



P A R T N E R S

advokátní kancelář

Osobní údaje zaměstnanců ve světle nových EU předpisů - GDPR

27. července 2017



*Naše znalosti
pro Váš úspěch*

PRAHA | BRATISLAVA | OSTRAVA

www.prkpartners.com

Program semináře

- I. Úvod do problematiky
- II. Základní principy zákona o ochraně osobních údajů a **GDPR**
- III. Povinnosti zaměstnavatelů při zaměstnávání osob
 1. Přijímání do zaměstnání
 2. Trvání pracovního poměru (osobní spis zaměstnance, fotografie zaměstnanců, apod.)
 3. Monitoring zaměstnanců - emaily, web, kamerové systémy, telefonické hovory, GPS
 4. Předávání osobních údajů do zahraničí
 5. Skončení pracovního poměru
- IV. Závěr

I. ÚVOD DO PROBLEMATIKY ZPRACOVÁNÍ ÚDAJŮ

Úvod - současná situace

- / zákon č. 101/2000 Sb., o ochraně osobních údajů (“Zákon“)
- / komplikovaná úprava - nejasná a nekonkrétní ustanovení
- / nedostatek literatury a soudních rozhodnutí
- / dozor a kontroly provádí **Úřad pro ochranu osobních údajů** (“Úřad“) - otevřený (web 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; proběhnou i legislativní úpravy Zákona
- / Senát 8.6.2017 schválil novelu, podle které budou inspektoráty práce kontrolovat a **trestat narušení soukromí** zaměstnanců

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

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

Hlavní změny EU nařízení GDPR

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

- / **soulad s předpisy** - důraz na prokazování ze strany správců (analýzy)
- / **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
- / **silnější vynutitelnost** - porušení povede k vyšším sankcím - pokuty až 20 mio EUR nebo 4% ročního celosvětového obrátu
- / **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

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

GDPR a údaje zaměstnanců

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 Zákon jen předpokládá zpracování údajů zaměstnanců)
- / 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

GDPR a údaje zaměstnanců

Omezení významu souhlasu zaměstnanců se zpracováním

- / neplatí pro základní vedení personálně-mzdové agendy, případně jiný právní titul pro zpracování (plnění smlouvy, oprávněný zájem) - vždy je vhodné mít (dovodit) jiný titul než souhlas
- / u jiných účelů založených na souhlasu bude nutné splnit zostřené požadavky GDPR (zejm. specifičnost a nepodmíněnost souhlasu), již nyní jsou polemiky, zda vůbec lze u zaměstnanců hovořit o svobodném souhlasu (který se navíc nadužívá, což Úřad kritizuje)

Rozšiřuje se informační povinnost zaměstnavatele (správce osobních údajů) vůči zaměstnancům (subjektům údajů)

- / důvodem je zrušení předchozí registrace u Úřadu
- / zaměstnanci mohou nově žádat o široké spektrum informací o tom, jak jsou jejich osobní údaje zpracovávány, v jakém rozsahu atd.
- / bude tak nutné upravit dokumentaci (písemné informace a souhlasy) pro zaměstnance

GDPR a údaje zaměstnanců

Posílení odpovědnosti a rozšíření povinností na straně smluvních partnerů zaměstnavatelů

- / vhodné provést revizi zapojení dodavatelů nakládajících s údaji zaměstnanců (poskytovatelé HRIS řešení, externí mzdové účtárny, recruitment agencies, “benefitní“ společnosti, agentury práce, smluvní lékař apod.) - zpracovatelů a případně smlouvy sladit s GDPR (čl. 28)

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)
- / pravděpodobně vzroste význam tzv. závazných podnikových pravidel (Binding Corporate Rules - BCRs) pro zpracování osobních údajů (v zahraničí anebo např. při zpracování v cloudu)

GDPR a údaje zaměstnanců

Nová ohlašovací povinnost incidentu na poli ochrany osobních údajů

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

Nová povinnost vést podrobné záznamy o zpracovávaných údajích zaměstnanců

- / jde o popis nakládání s údaji, které musí být zaměstnavatel schopen předložit na žádost Úřadu

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

Doporučení dalšího postupu před účinností GDPR

Provedení auditu veškerých procesů, pravidel a dokumentace týkající se nakládání s údaji zaměstnanců

- / 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

- / 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

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

- / každý zaměstnavatel musí nakládat s údaji svých zaměstnanců (ZP je de facto celý o zpracovávání osobních údajů)

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
- / další povinné databáze/evidence (úrazy, cizinci apod.)
- / evidence pro plnění povinností podle ZP (odměňování, benefity, dovolená, překážky v práci zdravotně postižení, BOZP, PLS apod.)
- / mzdové databáze (odvody, dávky, důchody apod.)
- / vyřizování stížností zaměstnanců
- / přiměřená kontrola zaměstnanců při použití vybavení zaměstnavatele
- / povinné uchovávání dokumentů/údajů po skončení vztahu

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

Další samostatné účely zpracování osobních údajů zaměstnanců

Vedle základního účelu - **vedení personálně-mzdové agendy** do úvahy připadají tyto samostatné účely 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

II. ZÁKLADNÍ PRINCIPY - PODROBNĚJŠÍ PŘEHLED ZMĚN (ROZDÍLY MEZI ZÁKONEM A **GDPR)**

Souhlas subjektu údajů (§ 4(n), 5/2)

- / svobodný a vědomý projev vůle obsahující svolení se zpracováním
- / nemusí být písemný, ale je nutné jej prokázat po celou dobu zpracování
- / souhlas neznamena možnost neplnit další povinnosti podle Zákona
- / stanovisko Úřadu č. 3/2014 varuje před nadbytečnými souhlasy (hrozí i pokutou, a to za špatné informování); **to bude asi prolomeno GDPR**
- / Zákon neřeší možnost odvolání, lze dovodit z § 87 NOZ

Výjimky

- / zpracování *nezbytné* pro dodržení právní povinnosti správce (zaměstnavatele)
- / zpracování *nezbytné* pro plnění (pracovní) smlouvy, nebo pro jednání o její uzavření
- / zpracování *nezbytné* pro ochranu práv a chráněných zájmů správce (zaměstnavatele) či jiné dotčené osoby; takové zpracování však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromí

Souhlas subjektu údajů – GDPR (čl. 7)

- / svobodný, **konkrétní**, informovaný a **jednoznačný** projev vůle
 - snaha o vymýcení blanketních (všeobecných) souhlasů
 - musí být důsledně zohledněna skutečnost, zda je souhlas podmíněn jinými plněními/službami, i když zpracování není nutné
- / v podobě prohlášení nebo jiného zjevného potvrzení svolení
- / správce musí být schopen doložit udělení souhlasu
- / při písemném vyjádření musí být **žádost o souhlas jasně odlišená** (oddělená) od ostatního textu (samostatně, ne v rámci VOP)
- / musí být **srozumitelný, snadno přístupný** za použití jasných a jednoduchých jazykových prostředků - jakákoliv část písemného vyjádření, která to nerespektuje, není závazná
- / **Ize kdykoliv odvolat**, což musí být stejně jednoduché jako udělení
 - musí být poskytnuta informace o nedotčenosti zákonnosti zpracování před jeho odvoláním (a tedy i o možnosti odvolání)

Souhlas udělený v souladu s GDPR před 25.5.2018 bude platit i nadále

I u zaměstnanců by **souhlas** měl být **až poslední možností**

Jiné základy zpracování (tituly) – GDPR (čl. 6)

Zpracování je zákonné, pokud je splněna **nejméně jedna z podmínek**:

- / souhlas pro jeden či více konkrétních účelů
- / zpracování je *nezbytné* pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu
- / zpracování je *nezbytné* pro splnění právní povinnosti správce
- / zpracování je *nezbytné* pro ochranu životně důležitých zájmů subjektu
- / zpracování je *nezbytné* pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
- / zpracování je *nezbytné* pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu

GDPR (čl. 6/4) zná i zpracování pro jiný účel než ten odsouhlasený, což ale budou spíše marginální výjimky

Informační povinnost vůči subjektu (§ 5/4, 11)

- / není nutná písemná forma, opět doporučujeme (pro prokázání splnění)
- / bez ohledu, zda je nutný souhlas či oznámení Úřadu, u souhlasu slouží k tomu, aby se subjekt rozhodl, zda jej udělí
- / při shromažďování, resp. při poskytnutí souhlasu

Povinný obsah

- / pro jaký účel a k jakým údajům, jakému správci a na jaké období
- / kdo a jakým způsobem bude údaje zpracovávat
- / komu mohou být osobní údaje zpřístupněny
- / poučení o právech na přístup, opravu a dalších právech dle Zákona
- / poučení, zda je poskytnutí osobních údajů dobrovolné nebo povinné (v takovém případě nutné poučit i o následcích odmítnutí poskytnutí)

Informační povinnost – GDPR (čl. 12 a násl.)

- / povinnost **platí obecně (vždy)**, a to v okamžiku získání údajů
- / **písemně či elektronicky** (ústní forma na požádání subjektu, což se těžko prokazuje) - vhodné mít textový formulář
- / **stručná, transparentní, srozumitelná, snadno přístupná forma**
- / zahrnuje informaci **o aspektech zpracování i o opatření při uplatnění práv subjektů** (do 1 měsíce s možným prodloužením)
- / poskytnutí informace je bezplatné, nejde-li o zjevně nedůvodnou či nepřiměřenou (opakovanou) žádost subjektu, kdy může chtít správce přiměřený poplatek nebo může žádosti nevyhovět
 - splnění podmínek pro odmítnutí/poplatek dokládá správce
- / informace mohou být doplněny standardizovanými, strojově čitelnými, **ikonami** (za účelem zvýšení srozumitelnosti a přehlednosti)
- / při pochybnostech o totožnosti subjektu může správce požádat o poskytnutí dodatečných informací k potvrzení totožnosti

Informační povinnost – GDPR (čl. 12 a násl.)

Povinný obsah obecné informace - při získání od subjektu

- / totožnost a kontaktní údaje správce, případně údaje pověřence
- / účely zpracování a právní základ zpracování (souhlas, zákon, apod.)
- / oprávněné zájmy správce či třetí strany, pokud jsou základem
- / kategorie příjemců osobních údajů
- / případný úmysl správce předat údaje do zahraničí mimo EU

Je-li to *nezbytné* pro spravedlivé a transparentní zpracování, tak i

- / doba uložení osobních údajů
- / existence práv subjektů, tj. přístup k údajům, jejich opravu či výmaz, omezení zpracování, námitka proti zpracování a na přenositelnost
- / informace o případném právu odvolat souhlas
- / informace o právu podat stížnost u dozorového orgánu
- / poučení, zda je poskytnutí údajů zákonným či smluvním požadavkem a zda je povinné a o možných důsledcích neposkytnutí
- / automatizované rozhodování, informace o takovém postupu

Práva subjektů údajů – GDPR (čl. 15)

Právo na přístup k osobním údajům

Subjekt údajů má právo získat od správce **potvrzení**, zda zpracovává jeho osobní údaje

Pokud ano, má subjekt právo získat **přístup k osobním údajům**

- / je-li to možné, měl by mít správce možnost poskytnout dálkový přístup k bezpečnému systému, který by umožnil přímý přístup k údajům

Současně má subjekt právo získat následující **informace**

- / účely zpracování, kategorie osobních údajů, kategorie příjemců, plánovaná doba uložení, existence práva na opravu, výmaz, omezení zpracování a právo námitky a stížnosti, informace o zdroji údajů a skutečnost, že dochází k automatizovanému rozhodování
- / pokud dochází k předání do třetích států, má právo na informace o vhodných zárukách

Správce na žádost poskytne **kopie údajů**

Zaměstnanci již nyní mají široká práva ve vztahu k přístupu k osobnímu spisu (§ 312 ZP)

Práva subjektů údajů – GDPR (čl. 16, 17)

Právo na opravu

Subjekt údajů má právo aby správce bez zbytečného odkladu opravil nepřesné osobní údaje

- / domníváme se, že (a to ani ve vazbě na zásadu přesnosti) to neznamena, že by zaměstnavatel musel vymazávat neaktuální údaje, třeba z osobních spisů (příjmení, adresy), neaktuální data by ale neměl dále používat (pracovat s nimi)

Právo na výmaz („právo být zapomenut“)

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se jej týkají, a to i údaje zveřejněné (kdy je nutné i informovat ostatní správce, aby údaje vymazali)

- / to neplatí při zpracovávání k plnění právní povinnosti (personálně-mzdová agenda) nebo obhajobu právních nároků (reálných)
- / může jít ale třeba o fotografii na internetu
- / právo se může týkat jen některého z konkrétních účelů (i když ty samé údaje správce musí/může zpracovávat pro jiné účely)

GDPR akcentuje pro případy udělení souhlasu dítětem

Práva subjektů údajů – GDPR (čl. 18, 19)

Právo na omezení zpracování

Subjekt má právo, aby správce omezil zpracování jeho údajů, pokud

- / popírá přesnost údajů, zpracování je protiprávní, údaje již nejsou potřebné nebo pokud vznesl námitku proti zpracování
- / údaje mohou být dále zpracovávány jen se souhlasem, pro obhajobu nároků, pro ochranu práv nebo důležitého veřejného zájmu

Oznamovací povinnost správce vůči příjemcům

Správce oznamuje jednotlivým příjemcům (mzdové účtárně nebo mateřské společnosti), jimž byly osobní údaje zpřístupněny, veškeré opravy, výmazy nebo omezení zpracování (podle čl. 16, 17/1 a 18)

- / to neplatí v případech, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí

Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje

Práva subjektů údajů – GDPR (čl. 20, 21)

Právo na přenositelnost údajů

Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, pokud

- / zpracování je založeno na souhlasu nebo smlouvě a současně se zpracování provádí automatizovaně (sociální sítě, banky)
- / neplatí pro kamerové systémy; co personálně-mzdová agenda?
- / neznamena to automaticky výmaz údajů (čl. 17 je nedotčen)

Subjekt může chtít, aby správce napřímo předal údaje jinému správci

Právo vznést námitku proti zpracování

Subjekt mající konkrétní důvod může namítat zpracování ve veřejném zájmu nebo pro ochranu oprávněných zájmů (kamerový systém)

- / správce může nadále pokračovat jen pokud prokáže, že chráněné zájmy převažují nad zájmy subjektu
- / informace o právu (jde hlavně o marketing) musí být oddělená

Práva subjektů údajů – GDPR (čl. 22)

Automatizované individuální rozhodování

Subjekt údajů má právo **nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování**, včetně profilování, které má pro něho právní účinky či se ho významně dotýká

- / to by se mohlo (spíše teoreticky) týkat třeba automatizovaných hodnotících programů (s přímou vazbou na odměňování) nebo třeba automatizovaných výstupů z GPS v autech (s přímou vazbou na náhradu škody nebo propuštění)
- / překonat to lze jen výslovným souhlasem (pokud nejde o nezbytné zpracování nutné k plnění/uzavření smlouvy nebo povolené zpracování zákonem)
- / při překonání musí správce provést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí

O všech právech (čl. 15-22 + 34) je nutné **informovat subjekty** údajů + je nutné informovat i o (ne)přijatých opatřeních (do *1 měsíce*)

Oznamovací (registrační) povinnost (§ 16 - 19)

- / neplatí u zpracovávání uloženého zvláštním zákonem nebo pokud je osobních údajů třeba k uplatnění zákonných práv a povinností - i tak ale platí povinnost uvést informace na webu
- / není nutná u zpracovávání pro účely pracovněprávního vztahu (naopak, ani nelze registrovat)
- / oznámení je nutné učinit před zahájením zpracovávání, v praxi registrace většinou do 5 dnů

Oznamuje se na on-line formuláři Úřadu, který obsahuje zejména

- / účel (účely) zpracování, kategorie subjektů údajů a osobních údajů
- / popis způsobu zpracování osobních údajů
- / místo zpracování (včetně adresy zpracovatele)
- / příjemce nebo kategorie příjemců, předpokládaná předání údajů do jiných států
- / popis opatření k zajištění ochrany osobních údajů

Předchozí konzultace s Úřadem – GDPR (čl. 36)

Registrační povinnost není v GDPR upravena, GDPR ale zná relativně omezené případy **předchozí konzultace s Úřadem**, pokud

- / z posouzení vlivu na ochranu údajů vyplývá, že by hrozilo u zpracování vyšší riziko, když by správce nepřijal opatření k jejich zmírnění

Pokud se Úřad bude domnívat, že by šlo o protiprávní zpracování údajů (porušující GDPR), zejména pokud správce nedostatečně určil či zmírnil riziko

- / upozorní na to správce (zpracovatele), a to písemně do 8 týdnů (s možností prodloužení o 6 týdnů) od obdržení žádosti o konzultaci
- / může uplatnit některou svou pravomoc (prověřit dále situaci, udělit napomenutí, požadovat nápravu, uložit omezení zpracování apod.)

Při konzultaci musí být Úřadu předloženy specifické informace o zamýšleném zpracování + si Úřad může vyžádat cokoliv dalšího

Lokální právo může požadovat povinné konzultace (a předchozí povolení Úřadu) i v dalších případech

Zabezpečení osobních údajů (§ 13 – 15)

Zaměstnavatel musí přijmout opatření, aby nemohlo dojít k

- / neoprávněnému nebo nahodilému přístupu
- / změně, zničení či ztrátě nebo neoprávněným přenosům
- / jinému neoprávněnému zpracování či zneužití - v praxi:
uzamykatelná kancelář a kartotéka s omezeným přístupem; počítače by měly mít heslo, být zálohovány, antivirová ochrana; u automatizového zpracování by mělo být dohledatelné, kdo, kdy a proč pracoval s údaji (logování)
- / dále musí zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření - není však stanovená sankce
- / zaměstnavatel by měl poučit své zaměstnance, kteří zpracovávají údaje, o povinnosti mlčenlivosti a možných postizích (pokuta 100.000 Kč a možný trestní postih)
- / dle Zákona je nutné uzavřít **písemnou smlouvu se zpracovatelem** (mzdovou účtárnou) podle § 6 - opět ale není stanovená sankce

Zabezpečení osobních údajů - GDPR (kap. IV, čl. 24-43)

Zaměstnavatel musí přijmout opatření k ochraně údajů

- / musejí být revidována a navíc **musí správce doložit soulad s GDPR**
- / GDPR klade důraz na **pseudonymizaci**, která by měla být zvažena zejména při komunikaci s externími poskytovateli služeb (mzdovka)
- / ochrana dat spočívá i v minimalizaci údajů, omezenosti uložení a přístupu k údajům - neměly by být přístupné neomezenému počtu osob bez zásahu člověka
- / při existenci **společných správců** (třeba v rámci jednotného HR systému v rámci skupiny) je nutné transparentně vymezit podíly odpovědnosti za plnění povinností dle GDPR, včetně informování
- / správce bude moci využít jen ty zpracovatele (mzdová účtárna), kteří poskytují dostatečné záruky ochrany údajů
 - dle písemné smlouvy s detailním obsahem, nebo zákona (PLS)
 - zpracovatel musí **umožnit audit** (budou tedy povinné?)
 - jsou použitelné dosavadní standardní smluvní doložky
 - řetězení zpracovatelů není zakázáno - přísnější pravidla

Zabezpečení osobních údajů - GDPR (čl. 32)

Zabezpečení zpracování údajů má zahrnovat mimo jiné (s přihlédnutím ke stavu techniky, nákladům, povaze, rozsahu, kontextu a účelům)

- / pseudonymizaci a šifrování osobních údajů
- / schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- / schopnost **obnovit dostupnost** osobních údajů a přístup k nim včas v případě fyzických či technických incidentů
- / proces **pravidelného testování, posuzování a hodnocení** účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování

Zohlední se i rizika, která představuje zpracování (zejm. náhodné či protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných údajů, nebo neoprávněný přístup k nim) a dodržování schválených **kodexů chování** či uplatňování schválených mechanismů v rámci vydaných **osvědčení**

GDPR výslovně neuvádí povinnost logování, ale i tak ji lze dovodit

Zabezpečení osobních údajů - 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

Zvláštní povinnosti (§ 5/1)

Zaměstnavatel musí

- / stanovit účel, prostředky a způsob zpracování osobních údajů (není nutné písemně)
- / zpracovat pouze přesné osobní údaje (aktualizovat údaje)
- / **shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu**
- / uchovávat údaje pouze **po nezbytnou dobu** (poté likvidace)
- / zpracovávat údaje pouze v souladu s účelem k němuž shromážděny
- / shromažďovat údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti
- / nesdružovat osobní údaje, které byly získány k rozdílným účelům

Zásady zpracování osobních údajů – GDPR (čl. 5)

Správce odpovídá při zpracování za **dodržení těchto zásad**, dle kterých osobní údaje musí být

- / ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (“zákonnost, korektnost a transparentnost“)
- / shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný (“účelové omezení“)
- / přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (“minimalizace údajů“)
- / přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby byly nepřesné údaje *s přihlédnutím k účelům* zpracovávání bezodkladně vymazány či opraveny (“přesnost“)
- / uloženy ve formě umožňující identifikaci subjektů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (“omezení uložení“)
- / zpracovávány způsobem, který zajistí náležité zabezpečení údajů, zejména pomocí vhodných technických či organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (“integrita a důvěrnost“)

Správce musí být schopen toto **dodržení souladu doložit** (“odpovědnost“) 35

Záznamy o činnostech zpracování – GDPR (čl. 30)

Správce vede **písemnou/elektronickou dokumentaci** obsahující

- / specifikace správce a případně i pověřence
- / účely zpracování
- / popis kategorie subjektu údajů a kategorií osobních údajů
- / kategorie příjemců
- / informace o případném předání údajů do třetí země (+ záruky)
- / plánované lhůty pro výmaz jednotlivých kategorií údajů
- / obecný popis technických a organizačních bezpečnostních opatření

Obdobné záznamy vedou i zpracovatelé

Záznamy musí být poskytnuty Úřadu na jeho požádání

Tato povinnost **neplatí pro podniky s méně než 250 zaměstnanci**,
ledaže zpracování

- / pravděpodobně představuje riziko pro práva a svobody subjektů
- / zpracování není příležitostné – což asi dopadá na údaje zaměstnanců
- / zpracování zahrnuje zvláštní kategorie údajů

Posouzení vlivu na ochranu údajů – GDPR (čl. 35)

Posouzení vlivu (tzv. DPIA) je nutné zejména v těchto případech, kdy u zpracování hrozí **vysoké riziko** pro práva a svobody subjektů

- / systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování (nebo vytěžování), a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad - teoreticky systémy hodnocení zaměstnanců/teamů
- / rozsáhlé zpracování zvláštních kategorií údajů
- / rozsáhlé systematické monitorování veřejně přístupných prostorů

Guidelines hovoří i o **monitoringu zaměstnanců** (počítače, internet) a **převodech dat mimo EU**

Další případy má zveřejnit Úřad (seznamy budou koordinovány)

Posouzení budou obsahovat popis a účely zpracování, posouzení nezbytnosti a přiměřenosti, posouzení rizik a opatření k jejich řešení

Podkladem bude případně i stanovisko pověřence a subjektů údajů

Pověřenec – GDPR (čl. 37 - 39)

V ČR **nový institut**, povinný pro zpracování

- / orgány veřejné moci
- / hlavní činnosti správce (zpracovatele) spočívá ve zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů
- / hlavní činnosti správce (zpracovatele) spočívají v rozsáhlém zpracování zvláštních kategorií údajů

Na běžného zaměstnavatele nedopadá (asi i když má pár aut s GPS nebo kamerový systém ve skladu), nejde-li třeba o maloobchodní řetězec, který má kamerové systémy + CRM (newsletterový) systém

Jde o celkem složitý institut

- / GDPR upravuje řadu okruhů, zejm. postavení a úkoly pověřence
- / detailní pravidla pak stanoví (již aktualizované) guidelines (vodítka), který i vypočítává povinné instituce - banky, pojišťovny, operátoři, internetové společnosti, nemocnice, security

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

Sankce podle Zákona (§ 45)

Správní delikt správce nebo zpracovatele

- / nestanoví účel, prostředky nebo způsob zpracování, nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona
- / zpracovává nepřesné údaje
- / shromažďuje nebo zpracovává údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu
- / uchovává údaje po dobu delší než nezbytnou k účelu zpracování
- / zpracovává osobní údaje bez souhlasu subjektu údajů
- / neposkytne informace v rozsahu nebo stanoveným způsobem
- / nepřijme nebo neprovede opatření pro zajištění bezpečnosti údajů
- / nesplní oznamovací povinnost vůči Úřadu

Pokuta do výše 5.000.000 Kč

- / až 10.000.000 Kč hrozí při ohrožení většího počtu osob nebo porušení povinností při zpracování citlivých údajů

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

Značný tlak na jednotnost výkladu GDPR 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“)

Trestněprávní odpovědnost

Neoprávněné nakládání s osobními údaji (§ 180/2 TZ)

Kdo, byť i z nedbalosti, **poruší povinnost mlčenlivosti** tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají

- / lze uložit trest odnětí svobody až na 3 roky (za určitých skutkových okolností až 8 roků)
- / lze spáchat i jen z nedbalosti (není tedy nutný úmysl zpřístupnit osobní údaje)
- / například, pokud pracovník personálního/IT oddělení, který v rámci svého zaměstnání neoprávněně sdělí nebo zpřístupní osobní údaje ostatních zaměstnanců, třeba i kamerový záznam
- / vážnou újmu může být například zesměšnění zobrazené osoby, ztrátu zaměstnání

III. Povinnosti zaměstnavatelů při zaměstnávání osob

- / Přijímání do zaměstnání
- / Trvání pracovního poměru
- / Monitoring zaměstnanců
- / Předávání osobních údajů do zahraničí
- / Skončení pracovního poměru

Přijímání do zaměstnání

- / Nakládání s údaji (životopisy) BĚHEM výběrového řízení
- / Nakládání s údaji (životopisy) PO SKONČENÍ výběrového řízení
- / Vedení databáze životopisů mimo výběrové řízení na volné místo
- / Možné požadované doklady
- / Povinnosti dle zákona o občanských průkazech
- / Povinnosti podle zákona o zaměstnanosti

Nakládání s údaji BĚHEM výběrového řízení

Nakládání s životopisy

- / jedná se o zpracování osobních údajů

Základní povinnosti

- / souhlas zájemců o práci není nutný (navíc jej lze dovodit)
- / informační povinnost vůči zájemcům o práci
- / oznámení Úřadu není nutné (praxe a výklad Úřadu)
- / zabezpečení životopisů

Doporučení: splnit informační povinnost již na webu

Nakládání s údaji BĚHEM výběrového řízení

Omezení dle zákoníku práce

- ✓ požadovat lze pouze údaje související s uzavřením pracovní smlouvy (§ 30/2 ZP) - výklad je nicméně celkem umírněný a stále dává zaměstnavateli právo posouzení vhodnosti zájemce o práci

Omezení dle zákona o zaměstnanosti

- ✓ zaměstnavatel nesmí vyžadovat osobní údaje, které:
 - neslouží k plnění povinností zaměstnavatele
 - informace, které odporují dobrým mravům a
 - informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace

Nejasné, zda lze za “špatné“ otázky uložit pokutu; nepochybně ale za diskriminaci

Nakládání s údaji BĚHEM výběrového řízení

- / s ohledem na daná omezení nelze dělat tzv. background checks (majetek, drogy), není-li pro to zvláštní věcný důvod související s budoucí prací
- / kontrolovat předchozí reference lze (souhlas zájemce není nezbytně nutný)
- / POZOR na poskytování informací po telefonu, ale § 314/2 ZP
- / máme za to, že je možné hledat informace i na internetu (Facebook apod.)

POZOR na obsah vstupních dotazníků - často obsahují zbytečné údaje a někdy i (omylem) citlivé údaje (typicky národnost, kdy ale zaměstnavateli jde o státní občanství)

Možné požadované doklady

Zaměstnavatel může v rámci výběrového řízení požadovat:

- / potvrzení o posledním zaměstnání
- / doklady o dosažené kvalifikaci
- / doklady týkající se administrace mzdy
- / trestní rejstřík, pokud to zákon stanoví nebo je to odůvodněné
- / doklad o zdravotní způsobilosti (nikoliv lékařské zprávy)
- / jiné doklady stanovené zvláštními právními předpisy
- / ...

Vše, u čeho prokáže potřebnost a co bude v souladu s § 316/4 ZP, tedy pokud je pro to dán věcný důvod spočívající v povaze práce a jde o přiměřený požadavek

Nakládání s údaji PO SKONČENÍ výběrového řízení

Doba uchování 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
- / není-li jiná domluva (souhlas zájemce o práci)

Možnost dalšího uchování

- / souhlas neúspěšných zájemců o práci nutný pro případnou další nabídku práce (oslovení)
- / informační povinnost vůči zájemcům
- / oznámení Úřadu (účel: **“vedení databáze zájemců o práci“**)
- / vždy platí povinnost zabezpečení životopisů
- / i při souhlasu musí být doba uschování omezena (obecně na 3 roky)

Vedení databáze životopisů bez konkrétního výběrového řízení

Rovněž se jedná o zpracování osobních údajů

- / povinnosti zaměstnavatele - obdobné jako při uchovávání životopisů po skončení výběrového řízení
- / je vhodné registrovat databázi u Úřadu a obdržet souhlas s uchováváním životopisu (např. vyplněním formuláře s poučením)

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

Povinnosti dle zákona o občanských průkazech

- / zaměstnavatel nesmí pořizovat kopie občanského průkazu bez souhlasu zaměstnance (zájemce o práci)
- / porušení je přestupkem fyzické osoby (nikoliv zaměstnavatele), která kopií bez souhlasu pořídí
- / pokuta (až 10.000 Kč)
- / platí i pro české cestovní doklady (pasy)

Doporučení: Zaměstnanec by měl na kopii napsat rukou souhlas, popřípadě podepsat text souhlasu

- / otázkou je, zda je uchovávaná kopie dokladu nezbytná - nezaznamenal jsem ale v praxi zatím jakýkoliv postih, i když se jedná o činnost proti smyslu (principům) Zákona (i **GDPR**)

Trvání pracovního poměru

- / Omezení požadovat informace
- / Vedení osobního spisu
- / Vedení databáze zaměstnanců, kterým poskytuje zaměstnavatel služby nebo zboží
- / Nakládání s fotografiemi zaměstnanců mimo spisy
- / Whistleblowing Policy

Omezení požadovat informace

- / ZP (§ 316/4) stanoví, že zaměstnavatel nesmí od zaměstnance vyžadovat informace, které bezprostředně nesouvisejí s prací

Zaměstnavatel nesmí vyžadovat informace zejména o

- / těhotenství, rodinných a majetkových poměrech
- / sexuální orientaci
- / původu
- / členství v odborech, členství v politických stranách nebo hnutích
- / příslušnosti k církvi nebo náboženské společnosti
- / trestněprávní bezúhonnosti

“Podtržené“ informace lze vyžadovat, pokud je pro to dán věcný důvod

- / spočívající v povaze práce a je-li tento požadavek přiměřený
- / informace nelze získávat ani prostřednictvím třetích osob

Vedení osobního spisu

Zaměstnavatel je oprávněn vést osobní spis zaměstnance (§ 312 ZP)

- / spis může obsahovat jen písemnosti, které jsou nezbytné pro výkon práce (platí i pro DPP a DPČ)

Jedná se o zpracovávání údajů v rámci zákona (vedení personálně-mzdové agendy):

- / informační povinnost vůči zaměstnancům (všeobecná)
- / dodržovat povinný rozsah a dobu uchovávání údajů
- / zabezpečit ochranu osobních údajů
- / plnit veškeré zvláštní povinnosti podle Zákona

- / i zde platí omezená možnost kopírování průkazů
- / nyní platí již jen velmi omezená povinnost uchovávat na pracovišti kopie pracovních smluv (do nahlášení u sociálky + DPP/DPČ)

Vedení osobního spisu

Obsahem pouze údaje potřebné dle zvláštních předpisů

- / zákona o zaměstnanosti
- / zákoník práce
- / BOZP
- / zákon o ochraně veřejného zdraví
- / zákon o specifických zdravotních službách (PLS)
- / předpisy v oblasti sociálního zabezpečení
- / předpisy v oblasti zdravotního pojištění
- / předpisy v oblasti daně z příjmů
- / ...

Jde o zpracování v rámci zákona (personálně-mzdová agenda), není tedy nutný

- / souhlas zaměstnance ani oznámení (registrace) Úřadu

Vedení osobního spisu

Obsah - údaje získané ze vstupního dotazníku

- / identifikační a adresní údaje zaměstnance
- / nařízené srážky ze mzdy (každý zaměstnavatel je dle § 294/1 OSŘ povinen si vyžádat potvrzení o srážkách)
- / jméno a kontakt na manžela/ku, popř. děti či rodiče pro případ úrazu/smrti
- / údaj o zdravotní pojišťovně zaměstnance
- / přehled o předchozích zaměstnáních včetně zápočtový list, popř. pracovního posudku
- / údaje o dosažené kvalifikaci a o jazykových znalostech (fotokopie příslušných vysvědčení) (nutné např. pro nabídku jiné vhodné práce při odvolání z vedoucího místa, reportování státním úřadům)
- / číslo bankovního účtu (pokud domluva o úhradě mzdy převodem)
- / ...

Vedení osobního spisu

Obsah - údaje související s pracovním poměrem

- / údaje ohledně odměňování včetně údajů o odměnách, bonusech (např. z důvodu výpočtu průměrného výdělku)
- / informace/souhlas se zpracováváním osobních údajů
- / informace o tom, do jaké kategorie byla zařazena zaměstnancova práce
- / informace o zdravotnickém zařízení poskytujícím preventivní péči
- / potvrzení o školeních v oblasti BOZP absolvovaných zaměstnancem
- / potvrzení o seznámení s pracovním řádem, předpisy, kolektivní smlouvou
- / údaje o případných pracovních úrazech a nemocech z povolání
- / údaje o disciplinárních řízeních (upozornění a výzvy, jejich řešení)
 - vše slouží k plnění povinností zaměstnavatele

Vedení osobního spisu

Obsah - údaje související s pracovním poměrem

- / pracovní smlouva a její změny (jmenovací dekret a manažerská smlouva), další informace o pracovním poměru (§ 37 ZP)
- / další dokumenty (dohoda o odpovědnosti, o zvýšení kvalifikace apod.)
- / potvrzení o zdravotní způsobilosti zaměstnance (lékařské prohlídky)
- / údaje o dovolené, náhradním volnu
- / evidence pracovní doby, práce přesčas, pracovní pohotovosti a noční práce
- / údaje o mateřské/rodičovské dovolené a dalších překážkách v práci
- / ...
 - vše slouží k plnění povinností zaměstnavatele

Vedení osobního spisu

Obsah - údaje související s pracovním poměrem

- / potvrzená přihláška k OSSZ, zdravotní pojišťovně, dani z příjmů
- / mzdový list
- / evidenční list důchodového pojištění
- / údaje ohledně odměňování včetně údajů o odměnách, bonusech (např. z důvodu výpočtu průměrného výdělku)
- / informace o rodinných příslušnících kvůli daňovým konsekvencím
- / roční zúčtování daně z příjmů
- / ...
 - u větších společností součástí mzdového spisu - při rozdělení by neměly být obě složky spisu přístupné všem

Vedení osobního spisu

Nahlédnutí do spisu je dle § 312 ZP umožněno pro:

- / nadřízení vedoucích zaměstnanců
- / 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 vedoucích, 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?
- / lze tímto právem bránit přemístění spisů do jiné budovy či země?

Vedení databáze zaměstnanců, kterým poskytuje zaměstnavatel služby nebo zboží

Není zvláštní právní úprava týkající se zaměstnanců, platí

- / obecné principy týkající se databáze zákazníků – postavení zaměstnance není z pohledu osobních údajů relevantní

Nutné splnit následující povinnosti (stejně jako u “obyčejných“ zákazníků):

- / informační povinnost
- / oznámení Úřadu není nutné (dle praxe Úřadu; pokud nedochází například k zasílání nabídek služeb/zboží v rámci marketingu)
- / zabezpečení databáze - limitovaný přístup, **nesdružování s osobním spisem zaměstnanců**
- / veškeré další povinnosti dle Zákona (GDPR)
- / souhlas zaměstnanců není nutný, pokud je zpracování nezbytné pro plnění smlouvy (poskytnutí úvěru)

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
 - informační povinnost
 - oznámení Úřadu (účel: “**podpora komunikace**“), vhodné pamatovat i na marketingové materiály (fotky z akcí/teambuildingu)
 - veškeré další povinnosti dle Zákona (GDPR)
- / otázkou je, zda z pohledu ZP nemůže jít o legitimní požadavek
- / 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

Whistleblowing Policy

- / implementace pravidel pro hlášení podezřelých okolností ve finanční oblasti (zejm. účetnictví, audit), založených na tzv. „SOX zákonu“ v USA
- / většinou telefonní nebo emailová linka provozovaná zahraniční firmou
- / na Slovensku od roku 2015 povinná u zaměstnavatelů s 50 a více zaměstnanci

Povinnosti zaměstnavatele, byť přímo neprovozuje:

- / oznámení Úřadu (jde o samostatný účel „Whistleblowing Policy“)
- / souhlas zaměstnanců není nutný
- / nutné split informační povinnost
- / projednání s odborovou organizací (působí-li u zaměstnavatele)
- / veškeré další povinnosti dle Zákona (zabezpečení zjištěných dat)

Monitoring zaměstnanců - úvod

Monitoring zaměstnanců je **stále aktuální téma**

GDPR může spojit s permanentním monitoringem nové povinnosti (pověřenec, povinné posouzení vlivu)

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

Není ani dostatek dalších zdrojů informací a vodítek jak postupovat

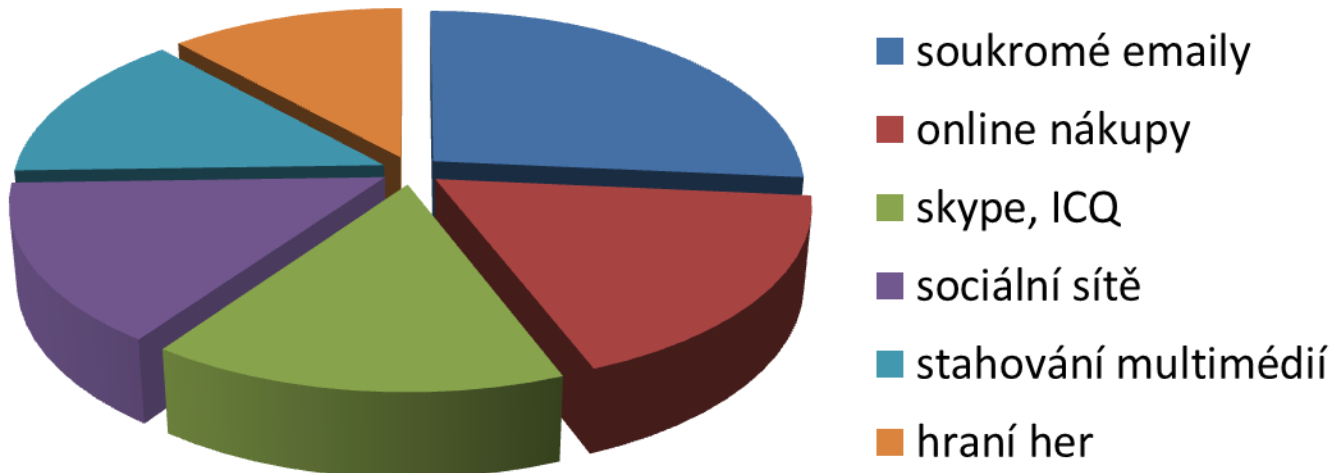
Obecně jde o sledování zaměstnanců, jejich aktivit a činností, typicky

- / monitoring emailů
- / 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

Listina základních práv a svobod

Ústavní práva zaměstnanců

- ✓ Čl. 7 - Nedotknutelnost osoby a jejího soukromí je zaručena.
- ✓ Čl. 10 - Každý má právo na ochranu před neoprávněným zasahováním do soukromého života. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.
- ✓ Čl. 13 - Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Ústavních práv se nelze vzdát a lze je omezit jen na základě zákona

Listina základních práv a svobod

Ústavní práva zaměstnavatelů

- / Čl. 11 - Každý má právo vlastnit majetek.
- / Čl. 26 - Každý má právo podnikat a provozovat jinou hospodářskou činnost.

Tato práva mohou stát proti právům zaměstnanců - v každém konkrétním případě je nutné provést test proporcionality a určit, které právo má přednost

Zákoník práce

§ 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 zaměstnavatele
- ✓ i když u zaměstnavatele platí absolutní zákaz, je nutné respektovat například přijatou emailovou poštu zaměstnance
- ✓ doporučuji stanovit základní pravidla pro soukromé použití (zejm. omezený rozsah, plnění pracovních povinností, vyloučení škody zaměstnavatele a neporušení jakýchkoliv povinností a práv)
- ✓ vhodné informovat o provádění přiměřené kontroly (prevence zneužití)

Zákoník práce

§ 316/2 ZP

Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorech 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 a povaha činnosti by měla mířit spíše na činnost zaměstnance
 - obecné použití; existují výklady, dle kterých se toto ustanovení týká výlučně soukromé komunikace zaměstnance, např. ze soukromého mobilu nebo soukromých emailů

Zákoník práce

§ 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.

- / nová úprava (od 2007) - zatím není mnoho judikatury ani článků
- / 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

Zákoník práce

- / ze zákoníku práce vypadlo (od 2007) ustanovení

Zaměstnavatel je povinen soustavně kontrolovat, zda zaměstnanci plní své pracovní úkoly tak, aby nedocházelo ke škodám (§ 170/2 ZP č. 65/1965 Sb.)

- / přesto je zaměstnavatel odpovědný za škodu způsobenou jeho zaměstnanci
- / nicméně je povinností všech vedoucích zaměstnanců řídit a kontrolovat práci podřízených zaměstnanců (§ 302 ZP) a připomínáme, že plnění povinností se mimo jiné neregistruje u Úřadu ani nepodléhá souhlasu subjektu údajů
- / dle rozličných vyjádření MPSV a Úřadu však není možné “soustavné sledování zaměstnanců za účelem kontroly plnění pracovních povinností“

Zákon o ochraně osobních údajů

- / součástí ochrany soukromí je i ochrana v oblasti osobních údajů upravená tímto zákonem a kontrolovaná Úřadu
- / přesto monitoring (např. přečtení emailu) není zpracováním osobních údajů; může to ale být porušením soukromí
- / ani Úřad není přitom jednotný v tom, zda nakládání s určitými výstupy (např. vypracování zprávy o tom, jak zaměstnanec nakládá s emaily) je zpracováním osobních údajů, zejména, zda jde o systematické zpracování nebo jen nahodilé shromažďování
- / pokud by šlo o zpracování osobních údajů, bylo by nutné splnit veškeré povinnosti dle tohoto zákona (včetně třeba registrace u Úřadu)
- Zákon neobsahuje specifickou úpravu monitoringu
- / hrozily by také vysoké pokuty (teoreticky až 10.000.000 Kč), a to teoreticky i vedle postihu od Inspekce práce

Zákon o inspekci práce

- / zatím zákon neumožňuje postih zaměstnavatele
- / 94 podnětů v 2014 - zanedbatelný počet (4000 podnětů na odměňování); “porušení“ (zejm. kamerové systémy) - předání Úřadu
- / legislativním procesem ale prošla novela, která zavádí nový přestupek na úseku ochrany soukromí a osobních práv zaměstnanců

VELKÝ PROBLÉM - (deklarovaný) striktní přístup inspekce, kdy ani řádně registrovaný kamerový systém prý nemusí obstát

Zaměstnavatel se dopustí správního deliktu tím, že

- / bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele neplní povinnost podle § 316/2 ZP a **narušuje soukromí zaměstnance** na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, ... (pokuta až 1.000.000 Kč)
- / v rozporu s § 316/3 ZP **nesplní informační povinnost** o rozsahu kontroly a o způsobech jejího provádění (pokuta až 100.000 Kč)

Trestní zákoník

Upozornění na možný trestněprávní postih (až 2 roky vězení)

TČ "porušování tajemství dopravovaných zpráv" (§ 182/1 TZ)

- např.: pracovník IT oddělení přečte soukromý e-mail zaměstnance = úmyslně poruší tajemství emailové zprávy

TČ "prozrazení a využití tajemství dopravovaných zpráv" (§ 182/2 TZ)

- např.: pracovník HR sděluje obsah soukromého emailu o nemoci zaměstnance jeho kolegům, aby poškodil jeho pověst = kdo v úmyslu způsobit jinému škodu prozradí tajemství, o němž se dozvěděl z emailové zprávy, která nebyla určena jemu, nebo kdo takového tajemství využije

Email je ale dopravovanou zprávou jen do okamžiku dojití na server adresáta

Monitoring emailů

Stanovisko Úřadu č. 2/2009

- / Úřad zastává striktní postoj ve prospěch zaměstnance (zástupci Úřadu jsou v rámci seminářů přístupnější)

Připouští:

- / sledovat počet došlých a odeslaných emailů prostřednictvím firemní e-mailové adresy, případě jejich hlavičky (vznikne-li podezření na zneužití prostředků zaměstnavatele)
- / číst soukromý e-mail zaměstnance může pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail (např. vyřízení emailu v době dlouhodobé nemoci) - nezmiňuje jiné případy (podezření apod.)

Nepřipouští:

- / sledování a zpracovávání obsahu korespondence (sporné, neboť samotné čtení emailů není zpracováváním osobních údajů, ale může jít o ochranu přepravovaných zpráv)

Inspektoráty práce se s tím patrně ztotožňují - manuál ale hovoří o “osobních“ emailech

Monitoring emailů

Dle našeho názoru je ad hoc kontrola obchodní komunikace možná

- ✓ **stanovení podmínek použití emailu** ve společnosti; asi ne absolutní zákaz - vždy ale omezeně při splnění svých povinností a úkolů a bez vzniku škody, dalších nákladů a porušení jakýchkoliv předpisů a práv
 - nutno aplikovat na všechny zaměstnance
- ✓ **přiměřený (omezený) rozsah** - nahodilé zpracování, resp. namátkové kontroly rozsahu emailu - plnění podmínek dle § 316/1 ZP
 - POZOR na dostupný software - ten by měl mít za úkol (ideálně skutečně) jen (hlavně) ochranu systému (viry, spamy, stahování dat)
 - čtení zpráv pouze při konkrétním podezření ze zneužití (nemoci)
- ✓ splnění informační povinnosti (nad rámec § 316/3 ZP) vůči zaměstnancům a odborům vyhlášením vnitřní směrnice po projednání s odbory (jsou-li) s uvedením možné kontroly i čtení (při podezření)
- ✓ souhlas zaměstnance není nutný (asi není vhodné o něj žádat)
- ✓ oznámení Úřadu sporné (nahodilé/systematické; resp. lze podřadit pod základní personálně-mzdové zpracování) - spíše nedoporučuji

Monitoring použití internetu

Stanovisko Úřadu č. 2/2009

- / úřad zastává striktní postoj ve prospěch zaměstnance (zástupci Úřadu jsou v rámci seminářů přístupnější)

Připouští:

- / 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“
- / jinak nelze, byť není dotčeno právo zaměstnavatele postihnout zaměstnance za nevyužívání pracovní doby a svěřených prostředků

Manuál **inspekce práce** nepřipouští kontrolu obsah navštívených webových stránek, ale zaměstnavatel může být informován o celkovém stráveném čase na internetu

Monitoring použití internetu

Rozhodnutí Nejvyššího soudu (21 Cdo 1771/2011, 16.8.2012)

- / zaměstnanec v září 2009 v rámci pracovní doby strávil přes 102 hodin prohlížením internetu (bez vazby na výkon práce)
- / zaměstnavatel provedl kontrolu - **nasadil software monitorující činnost zaměstnance** - a uvedené porušení povinností zjistil a se zaměstnancem okamžitě zrušil pracovní poměr
- / soud potvrdil, že bez souhlasu zaměstnavatele nelze využívat jeho výrobní prostředky (výpočetní techniku) a že v pracovní době se má zaměstnanec věnovat plnění pracovních úkolů
- / soud také uvedl, že **dodržování povinností může zaměstnavatel v přiměřené míře kontrolovat** (dle § 316/1 ZP), nesmí však nad rozumnou míru zasahovat do výkonu práce zaměstnance ani do jeho soukromí
- / okamžité zrušení bylo posouzeno jako platné
- / obdobné rozhodnutí i ohledně kontroly soukromých telefonátů (21 Cdo 747/2013, 7.8.2014) - neřeší nicméně aspekt soukromí

Monitoring použití internetu

Dle našeho názoru je monitoring možný za splnění povinností:

- / **stanovení podmínek použití internetu**; asi ne absolutní zákaz - vždy ale při splnění svých povinností a úkolů a bez vzniku škody, nákladů a porušení jakýchkoliv předpisů a práv
 - nutno aplikovat na všechny zaměstnance
- / **přiměřený (omezený) rozsah kontroly** plnění § 316/1 ZP
 - důraz na prevenci (blokování) spíše než na (průběžnou/ neomezenou) kontrolu, možnost evidence strávené doby, nikoliv profilování
- / splnění informační povinnosti (nad rámec § 316/3 ZP) vůči zaměstnancům a odborům vyhlášením vnitřní směrnice po projednání s odbory (jsou-li) - zmínit možnost kontrol
- / souhlas zaměstnance není nutný (lze jej nicméně doporučit)
- / oznámení Úřadu sporné (nahodilé/systematické; resp. kontrolu lze podřadit pod základní personálně-mzdové zpracování) - spíše nedoporučuji

Stanoviska a doporučení Pracovní skupiny dle článku 29

- ✓ skupina (označovaná jako WP 29), tedy zástupci národních úřadů (Úřadu) má klíčovou roli v oblasti osobních údajů (a tedy i monitoringu)
 - sjednocuje výklad a dává odborná stanoviska a doporučení

Working document on the surveillance of electronic communications in the workplace (tzv. WP 55) ze dne 29.5.2002

- ✓ dokument uceleným způsobem řeší možný monitoring 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 - stanovisko č. 8/2001, o zpracování osobních údajů v kontextu zaměstnání, ze dne 13.9.2001 (zmíněné Úřadem ve stanovisku č. 2/2009)

Kamerový systém

Zavedení kamerového systému = zpracování osobních údajů, pokud

- / je uchováván záznam - nejde jen o průběžný systém, a
- / lze identifikovat zaznamenané osoby, byť za pomoci policie - o zpracování osobních údajů jde i tehdy, pokud některé osoby ztotožnit nelze (např. z důvodu špatných světelných podmínek nebo s ohledem na oblečení zaznamenané osoby)
- / nejedná se o zpracování citlivých osobních údajů, i když je či může být ze záznamu zřejmý rasový původ zaznamenaných osob; to platí za předpokladu, že zaměstnavatel se záznamem dále nenakládá z tohoto pohledu

Kamerový systém je současně vnímán jako **opatření narušující soukromí zaměstnanců**, tedy opatření spadající do režimu § 316/2 ZP

- / takové opatření je možné dle textu zákoníku práce jen při existenci *závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele*

Kamerový systém – dvojí úprava

Na kamerové systémy dopadá ZP i Zákon

- / oba režimy přitom nejsou shodné (i kamerový systém bez záznamu je narušením soukromí)
- / není ani jasná vazba mezi nimi (úprava zákoníku práce je speciální a má přednost)
- / doposud je důležitější oblast osobních údajů (tj. působnost Úřadu), protože inspektoráty zatím nesankcionují porušování zákoníku práce
 - Úřad má i stanoviska a další podklady ke kamerovým systémům
 - existuje i několik rozhodnutí soudů, která se týkají pokut uložených Úřadem - jeho přístup je již znám a je celkem benevolentní
- / inspekce práce každopádně nebude posuzovat (a trestat) například, jak je zabezpečen kamerový záznam (to je již čistě zpracování osobních údajů) a patrně ani následné použití záznamu
- / i nadále tak **bude třeba mít pod kontrolou obojí režim**, jen možná důležitost úpravy zákoníku práce bude minimálně stejné důležitá jako oblast osobních údajů, zejména pokud jde o rizika postihu

Podmínky platnosti kamerového systému

Nutno sledovat jak úpravu Zákona, tak i ZP

- / platný kamerový systém, tedy systém realizovaný plně v souladu se zákonem, je podmínkou možnosti řádného použití záznamu
- / jinak hrozí, že třeba propuštění zaměstnance založené výlučně na kamerovém záznamu (krádež v noci) nemusí být v pořádku - nemusí být “ustáto“ u soudu při jeho napadením zaměstnancem
- / nejsou nicméně zcela jasná pravidla a vodítka, a i soudy někdy uvádějí, že třeba neregistrovaný kamerový systém neznamena automaticky nepoužitelný záznam coby důkaz
- / každý aspekt (propuštění, posouzení inspekcí práce a Úřadem) může mít vlastní, odlišný, režim a dopad
 - například propuštění může být posouzeno jako platné, ale inspekce práce nebo Úřad uloží pokutu za porušení ZP či Zákona
 - nebo naopak, případně může být závěr vždy negativní

Přístup inspekce práce ke kamerovým systémům

Dosavadní známé výklady inspekce práce k § 316/2 ZP

- / vycházíme především z manuálu SÚIP (dostupného na www.suip.cz), který je velice kusý a striktní (striktnější, než dosavadní přístup Úřadu)
- / zvláštní povaha činnosti zaměstnavatele je dána např. u vězeňské služby, na pokladnách čerpacích stanic, na pokladnách bank, na policejních služebnách apod.
- / zvláštní povaha činnosti zaměstnavatele však nezahrnuje uplatňování takových práv zaměstnavatele, jako např. ochranu majetku, zdraví, bezpečnosti zaměstnanců, dodržování technologie, prevence apod.
- / rovněž nelze přisvědčit argumentaci zaměstnavatelů, že uplatnění jejich práv nelze zabezpečit jiným způsobem nežli kamerovým systémem (tzv. princip proporcionality)
- / závažný důvod není zpravidla dán při výrobě běžných výrobků nebo při poskytování běžných služeb; je ale potřeba hodnocení vztáhnout ke konkrétnímu pracovišti a konkrétnímu zaměstnavateli
- / zavedení kontrolního mechanismu v rozporu se ZP bude možné postihnout pokutou až 1.000.000 Kč

Oznamovací povinnost Úřadu

Každý kamerový systém, dochází-li ke zpracování osobních údajů, je nutné oznámit Úřadu (jakožto **samostatný účel**)

- / zaměstnavatel je povinen oznámit zpracovávání Úřadu; musí uvést:
 - účel monitoringu - standardně ochrana majetku a zdraví (není možné (pouze) ke kontrole práce)
 - rozsah monitoringu (není možné v soukromých prostorách)
 - dobu uchovávání záznamu (musí být co nejkratší (v řádu dnů), zaměstnavatel musí umět odůvodnit, jinak hrozí neregistrace/sankce)
 - způsob splnění informační povinnosti
 - způsob zajištění před zneužitím
- / oznámení negarantuje plný soulad se Zákonem - je to spíše jen formalita, při které je nicméně vždy zapojen pracovník Úřadu
- / oznámení je nutné změnit/doplnit při změnách systému (navýšení počtu kamer), byť to Zákon výslovně neuvádí

Souhlas zaměstnanců s kamerovým systémem

Souhlas zaměstnanců není nutný - § 4/2 písm. e) Zákona

- / zpracování *nezbytné* pro ochranu práv a chráněných zájmů správce (zaměstnavatele) či jiné dotčené osoby; takové zpracování však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromí
- / dosud s tím není problém (potvrzení registrace systému Úřadem)
- / otázkou je přístup inspekce práce v budoucnosti, pokud jde o narušení soukromí zaměstnanců
- / **dle našeho názoru by se měl Zákon (§ 4/2 písm. e)) vykládat v souladu s § 316/2 ZP umožňující sledování zaměstnanců - kamerový systém za určitých podmínek**
- / takové podmínky jsou buď dány a kamerový systém lze implementovat bez souhlasu zaměstnanců, nebo dány nejsou a souhlas nepomůže

Informační povinnost ohledně kamerového systému

Splnění informační povinnosti vůči zaměstnancům (a dalším zaznamenaným osobám) - § 11 Zákona

Neplatí zvláštní úprava, povinná informace tak musí být kompletní s tím, že ji lze rozdělit na tabulky a dodatečnou písemnou informaci

Požadavky Úřadu na **tabulky** jsou následující

- / tabulky by měly upozorňovat na kamery před vstupem do monitorovaného objektu nebo prostor (v každém případě před záběrem kamery umístěné uvnitř objektu/prostoru)
- / tabulky musí být umístěny po celou dobu provozu systému
- / tabulky musí být dobře viditelné - musí být nepřehlédnutelné
- / text (i piktogram) musí být viditelný/čitelný i z větší vzdálenosti (2-5 m)
- / nestačí pouze piktogram (a text o monitoringu), ale tabulka by měla obsahovat i identifikaci správce (firma a IČO) a odkaz na zdroj, kde lze získat kompletní informaci (jméno osoby, vrátnice, telefonní číslo, email apod.)

Informační povinnost ohledně kamerového systému

Splnění informační povinnosti vůči zaměstnancům (a dalším zaznamenaným osobám) - § 11 Zákona

Požadavky Úřadu na tabulky jsou následující

- / identifikace správce i odkaz na zdroj informace musí být přesné a jasné, musí být možná i kontrola na webu Úřadu (registr správců)
- / pokud jsou v objektu pravidelně přítomny slabozraké či slepé osoby, měl by zde být i zvukové oznámení, speciální druh písma apod.
- / lze zvážit i cizí jazykovou mutaci, pokud se zde vyskytují zahraniční osoby
- / drobné nedostatky by neměly být trestány pokutou a neměly by znemožnit použití záznamu; i tak je vhodné být plně v souladu s požadavky



Informační povinnost ohledně kamerového systému

Splnění informační povinnosti vůči zaměstnancům (a dalším zaznamenaným osobám) - § 11 Zákona

Požadavky Úřadu na **kompletní informaci** o kamerovém systému a právech subjektů údajů podle § 12 a 21 Zákona

- / informace by měla být v textové podobě na webu a měla by být případně i zasílána na základě žádosti
- / informace by měla být lehce dostupná minimálně po dobu, kdy je objekt/prostor přístupný subjektům údajů (otevírací/pracovní doba)
- / informace by měla být dostupná po celou dobu zpracovávání údajů - provozování systému
- / informace by měla být aktualizovaná

Informační povinnost ohledně kamerového systému

Splnění informační povinnosti vůči zaměstnancům (a dalším zaznamenaným osobám) - § 11 Zákona

Požadavky Úřadu na obsah **kompletní informace**

- / účely zpracovávání
- / rozsah zpracování - kamerový systém se záznamem
- / identifikace správce - opět firma a IČO + sídlo
- / identifikace zpracovatele, pokud byl pověřen správcem provozováním
- / místo/místa zpracování (adresy), i kde se nakládá se záznamem
- / příjemce/kategorie příjemců záznamu - např. policie a další orgány
- / počet kamer a popis jejich umístění, případně schémata
- / doba uchovávání záznamu, vč. způsobu mazání (přepis ve smyčce)
- / režim fungování systému - nepřetržitý, detekce pohybu, pracovní doba
- / kontaktní údaje pro přijímání žádostí/stížností dle § 12 a 21 Zákona

Kamerový systém

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 nezbytný, pokud slouží k ochraně práv zaměstnavatele či jiné osoby), informační povinnost a nutnost registrace u Úřadu
- / v případě zvažované implementace spíše doporučuji **metodiku Úřadu** (<https://www.uoou.cz/metodicka-doporuceni/ds-3178/archiv=0>) - ta se nicméně nyní přepracovává a měla by být flexibilnější
- / v praxi ohledně kamerových systémů příliš problémů není - standardně se registrují k ochraně majetku, typicky ve skladech, kolem areálu apod.
- / uvidíme, jaký bude přístup inspektorátu práce (dřívější manuál je striktní)

Soudní judikatura ohledně kamerových systémů

Rozhodnutí Městského soudu v Praze (8A 182/2010, 2.9.2014)

- / zamítnutí žaloby firmy ohledně uložení pokuty Úřadu 100.000 Kč
- / důvodem byla porušení Zákona v souvislosti s kamerovým systémem v prodejnách - vždy 1 kamera snímající prodejní pult a pokladnu pořizovala snímek každých 10 vteřin, které se uchovávaly 1 rok na CD
- / účel byl ochrana majetku firmy, prevence krádeže a kontrola otevírací doby, monitorování pracovní doby a rozložení pracovní doby
- / soud dovodil, že se jedná o **nepřiměřený zásah do soukromí** (k danému účelu by postačovaly čipové karty, resp. snímání vstupu), navíc v rozporu s dílčím účelem (krádež nelze zjistit danou kamerou)
- / i doba uchovávání (všech) snímků není v souladu se Zákonem
- / byly dovozeny i nedostatky v informování o systému
- / kamerový systém nebyl ani registrován (omylem při (ne)odeslání), což ale dle soudu automaticky neznamená nepoužitelnost záznamu
- / **zavedení každého systému je nutné řádně zvážit a provést**

Soudní judikatura ohledně kamerových systémů

Rozhodnutí Nejvyššího správního soudu (1As 113/2012, 25.2.2015)

- / provozovatel kamerového systému na soukromém domě dostal pokutu 1.500 Kč, že bez souhlasu zabírá i ulici a vchod do sousedního domu, navíc neposkytl informaci a neohlásil systém Úřadu
- / soud dal za pravdu provozovateli, že systém byl nezbytný k ochraně jeho majetku a zdraví jeho i členů rodiny a že zásah do soukromí ostatních byl nevýznamný (v porovnání s důležitostí práv provozovatele)
- / důvodem bylo, že systém implementoval až po několika letech marného boje s vandaly a násilníky a že systém pomohl útokům (byť 2 pachatelé byly shledáni nevinnými z důvodu neztotožnění)
- / na druhou stranu porušil povinnost informační i registrační, za což ale dle soudu nelze provozovatele potrestat, protože právní úprava EU je nejasná a i správní praxe Úřadu je celkově nekonzistentní

Každý případ je nutné posuzovat individuálně

Záznamy telefonních hovorů

- / účelem je obchodní monitoring (zlepšování služeb) nebo potřeba pro uzavření/plnění/změnu smlouvy; mělo by tak jít o obchodní hovory
- / **stanovisko Úřadu č. 5/2013** - nutno odlišovat oba účely i skupiny subjektů údajů (zaměstnanci + zákazníci)

Obchodní monitoring

- / souhlas (potenciálních) klientů nutný, zaměstnanců nikoli (§ 5/2e)
- / oznámení Úřadu nutné

Nezbytné zpracování pro smluvní vztahy

- / souhlas zaměstnanců ani zákazníků není nutný (výjimky dle Zákona)
- / oznámení Úřad nevyžaduje

Společné pro oba účely

- / informační povinnost - platí vůči oběma skupinám subjektů
- / veškeré další povinnosti dle Zákona (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 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 (dle Zákona) je nicméně vhodné zmínit v rámci směrnice, která by řešila pravidla (zákazy) pro použití firemního vybavení
- / opět nedoporučuji absolutní zákaz, když realita je jiná, zejména pokud jde o soukromé fotografie a hudbu
- / kontrola by měla být příležitostná, časově omezená a decentní
- / kontrolu bych si dovolil považoval za součást personálně-mzdového zpracování, tedy bez nutnosti registrace u Úřadu a bez nutnosti mít souhlas zaměstnanců

Předávání osobních údajů do zahraničí

Správa HR záležitostí v rámci skupiny

- / v praxi je často po zaměstnavatelích vyžadováno předávání osobních údajů do zahraničí ze strany mateřské společnosti
- / údaje obvykle vyžaduje centrální vedení korporace, které s nimi pracuje obdobně jako lokální zaměstnavatel
- / předání osobních údajů (resp. jejich další zpracování) jde většinou nad rámec povinného zpracování zaměstnavatelem - není nezbytné, přestože se týká již zpracovávaných údajů, jde o jiný samostatný účel (Úřad nemá jednoznačný přístup)
- / účelem často **správa HR záležitostí v rámci skupiny**
- / zaměstnanci by tedy měli dát souhlas (nikoli s předáním, ale s celým zpracováním)
- / zaměstnanci by měli být informováni o předání
- / problematičnost při ukládání na serveru přístupném z jiných míst
- / není ani jasné postavení českého zaměstnavatele (ten je sice správce, ale pro jiný účel a v tomto případě je spíše jen "sběrným místem", tedy zpracovatelem)

Outsourcing činností zaměstnavatele

- / jinou formou spolupráce může být případ, kdy český zaměstnavatel pověří jinou společností (často sesterskou ve skupině), aby pro něj realizovala některé činnosti, typicky v rámci personálně-mzdové agendy
- / je-li to v rámci EU, je to stejná situace, jako kdyby poskytovatel služeb byla česká společnost
 - tj. je nutné o tom informovat zaměstnance, jejich souhlas ale není povinný (pokud jde o plnění zákonných povinností)
 - a neplatí ani žádné povinnosti vůči Úřadu

Předání limitovaného objemu dat pro “statistické“ účely dle současné praxe Úřadu souhlasu ani oznámení nepodléhá

- / i **GDPR** (recitál 48) zmiňuje možnost existence oprávněného zájmu zaměstnavatele, který je součástí korporace, na předání osobních údajů zaměstnanců v rámci skupiny podniků pro vnitřní administrativní účely

Výše uvedené principy platí i při předávání údajů v rámci ČR

Povinnosti vůči Úřadu

- ✓ obecně je k předání údajů do zahraničí mimo EU nutné povolení - předchozí souhlas s předáním

Není nutné:

- ✓ stejné postavení jako země EU mají i další státy EHP, Švýcarsko, Kanada + další státy "schválené" Komisí EU
- ✓ předání do v USA společnosti certifikované v rámci tzv. "Safe Harbor" - POZOR, Soudní dvůr Evropské unie zrušil 6.10.2015 příslušné rozhodnutí Komise - nově nahrazeno The EU-U.S. Privacy Shield
- ✓ pokud je uzavřena smlouva obsahující standardní smluvní doložky (smluvně zabezpečena ochrana údajů) nebo platí ve skupině závazná vnitropodniková pravidla (BCR) – mělo by platit i dle GDPR

Pokud předání (nakládání s údaji) není povinným zpracováním, oznámení (registrace) Úřadu nutné

Skončení pracovního poměru

- / Vedení osobního spisu
- / Oprávnění uchovávat osobní údaje pro případ sporu
- / Povinnost uchovávat určité osobní údaje na základě zvláštních zákonů

Vedení osobního spisu

Dochází ke změně účelu zpracování; vedení již není nezbytné pro administraci personálně-mzdové agendy

Povinnost uchovávat určité dokumenty

- / Zákoník práce neobsahuje žádnou úpravu - od 2007 ani neplatí, že jsou zaměstnavatelé povinni zaměstnanci vydat (vracet) písemnosti týkající se jeho osobních údajů
- / zvláštní předpisy (např. sociální zabezpečení, daň z příjmů)
- / jinak likvidace - zničení, vymazání, trvalé vyloučení ze zpracování

Možnost uchování údajů

- / pro účely ochrany práv pro případ eventuálního sporu, nebo (spíše výjimečně)
- / nabídky dalšího zaměstnání zaměstnanci (nutno mít souhlas)
- / pozor ale na analogické rozhodnutí Městského soudu ohledně uchování listin po skončení výběrového řízení

Oprávnění uchovávat osobní údaje (spisy) z důvodu ochrany pro případ sporu

Uchovávání spisů pro ochranu zaměstnavatele - svébytný účel zpracovávání

- / promlčení peněžitých nároků ve lhůtě 3 let (pozor na doručování soudem, které může trvat několik dalších měsíců)
- / rozsah uchovávaných osobních údajů musí být omezen na účel zpracování, tj. pro eventuální soudní spor
 - mělo by dojít k probírce spisu a
 - ponechání jen důležitých a potřebných dokumentů
- / souhlas není nutný - je to nezbytné pro ochranu práv zaměstnavatele
- / oznámení Úřadu se v praxi nepodává
- / pokud širší rozsah než u povinně uchovávaných písemností, musí být po uplynutí 3 (4?) let zlikvidovány - dle našich informací Úřad akceptuje delší lhůty dle interního skartačního řádu, byť ve svém názoru na webu nepřipouští uchovávání dat jen s odkazem na možné soudní řízení

Povinnost uchovávat určité osobní údaje na základě zvláštních zákonů

- / mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění (originály, 30/10 kalendářních roků)
- / evidenční listy důchodového pojištění (stejnopisy, 3 kalendářní roky)
- / záznamy o poživatelích důchodu (10 kalendářních roků)
- / doklady o druhu, vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a nemocech z povolání a záznamy o evidenci pracovní doby (30 kalendářních roků; 10 u poživatelů důchodu)

/ ...

tzv. **zásadní dokumenty o zaměstnaneckých záležitostech**, které musely být uchovávány i soukromými subjekty, “vypadly“ ze zákona o archivnictví v roce 2009

Povinnost předkládat archívu **osobní spisy významných osobností** politického, hospodářského, vědeckého, technického, kulturního, náboženského, církevního a sportovního života nyní na soukromé subjekty nedopadá (s výjimkou osob zřízených/založených územními samosprávnými celky)

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



CHAMBERS
EUROPE
AWARDS
for Excellence
2014
WINNER

CHAMBERS
EUROPE
AWARDS
for Excellence
2013
WINNER

