovat její přiměřenost a oprávněnost.

Dalším z práv subjektu je právo na omezení zpracování, které se uplatní např. v případech, kdy subjekt popírá přesnost údajů, a to na dobu potřebnou k ověření přesnosti těchto údajů, kdy je zpracování protiprávní a subjekt odmítá výmaz, kdy správce již osobní údaje nepotřebuje, ale požaduje je subjekt pro účely vlastních právních nároků, a konečně též v případě, kdy subjekt vznesl námitku proti zpracování (vizte níže), dokud nebude řádně vypořádána.

Nařízení GDPR toto právo omezení zpracování, respektive blokace, omezuje. Subjektu již dále není nabízena obecná úprava, ale taxativní výčet dle čl. 18 odst. 1 nařízení GDPR. Subjekt údajů má právo na to, aby správce omezil zpracování, když:

a) subjekt údajů popírá přesnost údajů;

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá omezení jejich použití;

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků.

Touto úpravou se snaží zákonodárce docílit toho, aby předmětné údaje, které mají posloužit při obhajobě právních nároků (nejen) subjektu, správce nemohl smazat. Z povahy a znění nařízení GDPR, které zakotvuje i vymazání osobních údajů jako jejich zpracování, by se takto správce dopustil neoprávněného zpracování a hrozila by mu pokuta, eventuálně i další postih dle vnitrostátních předpisů týkajících se např. maření vyšetřování;

d) subjekt údajů vznesl námitku proti zpracování dle čl. 21.

V takových případech bude zpracování těchto údajů omezeno od doby, kdy dojde žádost správci, který bez zbytečného odkladu posoudí její oprávněnost a vzápětí rozhodne o blokaci, a to do doby, dokud správce žádosti/námitce buď vyhoví, nebo nerozhodne o tom, že údaje uvedené v žádosti/námitce jsou nesprávné a nedůvodné, a zpracovávané údaje ponechá v původní podobě.

Dalším právem je právo na přenositelnost údajů, na základě kterého má subjekt právo získat údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.

Zcela zásadní je však skutečnost, že toto právo se uplatní pouze v případě, kdy je zpracování založeno na souhlasu nebo smlouvě a provádí se automatizovaně. Vždy je tedy nezbytné mít přehled o právním titulu, na základě kterého se děje předmětné zpracování a ke kterému subjekt vztahuje svou žádost.

Nařízení GDPR dále upravuje právo vznést námitku, které umožňuje subjektu údajů podat proti zpracování námitku v případě, kdy je toto zpracování prováděno na základě veřejného zájmu či oprávněného zájmu správce. V případě podání takové námitky není správce oprávněn osobní údaje dále zpracovávat, pokud neprokáže oprávněné důvody pro zpracování, které převažují nad zájmy subjektu údajů. Proti zpracování z titulů oprávněného nebo veřejného zájmu může tedy dle čl. 21 nařízení GDPR subjekt údajů kdykoliv vznést námitku.

Od okamžiku podání námitky je správce povinen omezit zpracování, a to až do okamžiku řádného vypořádání námitky. I na toto právo se vztáhne generální ustanovení čl. 12 nařízení GDPR, dle kterého má správce možnost námitku odmítnout, pokud se jedná o žádost zjevně nepřiměřenou, doplněné o obecnou nutnost identifikace žadatele.

Posledním z práv subjektu údajů je právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování. Automatickým individuálním rozhodováním se přitom rozumí takové zpracování, které je prováděno bez zásahu lidského prvku a které má právní účinky pro subjekt údajů nebo se ho obdobným způsobem významně dotýká. Profilování je pak definováno jako 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.

# Praktická část

### Dopady v případě záznamu v rejstříku trestů

V případě, že bude mít uchazeč záznam v rejstříku trestů, nemůže být jakýkoli záznam automaticky důvodem jeho odmítnutí.

Uchazeč o zaměstnání může předložení výpisu z trestního rejstříku odmítnout s odůvodněním, že zaměstnavatel nemá právo se s takovou informací seznamovat, případně se zeptat na důvod zaměstnavatele pro požadavek na tuto informaci. V praxi se bohužel takové odmítnutí neoprávněně zaměstnavatelem požadované informace může stát skrytým důvodem pro nepřijetí uchazeče.

Praktické možnosti obrany uchazeče o zaměstnání proti tomuto jednání jsou v podstatě trojí a ani jednu z nich není možno z pohledu možnosti nápravy nevyhovující situace hodnotit jako optimální.

První z těchto variant je podání stížnosti na příslušný inspektorát práce, který vykonává dohled nad dodržováním pracovněprávních předpisů zaměstnavatele. Vyžadování doložení výpisu z rejstříku při přijímacím řízení může být v konkrétních případech porušením zákoníku práce, popř. i zákona o zaměstnanosti, zejména pokud je výpis vyžadován jako informace, která bezprostředně nesouvisí s uzavřením pracovního poměru.

Z toho vyplývá, že se v tomto řízení nemůže domáhat uspokojení svých individuálních nároků, neboť pokud úřad práce po provedeném šetření shledá u zaměstnavatele pochybení, vyzve ho k odstranění zjištěných nedostatků a může mu případně i uložit finanční sankci.

Druhou možností je bránit se podáním podnětu na Úřad ochrany osobních údajů. V rámci informační politiky Úřadu tento poskytuje konzultační služby subjektům údajů v rozsahu jejich práv podle nařízení GDPR. Právě toto klíčové ustanovení, uvedené ve vyjádření Úřadu ze 4. června 2018, stanoví Úřadu povinnost takový podnět přijmout, prozkoumat a buď zahájit správní řízení, nebo zvolenou cestou problematiku konzultovat.

Dále se uchazeč může bránit v občanskoprávním řízení. Občanským zákoníkem je chráněna důstojnost člověka, která by v tomto případě mohla být porušena např. "dehonestující" inzercí pracovního místa.

K odstranění důsledků by v tomto případě byla řešením restituční (odstraňující) žaloba. Jedná se o soudní žalobu na ochranu osobnosti z důvodu rozdílného zacházení v přístupu k zaměstnání. Soudní spory však také trvají dlouho a žalobce je tak po značnou dobu vystaven nejistotě, jak soudní spor dopadne.

### Právní základ pro zpracování údaje o trestní činnosti

Pro zpracování údajů o trestné činnosti nestačí mít pouze právní základ podle čl. 6 odst. 1 GDPR. Pro zpracování údajů o trestné činnosti je navíc potřeba splnit podmínky dle čl. 10.

Ve všech případech, kdy je jako vhodný právní základ pro tento údaj zvláštní kategorie identifikován jiný právní základ než výslovný souhlas, je třeba z dokumentace vypustit nepotřebné souhlasy se zpracováním. O těchto právních základech pak je třeba zaměstnance vhodným způsobem informovat. Lze doplnit, že dle uvedené teoretické části bude souhlas jen zřídkakdy vhodným titulem pro zpracování údajů v pracovněprávní agendě.

V případě, že byl jako právní základ identifikován výslovný souhlas, lze pro zaměstnavatele obecně doporučit úpravy současných znění souhlasů tzn.:

* konkretizovat, aby byly souhlasy uděleny pro jasně vymezený a srozumitelný účel;
* oddělit souhlas od jiných prohlášení pro zajištění principu transparentnosti;
* zajistit udělení jednoznačnou kladnou akcí (např. zaškrtnutím pole nebo uvedením konkrétního údaje do označeného pole),
* doplnit o informaci, že souhlas lze odvolat, ale zpracování do okamžiku udělení tím nebude dotčeno, a
* doplnit další nezbytné informace o zpracování.

Ve všech případech, kdy je jako vhodný právní základ identifikován výslovný souhlas, který však nebyl udělen platně a v souladu s novou legislativou, by měl být opět získán platný souhlas, který této legislativě bude dále odpovídat. Souhlas by měl být získán od stávajících subjektů údajů nebo zpracování omezit na účely, které je možné realizovat bez souhlasu.

Ve všech případech, kdy byl jako vhodný právní základ pro zvláštní případy zpracování identifikován jiný zvláštní právní základ než výslovný souhlas, lze zaměstnavateli doporučit vypustit z dokumentace nepotřebné výslovné souhlasy se zpracováním.

### Účely zpracování s přihlédnutím k údajům o trestněprávní činnosti

V případě, že bylo auditem u zaměstnavatele zjištěno, že účely zpracování nejsou vymezeny dostatečným způsobem, je třeba veškerým identifikovaným procesům, jejichž prostřednictvím dochází ke zpracování osobních údajů, přiřadit jim účely zpracování. Účely by bylo vhodné vést centrálně na úrovni celého zaměstnavatele. V případě zaměstnavatele, který je součástí větší skupiny obsahujícího přeshraniční podniky, je třeba provést revizi compliance jednotlivých účelů zpracování s národním právem jednotlivých podniků.

V rámci interní evidence zaměstnavatele je vhodné ke každému účelu přiřadit kategorie subjektů údajů, jejichž osobní údaje jsou v rámci účelu zpracovávány, a také právní základ (titul) jejich zpracování. Vazbu mezi účely, kategoriemi subjektů údajů a právními základy je současně třeba promítnout do informací poskytovaných v rámci plnění informační povinnosti.

U tzv. dalších zpracováních (např. zpracování zveřejněných osobních údajů z veřejných rejstříků) má být provedeno posouzení slučitelnosti dle čl. 6 odst. 4 GDPR. V rámci tohoto posouzení by mělo být posouzeno, jestli je slučitelný účel, pro který zaměstnavatel údaje zpracovávat, s účelem, pro který byly osobní údaje původně shromážděny a zveřejněny.

### Informování o zpracování údajů vč. kategorie dle čl. 10 Nařízení GDPR

Zaměstnavatel je povinen zajistit informování všech subjektů údajů o aspektech zpracování osobních údajů dle čl. 13 a 14 Nařízení GDPR. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, je třeba mu poskytnout informace o zpracování v okamžiku získání údajů.

Jestliže osobní údaje nebyly získány od subjektu údajů, je třeba tyto informace poskytnout:

* 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 zaměstnavatel v úmyslu zpřístupnit jinému příjemci.

Best-practise při informování zaměstnance je využití více vrstev plnění informační povinnosti. Informování pak může být rozděleno na mandatorní údaje, poskytované v rámci principu transparentnosti zaměstnanci ihned v srozumitelné a lehce pochopitelné formě, a zbývající informace přesunout do vnitřní směrnice či dokumentu, který bude obsahovat veškeré údaje požadované Nařízením GDPR.

Ve všech případech, kde je subjektu údajů společně se základní informační vrstvou poskytována další dokumentace, by měl zaměstnavatel zajistit, aby detailnější informace byly obsaženy v další dokumentaci poskytované společně se základním dokumentem. Ve výjimečných případech, kde je prostor pro informování subjektu údajů limitovaný (např. v rámci upozornění na použití kamerového systému), doporučujeme odkazovat na další dokumentaci v elektronické podobě (např. webové stránky) a současně uvést, jak může subjekt údajů tyto informace obdržet v listinné podobě (např. na vyžádání na pobočce).

Informace, které je nezbytné subjektu údajů poskytnout, závisí na okolnostech konkrétního zpracování. V případě, že dochází ke zpracování na základě oprávněného zájmu, subjekt údajů by měl být navíc poučen o právu vznést námitku proti zpracování dle čl. 21 Nařízení GDPR. Další významné skutečnosti mohou vyplývat ze specifik konkrétního zpracování.

V rámci základního dokumentu nebo do další dokumentace doporučujeme uvést:

* právní základ pro zpracování pro jednotlivé účely,
* u účelů, pro které jsou osobní údaje zpracovány na základě oprávněného zájmu, tento oprávněný zájem,
* kategorie příjemců, kterým zaměstnavatel osobní údaje předává (pokud je příjemcem skupina subjektů, např. skupina společností, je v rámci listinné dokumentace je možné jako příjemce označit skupinu subjektů a odkázat na aktuální seznam jejích členů na webových stránkách; v případě změny v okruhu členů, která by překračovala legitimní očekávání subjektu údajů, je třeba subjekt o takové změně informovat),
* dobu, po kterou budou osobní údaje zpracovány,
* poučení o právu na přístup dle čl. 15, právu na opravu dle čl. 16, právu na výmaz dle čl. 17, právu na omezení zpracování dle čl. 18, právu na přenositelnost v rámci čl. 20 a právu vznést námitku proti zpracování dle čl. 21 GDPR, a to s konkrétní specifikací, ve vztahu ke kterým účelům zpracování, resp. údajům se tato práva vztahují a jak je možné je uplatnit,
* pokud je zpracování založeno na souhlasu, informaci o tom, že souhlas lze kdykoliv odvolat a že odvoláním není dotčena zákonnost zpracování do okamžiku odvolání,
* informaci o tom, jestli je poskytnutí osobních údajů zákonným nebo smluvním požadavkem a jaké následky má neposkytnutí údajů;
* skutečnost, zde dochází v rámci tohoto účelu k automatizovanému rozhodování dle čl. 22 odst. 1 a 4 GDPR, a přinejmenším smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového rozhodování pro subjekt údajů, a
* poučení o možnosti podat stížnost u ÚOOÚ.

V případě, že jsou tyto informace poskytovány v rámci další dokumentace, doporučujeme, aby dokumentace byla specifická dle konkrétních aktivit zpracování, které se v daném případě subjektu údajů týkají. V případě, že je v rámci jednoho dokumentu poskytována informace pro více subjektů, popř. zahrnuje informace o více aktivitách zpracování, které se nemusí konkrétního subjektu údajů týkat, doporučujeme, aby byly odlišeny informace o zpracování údajů odlišných subjektů údajů a v rámci odlišných aktivit. V případě, že je takto strukturovaná dokumentace poskytována v elektronické podobě, doporučujeme do ní začlenit interaktivní navigaci umožňující snadnější orientaci jednotlivých subjektů údajů.

Informace o zpracování osobních údajů prostřednictvím docházkového systému a CCTV lze uvést do jednotného dokumentu, kterým budou zaměstnanci informování. Tento dokument pak lze, spolu s piktogramem CCTV, ponechat na recepci či jiném místě, kde by zaměstnanci důvodně očekávali jeho přítomnost.

Ve vztahu k subjektům údajů, se kterými má zaměstnavatel přímý vztah (tzn. nejde o agenturní zaměstnávání), doporučujeme dodatečné informování těchto subjektů údajů o zpracování v rozsahu, ve kterém výše uvedené informace o zpracování ještě nemají. Informování doporučujeme provést např. v rámci pravidelné komunikace se subjektem údajů v rámci udržování obchodních a pracovněprávních vztahů.

V návaznosti na katalogizaci osobních údajů doporučujeme pro každý účel ověřit, zda jsou veškeré používané osobní údaje nezbytné pro jeho dosažení. U údajů, jejichž zpracování představuje zvýšené riziko pro subjekt údajů (zvláštní kategorie údajů) doporučujeme nezbytnost zpracování pro každý účel zdůvodnění a toto zdůvodnění zdokumentovat.

Pokud bude v rámci posouzení nezbytnosti zpracování zjištěno, že pro nějaký účel jsou zpracovávané osobní údaje, které nejsou pro tento účel nezbytné, doporučujeme v rámci tohoto účelu tyto přebytečné údaje přestat zpracovávat. Pro daný účel doporučujeme zavést vhodná technická a organizační opatření tak, aby tyto osobní údaje nebyly pro řešený účel zpracovávány, popř. zpracování osobních údajů ukončit, pokud nejsou potřené pro žádný účel (viz dále). Stejně doporučujeme postupovat, pokud údaje pro určitý účel přestanou být nezbytné v průběhu zpracování.

V případě, že po omezení zpracování na nezbytné údaje vyjde najevo, že některé osobní údaje nejsou potřeba pro žádný účel, doporučujeme jejich zpracování ukončit a tyto osobní údaje zlikvidovat, tedy vymazat nebo anonymizovat. V některých případech bude nutné řešit, zda jde opravdu o anonymizaci (zda subjekty již nejsou identifikovatelné). V těchto případech je nutné zvážit míru rizika, kterou chce zaměstnavatel nést. Na základě tohoto předpokladu je možné určit rozsah ponechaných údajů a související technická a organizační opatření.

Společně s posouzením dle předešlých odstavců je třeba zajistit, aby byly údaje zpracovávány pouze po nezbytnou dobu, kterou vyžaduje účel zpracování. Prostřednictvím interních opatření je třeba dodržování takové doby nastavit, a u údajů které jsou již nyní zpracovávány déle než nezbytně dlouho jejich zpracování ukončit.

Doporučujeme zrevidovat a upravit stávající dokumentaci (směrnice, pracovní postupy, metodické pokyny) a dotvořit chybějící dokumentace vymezující náplň práce a přístupová oprávnění tak, aby byl přístup k osobním údajům omezený pouze pro daný účel.

Mělo by být explicitně vyjmenované neoprávněné nakládání s osobními údaji zaměstnanců, které nelze z povahy věci zabezpečit jiným technickým či organizačním řešením; tj. zákaz sdílení osobních údajů mimo osobu zaměstnavatele pro osobní účely (např. prostřednictvím osobních emailů), vytváření fotek obrazovek - "print screenů", export dat pro soukromé účely, tvorba "vlastních" souborů (např. Excelů) se záznamy o zaměstnancích, které nesouvisí s plněním smlouvy, atd.

Lze doporučit nastavit proces, který bude v pravidelných intervalech ověřovat zabezpečení údajů, a to ve spolupráci s IT oddělením, které bude ve většině případů gestorem zabezpečení.

V rámci vztahů s dodavateli, kteří jsou v postavení zpracovatelů osobních údajů, je nezbytné smluvně uzavřít zpracovatelské doložky dle čl. 28 odst. 3 GDPR do v současnosti uzavřených smluv, resp. ověřit, zdali sjednané doložky požadavkům GDPR odpovídají. Zaměstnavatel by měl navíc dle čl. 28 odst. 1 GDPR využívat pouze takové dodavatele (bez ohledu na to, zda jde o dodavatele IT servisu, mzdového oddělení, externí daňové kanceláře nebo dodavatele zboží), kteří mu poskytnou dostatečné záruky zavedení vhodných technických a organizačních tak, aby dané zpracování splňovalo požadavky podle GDPR a aby byla zajištěna ochrana práv subjektů údajů.

V rámci nastavení vztahů s dalšími správci, kterým jsou v rámci některých aktivit předávány osobní údaje, by mělo také dojít k dílčím úpravám.

Z informací poskytnutých prostřednictvím dotazníků je patrné, že dochází k předávání údajů subjektů společnostem ve skupině, byť jsou označovány za zpracovatele. V kontextu popisu aktivit se ovšem lze domnívat, že společnosti ve skupině budou vůči některým zpracováním v pozici správce.

Předání osobních údajů je zvláštním druhem zpracování, pro který potřebuje zaměstnavatel právní základ. Pro správný způsob určení a úpravy právního základu viz výše. V souvislosti s tím je třeba stanovit účely a tituly zpracování. Doporučujeme zároveň jednoznačně odlišit, ve kterých případech půjde o předávání zpracovateli a kdy správci, příp. o společné správce.

Na základě výše uvedeného je nutné předávání osobních údajů zakotvit smluvně. Současně by mělo být ověřeno, jakým způsobem je zajištěno zabezpečení údajů u smluvních společností.

Zaměstnavatel by měl provést v souladu se zásadou minimalizace údajů posouzení, jestli je pro potřeby dané aktivity nezbytné předávat dalším správcům osobní údaje v rozsahu, v jakém je předává. Pokud dojde k závěru, že některé osobní údaje není nezbytné předávat, měla by předávání těchto osobních údajů zastavit.

Zaměstnavatel by měl zároveň nastavit pravidelný proces prověřování zpracovatelů, jestli stále poskytují dostatečné záruky souladu s GDPR.

Se zpracovateli, kteří poskytnou zaměstnavateli dostatečné záruky souladu s GDPR, může zaměstnavatel pokračovat ve spolupráci, avšak doporučujeme upravit zpracovatelské doložky ve smlouvách, které s nimi má zaměstnavatel uzavřené.

Ve zpracovatelské doložce by měl být stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie osobních údajů a dále by měl zaměstnavatel zavázat zpracovatele, aby:

* zpracovávali osobní údaje pouze na základě doložených pokynů,
* zajistili mlčenlivost osob, které budou k osobním údajům oprávněně přistupovat (např. ve formě NDA doložek),
* přijali všechna organizační a bezpečnostní opatření k zajištění důvěrnosti a integrity zpracovaných osobních údajů v souladu s čl. 32 GDPR,
* dodržovali zákaz zapojení dalších zpracovatelů bez souhlasu zaměstnavatele (anebo pokud zaměstnavatel dá obecný souhlas k zapojení dalších zpracovatelů, aby byla o tomto zapojení dopředu informována),
* byli zaměstnavateli nápomocni při vyřizování práv subjektů údajů podle GDPR (tedy aby zajistil potřebnou technickou i organizační součinnost),
* byli zaměstnavateli nápomocni při zajišťování souladu s povinnostmi oznamování a ohlašování bezpečnostních incidentů (zde doporučujeme jasně vymezit povinnosti zpracovatele ohledně hlášení a vyšetřování incidentů), posouzení vlivu na ochranu osobních údajů (např. doložením potřebné dokumentace svého zabezpečení) a předchozí konzultace dle GDPR,
* v souladu s rozhodnutím zaměstnavatele všechny osobní údaje vymazali nebo je vrátili zaměstnavateli po ukončení poskytování služeb spojených se zpracováním osobních údajů,
* poskytli zaměstnavateli veškeré informace potřebné k doložení souladu s GDPR a plnění povinností dle zpracovatelské smlouvy a umožnili mu provádět audity, včetně inspekcí, prováděné jím samotným nebo auditorem, kterého zaměstnavatel pověří.

# Závěr

Tato studie ve své praktické části popisuje veškeré změny, kterých by se zaměstnavatelé s agendou zpracovávání údajů o trestněprávní činnosti měli držet, pokud chtějí splnit nároky kladené Nařízením GDPR i současným zněním zákona o zpracování osobních údajů v legislativním procesu.

V rámci dotazování bylo zjištěno, že Nařízení GDPR **je** zaměstnavateli reflektováno.

V rámci dotazování bylo zjištěno, že na zpracování údajů o trestněprávní činnosti **není ze strany zaměstnavatele kladen žádný důraz.**

V rámci dotazování byly zjištěny časté nesoulady ohledně výkladu Nařízení GDPR.

V rámci teoretické části byly popsány za použití odborné literatury klíčové body pro základy zpracování údajů o trestněprávní činnosti včetně zvolení vhodného právního základu.

V rámci praktické části byly připraveny doporučení, které se týkají zpracovávání jak údajů o trestněprávní činnosti, tak osobních údajů běžné kategorie. Tato doporučení přitom úzce souvisela s vhodnými předpoklady, které mají nastat před zahájením zpracováním údajů o trestněprávní činnosti.

Tato studie nemůže nahradit poradenství profesionálních právníků.

V Praze dne 31. října 2018