PRK PARTNERS

advokátní kancelář

Nakládání s osobními údaji zaměstnanců

5. prosince 2017

FORUM

Naše znalosti pro Váš úspěch

PRAHA | BRATISLAVA | OSTRAVA

www.prkpartners.com

Úvod - současná situace

- zákon č. 101/2000 Sb., o ochraně osobních údajů ("Zákon")
- stručná a ne příliš jasná a konkrétní ustanovení; nedostatek literatury a soudních rozhodnutí
- dozor a kontroly provádí **Úřad pro ochranu osobních údajů** ("Úřad") – otevřený a vstřícný (veškeré prameny na www.uoou.cz)
- Úřad poskytuje i poradenství (telefon, email, osobní), někdy však protichůdné výklady a nekvalitní výstupy; Úřad vydává i stanoviska
- pokuty nad 200.000 Kč výjimečné (max. pokuta 10.000.000 Kč)
- v současné chvíli je celý systém relativně stabilní a klidný (snad s výjimkou monitoringu zaměstnanců)
- dlouho očekávané nařízení EU o ochraně osobních údajů (tzv. GDPR) nabyde plné účinnosti **25.5.2018** - do té doby musí být vše v souladu; připravuje se nový zákon o zpracování osobních údajů
- 29.7.2017 nabyla účinnosti novela, podle které mohou inspektoráty práce kontrolovat a **trestat narušení soukromí (monitoring)** zaměstnanců

Hlavní změny EU nařízení GDPR

Mnohem podrobnější nařízení (173 recitálů, 99 článků, cca 100 stran) nahradí současnou Směrnici o ochraně osobních údajů a příslušné národní předpisy (v ČR Zákon) a bude přímo účinné v jednotlivých státech

- **silnější vynutitelnost** - porušení povede k vyšším sankcím - pokuty až 20 mio EUR nebo 4% ročního celosvětového obratu
- **práva subjektů údajů** - osobní údaje mají být pod jejich kontrolou
- **porušení ochrany** - správci budou povinni informovat Úřad, a v některých případech i subjekty údajů, o incidentech
- **pověřenec pro ochranu údajů (tzv. DPO)** - společnosti budou v určitých případech povinny jmenovat odpovědnou osobu (nikoliv ale jen z titulu zaměstnávání)
- **jediné správní místo** - národní úřad pro ochranu osobních údajů státu centrály bude vystupovat jako vedoucí regulátor pro otázky dodržování pravidel
- **soulad s předpisy** - důraz na prokazování ze strany správců (analýzy)

Základní principy (souhlas, jiné tituly, zabezpečení) **se nemění**

Kontrolní činnost Úřadu – výroční zprávy

Relativně velmi malý počet kontrol (7 inspektorů)

- **2016** – 116 kontrol (bez rozlišení) / 53 řízení o porušení zákona
- **2015** – 135 kontrol (bez rozlišení) / 49 řízení o porušení zákona
- **2014** – 144 kontrol (bez rozlišení) / 78 řízení o porušení zákona
- **2013** – 139 kontrol (bez rozlišení) / 101 řízení o porušení zákona
- **2012** – 129 kontrol (bez rozlišení) / 118 řízení o porušení zákona
- **2011** – 179 kontrol (bez rozlišení) / 132 řízení o porušení zákona
- **2010** – 161 kontrol (bez rozlišení) / 113 řízení o porušení zákona
- **2009** – 143 kontrol (bez rozlišení) / 89 řízení o porušení zákona
- **2008** – 112 kontrol (plán. 12, stížnost 100) / 95 řízení o porušení zákona
- **2007** – 112 kontrol (bez rozlišení) / 43 rozhodnutí o uložení pokuty
- **2006** – 113 kontrol (plán. 14, stížnost 99) / uloženo 64 pokut

Velká většina zjištěných nedostatků končí nápravou stavu (§ 40a Zákona)

Oznamování incidentů - GDPR (čl. 33 a 34)

Oznamování incidentů (případů porušení zabezpečení) Úřadu

- povinné u jakéhokoliv porušení, a to bez zbytečného odkladu (*72* hod)
- neplatí jen je-li nepravděpodobné riziko pro práva a svobody subjektů (typicky při nemožnosti identifikace subjektů)
- obsahem je popis incidentu, rozsahu, rizik a přijatých opatření

Oznamování incidentů subjektům

- povinné při pravděpodobném vysokém riziku pro práva a svobody
- opět bez zbytečného odkladu (bez uvedení lhůty)
- musí být jasně a jednoduše formulované (pokud jde o popis)
- není nutné, pokud byla přijata opatření, kterými se uniklá data stala nesrozumitelnými (šifrování), nebo následná opatření sníží riziko nebo by to vyžadovalo nepřiměřené úsilí (asi nepoužitelné u zaměstnanců)

Vedle výše uvedeného musí správce evidovat veškeré incidenty a okolnosti oznámení mají vliv i na sankci (její výši)

Zcela nové - nutné nastavit procesy a připravit dokumentaci

Detailní pravidla obsahují vodítka WP 250

Sankce podle GDPR (čl. 83)

Zásadní nárůst výše možných pokut

- 20 mio EUR nebo 4% celosvětového obratu v předchozím finančním roce (podle toho, co je vyšší)
- dle výkladu jde o obrat celé skupiny (nikoliv jen lokální pobočky)
- u některých povinností (porušení článků GDPR) je pokuta poloviční
- stejné pokuty hrozí i za porušení procesních pravidel (nesplnění pokynu nebo nekomunikace s Úřadem)

Při ukládání pokut se zohlední *mimo jiné*

- míra odpovědnosti správce s přihlédnutím k bezpečnostním opatřením
- míra spolupráce s Úřadem ze účelem nápravy nebo zmírnění účinků
- zda správce své porušení oznámil či nikoliv

Tlak na jednotnost výkladu GDPR (WP 253) by měl vést k obdobným pokutám v rámci EU, a to i jako pojistka proti účelovým přesunům činnosti

- zástupci Úřadu již nyní deklarují nárůst (v případě T-Mobile by za GDPR byla pokuta v řádu “stamiliónů korun“)

GDPR nemá specifickou úpravu

Důvodem přijetí nového GDPR nebyly údaje zaměstnanců, resp. nějaké plošné problémy při jejich nakládání (ochraně) ze strany zaměstnavatelů

- **GDPR neobsahuje žádnou zvláštní úpravu** dopadající na zaměstnavatele (obdobně jako současný Zákon)
- nová pravidla GDPR ale dopadnou i na zaměstnavatele a jejich zaměstnance, stejně jako na ostatní subjekty údajů
- zaměstnanci již nyní mají řadu privilegií (jde ale o povinné zpracování)
- GDPR (čl. 88) předpokládá legislativní iniciativu států, pokud jde o
  - konkrétnější pravidla zpracování osobních údajů zaměstnanců, zejména náboru, plnění pracovní smlouvy a zákona/KS, řízení, plánování a organizace práce, zajištění rovných podmínek, BOZP, ochrany majetku zaměstnavatele/zákazníků, ukončení PP, a dále i opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, včetně transparentnosti zpracování, předávání údajů v rámci skupiny a monitoring
- těmito předpisy jsou zejm. ZP a zákon o zaměstnanosti; český stát nebude pravděpodobně proaktivní při vymýšlení dalších pravidel

V květnu 2018 tak nebudou další (podrobnější) pravidla

Omezení použitelnosti souhlasu dle GDPR

Významná změna přístupu k souhlasům (resp. potvrzení trendu)

- souhlas není nutný pro základní účel - personálně-mzdovou agendu, resp. dle výkladů (i stávajících - viz stanovisko Úřadu č. 3/2014) je nežádoucí (ačkoliv to GDPR - čl. 6 - jasně neuvádí)
- u jiných účelů založených na souhlasu bude nutné splnit zostřené požadavky GDPR, zejm. dobrovolnost a nepodmíněnost souhlasu, což již nyní vede k závěrům, že **souhlas zaměstnance obecně nefunguje** (zmiňuje to i WP29)
  - to se může týkat použití fotografie mimo spis, případně zasílání údajů mateřské společnosti (pokud to vyžaduje a s údaji provádí rozsáhlou personalistiku)
- souhlasem nelze překonat porušování principů a povinností GDPR
- souhlas nepřipadá do úvahy ani při monitoringu zaměstnanců, neboť ti mají právo na soukromí dané Listinou základních práv a svobod

Vždy je vhodné mít (dovodit) jiný titul než souhlas, zejm. plnění smlouvy, plnění zákonné povinnosti, oprávněný zájem

Široká informační povinnost dle GDPR

Nadále platí široká informační povinnost zaměstnavatele vůči zaměstnancům

- důvodem je i zrušení předchozí registrace u Úřadu
- zaměstnanci mohou žádat o široké spektrum informací o tom, jak jsou jejich osobní údaje zpracovávány, v jakém rozsahu atd.
- platí ohledně všech dílčích zpracování - i těch povinných

Bude tak nutné upravit dokumentaci pro zaměstnance (a Úřad)

- vhodná je **ucelená písemná informace o zpracování v rámci zaměstnavatele**, včetně souhlasu pro určitá dílčí zpracování (fotografie), souhlas by měl být jasně oddělen od ostatního textu a navázán jen na dílčí zpracování
- současně *doporučujeme* i přijetí (aktualizaci) **směrnice o zpracování údajů** – praktický manuál zejména pro personalisty a vedoucí
- součástí směrnice mohou být i **povinné záznamy** (čl. 30 GDPR)

Otázkou je použitelnost stávajících dokumentů (recitál 171)

Zpřístupnění údajů externím subjektům

Posílení odpovědnosti a rozšíření povinností na straně smluvních partnerů zaměstnavatelů (čl. 28 a 26)

- zpřísnění a zpřesnění úpravy obsahu smlouvy o zpracování údajů
  - nadále zapojení partnerů není podmíněno souhlasem zaměstnanců
- vhodné provést revizi zapojení dodavatelů nakládajících s údaji zaměstnanců (poskytovatelé HRIS řešení, externí mzdové účtárny, externí HR, "benefitní" společnosti, BOZP/PO poradci, recruitment agencies, závodní lékaři, agentury práce, odborové organizace, mateřské společnosti) kteří mohou mít postavení
  - **zpracovatelů** podle čl. 28
  - **společných správců** podle čl. 26
  - **"obyčejných" příjemců** (i v tomto případě je vhodné řešit)
- nutné sladit smlouvy s GDPR - uzavřením dodatku (i když není zcela jasné, zda je třeba u zpracovatelů smyslem či. 28 skutečně to, aby smlouvy obsahovaly (opsaly) zde uvedené požadavky)
- nejasné, zda lze postihnout zpracovatele za případný nesoulad

Údajů mimo EU – zvýšená rizika a povinnosti

Posílení odpovědnosti zaměstnavatelů při přeshraničních transferech osobních údajů zaměstnanců

- zaměstnavatelé musejí být schopni prokázat legitimitu transferů a minimální míru ochrany osobních údajů v zahraničí
- při masivních anebo systematických převodech údajů mohou být zaměstnanci v pozici tzv. zranitelných subjektů; s tím je spojena náročná povinnost vypracovat zprávu o posouzení vlivu na ochranu osobních údajů a povinnost předchozí konzultace Úřadu (tzv. DPIA) – viz vodítka WP 248
  - tyto povinnosti by mohly dopadat i na různá cloudová řešení a centrální HR systémy uložené na serverech ve třetích státech
  - dle WP 248 se tato povinnost týká až nově zahájených zpracování
- pravděpodobně vzroste význam tzv. závazných podnikových pravidel (Binding Corporate Rules - BCRs) pro zpracování osobních údajů (v zahraničí anebo např. při zpracování v cloudu)

Nové instituty dle GDPR

Nová ohlašovací povinnost incidentu na poli ochrany osobních údajů (čl. 33 a 34)

- nově bude povinné hlásit jakékoliv porušení zabezpečení údajů (jejich zneužití, únik apod.) Úřadu, nejpozději do 72 hodin
- v případě zvlášť závažných úniků i všem zaměstnancům (stejně jako dalším subjektům údajů), a to bezodkladně

Bude nutné nastavit interní procesy pro splnění této povinnosti a připravit dokumenty; patrně to ale není úkol pro HR

Nová povinnost vést podrobné záznamy o zpracovávaných údajích zaměstnanců (čl. 30)

- jde o popis nakládání s údaji, které musí být zaměstnavatel schopen předložit na žádost Úřadu
- nejasné uplatnění výjimky pro malé podniky u zaměstnaneckých dat

Nové instituty dle GDPR

Nové právo na přenos údajů k jinému správci (data portability) (čl. 20)

- jediné zcela nové právo subjektů údajů
- smyslem je snadný přechod spotřebitele k jinému poskytovateli služeb (podpora konkurence)
- u zaměstnanců nejasné použití - WP 242 hovoří o použitelnosti například v oblasti výplat a náhrad a vnitřního náboru (str. 8 vodítek)
- lze doporučit spíše akceptovat žádost a předat omezená data

Nová povinnost jmenovat pověřence - DPO (čl. 37 - 39)

- platí pro zvláštní skupiny správců a zpracovatelů (orgány veřejné moci, rozsáhlé pravidelné a systematické monitorování, rozsáhlé zpracování zvláštních kategorií údajů)
- obecně by ani zaměstnávání velkého počtu zaměstnanců, potažmo třeba činnost velké mzdové účtárny (zpracovatele) neměla vést k této povinnosti (nebudou-li pro to jiné důvody) - viz WP 243 (bod 2.1.2)

Nové instituty dle GDPR

Zavedení institutu posouzení vlivu na ochranu údajů (DPIA) (čl. 35)

- povinnost při vysoce rizikových zpracování provést detailní analýzu dopadů - patrně nejkomplikovanější nová povinnost
- GDPR uvádí 3 povinné případy (systematické a rozsáhlé automatické vyhodnocování osobních aspektů, rozsáhlé zpracování zvláštních kategorií údajů a rozsáhlé systematické monitorování veřejně přístupných prostorů)
- WP 248 dále zmiňuje aspekty typu (systematický monitoring, rozsáhlé zpracování, zranitelné subjekty, převody dat mimo EU) s tím, že kombinace 2 aspektů by měla/mohla vést k povinnému posouzení
- WP 248 výslovně zmiňují monitoring zaměstnanců (počítače, web)
- dle WP 248 DPIA povinná až pro zpracování zahájená po 25.5.2018

Předchozí konzultace s Úřadem (čl. 36)

- povinná v návaznosti na DPIA a před započetím zpracování
- podrobněji upravená obdoba dnes plošné (s výjimkou zpracování povinného na základě zákona) registrační povinnosti

Změna přístupu k povinnosti mlčenlivosti

Povinnost mlčenlivosti zaměstnanců a dalších zástupců správců a zpracovatelů

- dnešní předpisy stanoví jednoznačně povinnost mlčenlivosti, a to i po skončení zaměstnání (§ 15 zákona č. 101/2000 Sb.)
- GDPR výslovnou a jednoznačnou úpravu nemá, hovoří pouze o povinnosti respektovat pokyny správce (čl. 29), u zástupců zpracovatele má zpracovatel zajistit smluvní nebo zákonnou povinnost mlčenlivosti (čl. 28/3.b))
- návrh nového zákona o zpracování osobních údajů mlčenlivost stanoví v § 12 jen pro DPO a jemu podřízené osoby (ne obecně pro všechny osoby s přístupem k údajům - § 42 návrhu se týká "neunijního" zpracování)
- nejsou stanoveny ani žádné sankce (přestupky) pro zaměstnance a jiné zástupce; dnes hrozí např. personalistům pokuta až 100.000 Kč
- **dle Úřadu se fakticky nic nemění**, resp. zaměstnavatel si může (spíše musí) nastavit vlastní pravidla mlčenlivosti
- snad nebude docházet ke zpochybnění ze strany zaměstnanců porušujících mlčenlivost (při absenci výslovné zákonné mlčenlivosti)

Doporučení dalšího postupu před účinností GDPR

Provedení auditu veškerých procesů, pravidel a dokumentace týkající se nakládání s údaji zaměstnanců z pohledu práva a IT

- s ohledem na budoucí úpravu (sankce) je nutné mít pod kontrolou jaká data se zpracovávají, v rámci jakých systémů, jak je s daty dále nakládáno, kdo k nim má přístup, jaká je ochrana údajů, zda a jak se data aktualizují a likvidují
  - v praxi se i u renomovaných společností setkáváme s “překvapivým nepořádkem“ a až zarážející bohorovností, často se jedná o absolutní neznalost systémů a procesů, nebo o případy neomezeného sdílení dat ve skupině (jednotný HR systém)
- daným procesům a pravidlům by měly odpovídat interní dokumenty (směrnice a hlavně informace/souhlasy zaměstnanců)
- celou oblast je vhodné provést koordinovaně, v součinnosti s kolegy, kteří se zabývají údaji zákazníků a jiných skupin subjektů údajů
- pokud fungujete ve skupině, je vhodná/nutná koordinace s centrálou

Pokud nyní neplníte Zákon, zcela jistě budete porušovat i GDPR

Základní pojmy podle Zákona a GDPR

Osobní údaj; GDPR drobně rozšiřuje o lokační údaje a síťový identifikátor

- jakákoliv informace týkající se určené nebo určitelné FO (**subjektu údajů**, nikoliv PO), na jehož základě se dá přímo či nepřímo identifikovat - identifikační, adresné a popisné údaje
- nejedná se jen o jména, čísla a kontaktní údaje

Zpracování osobních údajů; GDPR platí i pro jednorázové operace

- jakákoliv systematicky prováděná operace nebo soustava operací s osobními údaji, zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace
- nahodilé shromažďování údajů není zpracováním, pokud tyto údaje nejsou dále zpracovávány (o to by se mohlo jednat třeba u nahlédnutí do emailové schránky) - GDPR toto již neupravuje

Správce (zaměstnavatel), **zpracovatel** (mzdová účtárna), **příjemce** (mateřská společnost); GDPR nemění (nově upravuje společné správce)

Citlivé osobní údaje (§ 4(b), 9)

- údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin (pouze záznam v TR, nikoliv "čistý" rejstřík), zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv genetický údaj, případně i biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů
- nakládání s fotografiemi a kamerovým záznamem není zpracování citlivých údajů (pokud správce s těmito aspekty nepracuje)

Platí výše uvedené zásady, s výjimkou

- souhlas musí být výslovný (nelze jej dovodit z jednání subjektu údajů)
- souhlas není nutný, pokud je zpracování nezbytné pro dodržení povinností a práv zaměstnavatele v oblasti pracovního práva a zaměstnanosti (diskriminace, postižení, nikoliv účast v odborech)

GDPR principy nemění; používá pojem zvláštní kategorie údajů (čl. 9), údaje o trestných činech dává do samostatné skupiny (čl. 10)

Hlavní zásady / povinnosti při zpracování

Souhlas subjektu údajů

- existuje řada výjimek z povinnosti mít souhlas - hlavně vedení základní personálně-mzdové agendy a ochrana práv správce; GDPR přejímá

Informační povinnost

- bez ohledu na případný souhlas je vždy nutno poskytnout subjektům údajů povinné informace o zpracování; GDPR precizuje a zpřísňuje

Oznamovací (registrační) povinnost

- předchozí oznámení zpracování Úřadu - není nutné, pokud je zpracování povinné; GDPR zná (omezené) předchozí konzultace Úřadu

Zabezpečení osobních údajů

- přijetí (a zdokumentování) bezpečnostních opatření; GDPR rozvíjí dál

Zvláštní povinnosti

- vždy platí i zvláštní povinnosti přímo upravující zpracování; GDPR klade důraz na prokazování splnění povinností správcem + nové instituty

Tyto kategorie je nutné mít pod kontrolou u každého účelu zpracování

Vedení personálně-mzdové agendy

Základní účel zpracovávání osobních údajů zaměstnanců

- zaměstnavatel musí nakládat s údaji svých zaměstnanců (ZP je de facto celý o zpracovávání) - plnění zákonných/smluvních povinností

Toto zpracování v sobě zahrnuje mimo jiné i:

- práce s životopisy kandidátů během výběrového řízení
- použití fotografie ve spisu či na vstupní průkazce zaměstnance
- evidence práce - docházkové/vstupní systémy; stanovisko Úřadu č. 3/2009 ohledně biometrické identifikace či autentizace zaměstnanců
- další povinné databáze/evidence (úrazy, cizinci apod.)
- evidence pro plnění povinností podle ZP/smlouvy (odměňování, benefity, dovolená, překážky v práci, postižení, BOZP, PLS); stanovisko Úřadu č. 2/2014 o dynamickém biometrickém podpisu
- vyřizování stížností zaměstnanců
- přiměřená kontrola zaměstnanců při použití vybavení zaměstnavatele
- mzdové databáze (odvody, dávky, důchody apod.; povinná dokumentace)
- povinné uchovávání dokumentů/údajů po skončení vztahu

GDPR nemá specifickou právní úpravu (viz i čl. 88)

Další samostatná zpracování osobních údajů zaměstnanců

Vedle základního účelu - **vedení personálně-mzdové agendy** do úvahy připadají tato samostatná zpracování

- *vedení databáze zájemců o práci (CV i po/bez výběrového řízení)*
- *podpora komunikace - fotografie na internetu/intranetu, PR materiály*
- *správa HR záležitostí v rámci skupiny (mateřskou společností)*
- Whistleblowing Policy
- uchovávání údajů bývalých zaměstnanců (jiných než povinných)
- kamerový systém s uchováváním záznamu
- monitoring emailů - monitoring internetu (permanentní)
- nahrávání telefonních hovorů
- monitoring GPS služebních vozidel (dalšího vybavení)
- databáze zaměstnanců - zákazníků
- nakládání s údaji rodinných příslušníků pro kontaktování
- …

Nakládání s údaji BĚHEM výběrového řízení

Nakládání s životopisy

- jedná se o zpracování osobních údajů, které v praxi obecně nezpůsobuje větších problémů

Základní povinnosti

- souhlas zájemců o práci není nutný (navíc jej lze dovodit), neboť zde je jiný titul - nezbytnost pro uzavření (pracovní smlouvy)
- informační povinnost vůči zájemcům o práci
- oznámení Úřadu není nutné (praxe a výklad Úřadu)
- zabezpečení životopisů

Doporučujeme splnit informační povinnost na webu + i v listinné informaci předávané fyzicky zájemcům (“v zasedačce“, kde lze získat i souhlas, je-li potřebný), případně i v inzerátu (v inzerátu lze uvést jen odkaz na web)

Nakládání s údaji PO SKONČENÍ výběrového řízení

Doba uchovávání životopisů omezena

- pouze nutná doba ke stanovenému účelu
- po skončení výběrového řízení by měla následovat likvidace, resp. vrácení (to již není povinné ani při skončení zaměstnání)
- Městský soud v Praze potvrdil pokutu Úřadu za nevrácení listin

Možnost dalšího uchovávání

- souhlas neúspěšných zájemců o práci nutný pro případnou další nabídku práce (oslovení) - nelze presumovat (nutno aktivně); snad platí i podle GDPR, které jinak značně akcentuje oprávněné zájmy
- informační povinnost vůči zájemcům
- oznámení Úřadu (**účel: "vedení databáze zájemců o práci z účelem umožnění další nabídky zaměstnání"**)
- vždy platí povinnost zabezpečení životopisů
- i při souhlasu musí být doba uchování omezena (obecně max. 3 roky)

Nakládání s údaji PO SKONČENÍ výběrového řízení

Bez souhlasu (který se obtížně získává od zájemců, se kterými zaměstnavatel není v kontaktu) lze uvažovat o uchovávání údajů po/bez výběrového řízení pro tyto účely:

- obrana práv zaměstnavatele (proti námitkám neúspěšných zájemců)
- vedení "blacklistu", tedy seznamu nevhodných kandidátů

Účelu musí odpovídat rozsah uchovávaných údajů + je nutné splnit i informační povinnost a patrně i ohlásit zpracování u Úřadu

- neexistuje žádná judikatura nebo stanovisko Úřadu

Uchování údajů BEZ konkrétního výběrového řízení

- i zde lze dovodit nezbytnost pro uzavření budoucí smlouvy
- je nutné poskytnout informaci o zpracovávání údajů, zejm. ohledně délky uchovávání údajů
- lze ukládat osobní údaje potenciálních kandidátů, i bez nutnosti informování (viz čl. 14/3 písm. b) GDPR)

Vedení osobního spisu

Nahlédnutí do spisu je dle § 312 ZP umožněno pro:

- nadřízení vedoucí zaměstnanci
- státní orgány:
  - orgán inspekce práce, úřad práce
  - soud, státní zástupce, příslušný orgán Policie ČR
  - NBÚ, Úřad a zpravodajské služby

Špatná právní úprava

- chybí mimo jiné personalisté nebo výše postavení nadřízení vedoucí, právníci, interní audit
- není zmíněno ani právo činit si výpisky a pořizovat stejnopisy

Zaměstnanec může nahlížet, činit si výpisky a pořizovat stejnopisy dokladů, a to na náklady zaměstnavatele

- co po skončení pracovního poměru? (GDPR problém překonává)
- lze tímto právem bránit přemístění spisů do jiné budovy či země?

Nakládání s fotografiemi mimo spisy

Použití fotografie na intranetu/internetu (či na vizitkách či nástěnce)

- není zvláštní úprava týkající se zaměstnanců, platí obecné principy
- není součástí vedení personálně-mzdové agendy, nutné splnit následující povinnosti:
  - souhlas zaměstnanců (možné odlišnosti při odvolání dle GDPR)
  - informační povinnost
  - oznámení Úřadu (**účel: "<u>podpora komunikace</u>"**), vhodné pamatovat i na marketingové materiály (fotky z akcí/teambuildingu)
  - veškeré další povinnosti dle Zákona (GDPR)
- <u>otázkou je, zda z pohledu ZP i GDPR nemůže jít v určitých omezených případech (zástupci vedení, obchodní zástupci) o legitimní požadavek</u>
- zveřejnit jméno, funkci, email na webu lze i bez souhlasu zaměstnance

Použití fotografií ve spisu nebo na průkazu (vstupní kartě) - dle Úřadu jde o zpracování v rámci plnění povinností zaměstnavatele (vedení personálně-mzdové agendy); i fotografie by měla být zabezpečena

Správa HR záležitostí skupiny

Mateřská společnost často vyžaduje po zaměstnavateli předání údajů zaměstnanců, se kterými pracuje obdobně jako zaměstnavatel

- předání údajů (resp. jejich další zpracovávání) jde většinou nad rámec povinného zpracování zaměstnavatelem - není nezbytné, přestože se týká již zpracovávaných údajů, jde o jiný samostatný účel
- účelem často "**správa HR záležitostí v rámci skupiny**"
- zaměstnanci by tedy měli dát souhlas (nikoli s předáním, ale s celým zpracováním) + by měli být informováni o předání
- není ani jasné postavení českého zaměstnavatele; podle GDPR by se mělo jednat o vztah společných správců (čl. 26)

Jinou formou spolupráce může být **případ, kdy český zaměstnavatel pověří jinou společnost (často sesterskou ve skupině), aby pro něj realizovala jako zpracovatel některé činnosti, typicky v rámci personálně-mzdové agendy**

Předání limitovaného objemu dat pro "statistické či administrativní" účely dle současné praxe Úřadu souhlasu nepodléhá

- GDPR to potvrzuje (recitál 48) – zmiňuje existenci oprávněného zájmu

Whistleblowing Policy

- zavedení pravidel pro hlášení podezřelých okolností ve finanční oblasti (zejm. účetnictví, audity), založených na tzv. „SOX zákonu“ v USA
- většinou telefonní nebo emailová linka provozovaná zahraniční firmou
- WP 117 - Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes
- na Slovensku od roku 2015 povinná u zaměstnavatelů s 50 a více zaměstnanci (v ČR se nestihly probrat 2 návrhy zákonů)

Povinnosti zaměstnavatele, byť přímo neprovozuje:

- oznámení Úřadu (jde o samostatný **účel „Whistleblowing Policy“**)
- souhlas zaměstnanců není nutný - dle komentářů k GDPR plnění zákonné povinnosti vyplývající z práva třetích států není relevantní
- nutné split informační povinnost
- projednání s odborovou organizací (působí-li u zaměstnavatele)
- veškeré další povinnosti dle Zákona (zabezpečení zjištěných dat)
- lokální schránka pro stížnosti zaměstnanců spadá pod povinnost zaměstnavatele dle § 276/9 ZP

Monitoring zaměstnanců - úvod

Monitoring zaměstnanců je **stále aktuální téma**

GDPR může spojovat s permanentním monitoringem nové povinnosti (pověřenec, povinné posouzení vlivu) - viz WP 243 a 248

Právní **úprava je velmi problematická** - neobsahuje definici monitoringu

Není dostatek zdrojů informací – nejlepší vodítka poskytují WP 55 a 249 (nové technologie)

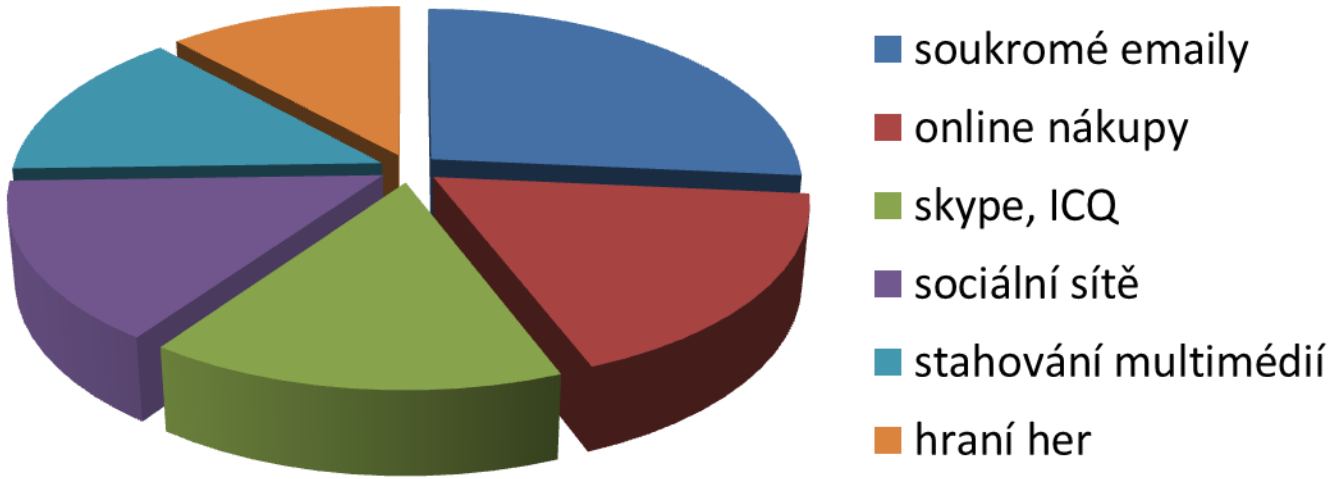
Obecně jde o sledování zaměstnanců, jejich aktivit a činností, typicky

- monitoring emailů (včetně DLP a obdobných systémů)
- monitoring použití internetu
- kamerový systém
- zaznamenávání telefonických hovorů
- monitoring pohybu služebních vozidel (GPS)
- lokátory pohybu jiného vybavení
- monitoring počítače a dalšího vybavení zaměstnance
- …

Trocha statistiky

TruconneXion

- 75% firem monitoruje zaměstnance
- 52 minut - průměrný rozsah zneužití pracovní doby denně
- 32.760 Kč v průměru zaplatí firmy ročně zaměstnanci za surfování
- do 20 minut denně firmy akceptují coby “zdravý relax“



Přehled právní úpravy

- Mezinárodní úmluvy (zejm. Mezinárodní pakt o občanských a politických právech a Úmluva o ochraně lidských práv a základních svobod)
- Listina základních práv a svobod (č. 2/1993 Sb.)
- **Zákoník práce**
- Zákon o ochraně osobních údajů
- Zákon o inspekci práce (č. 251/2005 Sb.) – již schválená novela
- Trestní zákoník (č. 40/2009 Sb.)
- Soudní rozhodnutí (evropská a česká)
- Stanoviska Úřadu pro ochranu osobních údajů
- Stanoviska a doporučení Pracovní skupiny dle článku 29

Zákoník práce – Ad hoc kontrola

Dle **§ 316/1 ZP** *zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*

- nová úprava (od 2007) - zatím není mnoho judikatury ani článků
- jednoznačný zákaz pro zaměstnance - pozor ale na tolerování, které lze považovat za souhlas a na přístup k soukromí v rámci Evropy
- i když u zaměstnavatele platí absolutní zákaz, nelze vyloučit např. soukromou přijatou emailovou poštu zaměstnance
- doporučujeme stanovit základní pravidla pro soukromé použití (zejm. omezený rozsah, plnění pracovních povinností, vyloučení škody zaměstnavatele a neporušení jakýchkoliv povinností a práv) *POZOR ale na daňové aspekty*
- vhodné informovat o provádění přiměřené kontroly (prevence zneužití)

Je v zájmu zaměstnavatelů se pohybovat, a to skutečně a pouze, v této kategorii omezeného monitoringu

Zákoník práce – Permanentní monitoring

Dle § 316/2 ZP nesmí z*aměstnavatel bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách tím, že jej podrobuje otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci*.

- nejasné ustanovení - výklady se naprosto liší, pokud jde o
  - navázání možnosti monitoringu na specifickou činnost zaměstnavatele; jsou i názory, dle kterých je možnost sledování (monitoringu) dána všem zaměstnavatelům (jde o činnost zaměstnavatele v užším smyslu)
  - obecné použití; existují výklady, dle kterých se toto ustanovení týká výlučně soukromé komunikace zaměstnance, např. ze soukromého mobilu nebo soukromých emailů

Otázkou je, zda třeba kamerový systém bude vždy považován za permanentní monitoring dle tohoto ustanovení (výjimkou by byl jistě "noční" záznam ze skladu), když se záznam používá až při řešení incidentů

Zákoník práce - Permanentní monitoring

§ 316/3 ZP

Jestliže je u zaměstnavatele dán závažný důvod, který odůvodňuje zavedení kontrolních mechanismů, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

- dle mého názoru dopadá jen na permanentní monitoring podle § 316/2 ZP
- není zcela jasné, co se myslí "přímým informováním" - směrnice by měla dostačovat
- informace (směrnice) by měla obsahovat stručné vymezení, kdy se provádí sledování (např. GPS v autech), nebo kdy ke sledování může dojít (např. čtení emailů z důvodu nepřítomnosti zaměstnance); danou problematiku lze zakomponovat do povinné informace o zpracovávání osobních údajů

Monitoring emailů a Internetu

Stanovisko Úřadu č. 2/2009

- Úřad zastává striktní postoj ve prospěch zaměstnance

Připouští:

- sledovat počet došlých a odeslaných emailů prostřednictvím firemní emailové adresy, případě jejich hlavičky (vznikne-li podezření na zneužití prostředků zaměstnavatele); číst soukromý email zaměstnance může pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní email (např. vyřízení emailu v době dlouhodobé nemoci)
- sledování používání webu nebo statistické sledování využívání přístupu k internetu, pokud existuje závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele - například mezinárodní bankovní převody nebo dozor nad prací vězňů

Manuál SUIP (metodika pro inspektoráty práce)

- u emailů platí obdobné, ale ohledně “osobních“ emailů
- kontrola obsahu navštívených webových stránek není přípustná, zaměstnavatel ale může být informován o celkovém stráveném čase

Nejvyšší soud připustil 1měsíční kontrolu webu (21 Cdo 1771/2011)

Kamerový systém se záznamem

Stanovisko Úřadu č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů

- nejedná se o specifické stanovisko týkající se kamer na pracovišti
- specifikuje zásady implementace kamerového systému - zejména pokud jde o souhlas (který není na místě, pokud systém slouží k ochraně práv zaměstnavatele či jiné osoby), informační povinnost (a nutnost registrace u Úřadu)
- v případě implementace je vhodné prostudovat metodiku Úřadu, která nicméně byla stažena z webu Úřadu a je otázkou, zda se tam vrátí přepracovaná (flexibilnější)
- v praxi **ohledně kamerových systémů nyní příliš problémů není** - standardně se registrují k ochraně majetku, např. ve skladech, kolem areálu
- naopak se již nnyí **nepřipouští systémy za účelem kontroly zaměstnanců** (výkonnost, dodržování pracovních postupů)
- uvidíme, jaký bude přístup inspektorátu práce; manuál je striktní a hovoří o tom, že běžný zaměstnavatel nemůže mít kamerový systém
- existuje řada soudních rozhodnutí, zejm. následných po kontrole Úřadu

Stanoviska a doporučení Pracovní skupiny dle článku 29

Skupina (označovaná jako WP29), tedy zástupci národních úřadů (ÚOOÚ) a budoucí Sbor dle GDPR má klíčovou roli v oblasti osobních údajů (a tedy i monitoringu) - sjednocuje výklad a dává odborná stanoviska a doporučení

Nové Opinion 2/2017 on data processing at work (WP 249) ze dne 8.6.2017 (které se zaměřuje na nové technologie) doplňující Working document on the surveillance of electronic communications in the workplace (WP 55) ze dne 29.5.2002

- relativně ucelená úprava možného monitoringu, zejména emailů a internetu
- připouští i skrytý monitoring (bez informování), pokud existuje oprávněné podezření na nezákonné jednání zaměstnance
- důraz je kladen na férovost a transparentnost jednání zaměstnavatele, přiměřenost monitoringu a poskytnutí řádných informací zaměstnancům
- navazuje na WP 48 - Opinion 8/2001 on the processing of personal data in the employment context ze dne 13.9.2001 (zmíněné Úřadem ve stanovisku č. 2/2009)

Záznamy telefonních hovorů

Stanovisko Úřadu č. 5/2013 – dle kterého účelem může být obchodní monitoring (zlepšování služeb) nebo potřeba pro uzavření/plnění/změnu smlouvy; mělo by tak jít o obchodní hovory

- nutno odlišovat oba účely i skupiny subjektů údajů (zaměstnanci + zákazníci)

Obchodní monitoring

- souhlas (potenciálních) klientů nutný, zaměstnanců nikoli
- oznámení Úřadu nutné (nyní relativizováno samotným Úřadem)

Nezbytné zpracování pro smluvní vztahy

- souhlas zaměstnanců ani zákazníků není nutný (výjimky dle zákona)
- oznámení Úřadu se ani dříve nevyžaduje

- Společné pro oba účely
  - informační povinnost - platí vůči oběma skupinám subjektů
  - veškeré další právní povinnosti (záznam jen po nezbytnou dobu)
- manuál inspekce práce neumožňuje odposlouchávání osobních hovorů

Monitoring služebních vozidel (GPS)

Jedná se o **zpracování osobních údajů**, navíc upravené v **§ 316 ZP**

- klíčové je vymezení účelu GPS
- **plnění jiných povinností** (vedení knihy jízd/evidence řízení a přestávek) i **ochrana majetku (proti krádeži)** by mělo být bezproblémové
  - souhlas zaměstnanců není nutný; registrace u Úřadu jen ohledně ochrany majetku
- nejasný je monitoring za účelem **kontroly zaměstnanců**, tj. zda jezdí, resp. plní pokyny jak/kudy jezdit, vyhodnocování stylu jízdy apod.
  - tento účel se s jistotou nebude líbit **inspekci práce** (odmítá obecně GPS), až budou kontrolovat neporušování soukromí zaměstnanců; restriktivní výklad § 316/2 ZP - dopadá jen na jaderné elektrárny apod.
  - riziko neřeší ani souhlas zaměstnanců (i tak jej doporučujeme)

Nutné plnit informační povinnost (vůči zaměstnancům) i další povinnosti

Snad lze provést limitovanou ad hoc kontrolu i bez specifické registrace u Úřadu a její výsledky použít u soudu při propuštění

Kontrola obsahu počítačů a dalších úložišť

Přiměřená (nepermanentní) kontrola je možná dle § 316/1 ZP

- může ji realizovat každý zaměstnavatel a není nutné o ní ani specificky informovat zaměstnance (z pohledu ZP)
- informaci o možné kontrole (z pohledu ochrany osobních údajů) je nicméně vhodné zmínit v rámci směrnice, která by řešila pravidla (zákazy) pro použití firemního vybavení
- opět nedoporučujeme absolutní zákaz, když realita je jiná, zejména pokud jde o soukromé fotografie a hudbu
- kontrola by měla být příležitostná, časově omezená a decentní
- takovouto kontrolu si dovolujeme považovat za součást personálně-mzdového zpracování (viz i povinnost vedoucích zaměstnanců kontrolovat práci podřízených podle § 302 ZP), tedy bez nutnosti mít souhlas zaměstnanců (a nyní bez nutnosti registrace u Úřadu)

Zajímají Vás pracovněprávní novinky?
Chcete vědět vše důležité pro personální praxi okamžitě?

Přihlaste se ke sledování našeho LinkedIn kanálu

Labour Law News by PRK Partners

Děkuji za pozornost

JUDr. Jaroslav Škubal

PRK Partners s.r.o.
advokátní kancelář

Jáchymova 2, 110 00 Praha 1
Tel.: +420 221 430 111 | Fax.: +420 224 235 450

jaroslav.skubal@prkpartners.com

Získáte vše. Samozřejmě.
Bez kompromisů.

www.prkpartners.com

THE LAWYER
EUROPEAN CONFERENCE & AWARDS
WINNER
Law Firm of the Year: Central Europe
2012

CHAMBERS EUROPE AWARDS for Excellence 2014 WINNER

CHAMBERS EUROPE AWARDS for Excellence 2013 WINNER

2016 právnická firma roku

2015 právnická firma roku

2014 právnická firma roku