**APLIKACE GDPR PRO ZAMĚSTNANCE A ZAMĚSTNAVATELE**

**Expertní skupina legislativní oblast**

Mgr. Luděk Mazuch

Mgr. Denisa Heppnerová

Ing. Petr Dufek

JUDr. Libuše Brádlerová

Jan Juračka

Říjen 2018

Obsah

[1. Úvod – zaměření studie 3](#_Toc528325661)

[2. Právní rámec 4](#_Toc528325662)

[2.1. Zákon o ochraně osobních údajů 4](#_Toc528325663)

[2.2. Obecné nařízení EU o ochraně osobních údajů 4](#_Toc528325664)

[2.3. Nový zákon o zpracování osobních údajů, doprovodný zákon 4](#_Toc528325665)

[3. Základní zásady 5](#_Toc528325666)

[3.1. Základní zásady 5](#_Toc528325667)

[3.2. Subjekt údajů u zaměstnavatele 6](#_Toc528325668)

[3.3. Právní základ zpracování 8](#_Toc528325669)

[3.4. Rozsah údajů 10](#_Toc528325670)

[3.5. Zvláštní kategorie osobních údajů 14](#_Toc528325671)

[4. Analýza 15](#_Toc528325672)

[4.1. Postup 15](#_Toc528325673)

[4.2. Osobní data zaměstnanců 18](#_Toc528325674)

[4.3. Osobní data uchazečů o zaměstnání 20](#_Toc528325675)

[4.4. Zabezpečení 21](#_Toc528325676)

[5. Zpracovatelé – dodavatelé služeb 24](#_Toc528325677)

[6. Záznamy zpracování a předchozí posouzení vlivu 26](#_Toc528325678)

[7. Práva subjektu údajů 28](#_Toc528325679)

[8. Ohlašování případů porušení zabezpečení 29](#_Toc528325680)

[9. Zákon o zpracování osobních údajů 30](#_Toc528325681)

[10. Propojení článků a recitálů GDPR 32](#_Toc528325682)

# Úvod – zaměření studie

Úvodem je třeba konstatovat, že nelze vytvořit univerzálně použitelnou metodiku pro všechny případy, které mohou v praxi nastat, a už vůbec ne v této fázi – je třeba vzít v úvahu, že nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR – *dále jen* **nařízení**) nabylo účinnosti teprve nedávno, a i když ve svých 99 článcích a 173 recitálech je poměrně obsáhlé, existuje řada výkladů a názorů k některým ne zcela jasným otázkám jejich aplikace.

Ani ke dni finalizace této studie (konec října 2018) nejsou schváleny české implementační předpisy, které by měly některé věci zpřesnit. Jedná se o dva zákony - zákon o zpracování osobních údajů a doprovodný zákon o změně dotčených právních předpisů).

Studie by tak měla posloužit jako základní pomůcka pro počáteční implementaci nařízení GDPR.

Samo nařízení je, jak už bylo uvedeno, velmi obsáhlé, řada povinností, o kterých se všeobecně píše nebo mluví, se vztahuje pouze na některé zpracovatele nebo některé typy zpracování. V první části nařízení jsou formulovány záměry, strukturované ve 173 bodech (tzv. recitály). Ve druhé části obsahuje nařízení 99 článků, tedy vlastních právních norem. Recitály jsou nicméně důležité pro výklad jednotlivých článků a institutů, proto je v závěru tohoto materiálu zpracována tabulka jejich vzájemného propojení.

# Právní rámec

## Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů byl základním právním předpisem upravujícím ochranu osobních údajů a činnost Úřadu pro ochranu osobních údajů, a to s účinností od 1.6.2000, až do nabytí účinnosti nařízení GDPR, tj. do poloviny roku 2018.

Zákon přinesl do našeho právního řádu poprvé některé pojmy z oblasti ochrany osobních údajů, a zavedl povinnosti pro osoby, které osobní údaje využívají.

Stále, než bude nahrazen novým zákonem, upravuje postavení a působnost Úřadu pro ochranu osobních údajů (uoou.cz).

## Obecné nařízení EU o ochraně osobních údajů

Obecné nařízení stanovuje práva a povinnosti při zpracování osobních údajů. V tomto rozsahu zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů nahrazuje.

## Zákon o zpracování osobních údajů, doprovodný zákon

Celý právní rámec má dotvářet adaptační zákon, kterým bude nahrazen zákon č. 101/2000 Sb. Tento zákon by měl obsahovat upřesnění i povolené odchylky či zvláštní úpravy k nařízení GDPR.

Zákon je ve sněmovně od konce března 2018 a je předmětem řady pozměňovacích návrhů. Původní plán byl věnovat se v této studii alespoň částečně také tomuto zákonu, avšak vzhledem k výše uvedenému je to možné pouze velmi rámcově (kapitola 9).

Stejný osud má doprovodný zákon, kterým se mění řada zákonů v souvislosti s přijetím zákona o zpracování osobních údajů, a to právě v souvislosti se zpracováním osobních údajů především státními orgány a úřady.

# Základní zásady

Prvním a zásadním krokem v každé firmě je **analýza** situace ve firmě, tedy v podstatě identifikace

* jaká data shromažďuje a jak,
* kdo s daty přichází do styku a jak s nimi nakládá,
* jaká data ukládá a archivuje a jakým způsobem,
* zda a jaká existuje "díra" v jejich ochraně (proto se někdy analýza označuje jako GAP analýza, tedy analýza mezery).

## Základní zásady

Nařízení se týká ochrany **osobních údajů fyzických osob**. Článek 4. nařízení jako definici **osobního údaje** uvádí, že se jedná o veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů), přičemž identifikovatelnou fyzickou osobou je fyzická osoba, kterou **lze přímo či nepřímo identifikovat**, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Nejedná se tedy o uzavřený věcný výčet toho, co je či není "osobním údajem".

Osobní údaje musí být:

|  |  |
| --- | --- |
| zpracovávány korektně a zákonným a transparentním způsobem | **zákonnost, korektnost a transparentnost** |
| shromažďovány pro určité, výslovně vyjádřené a legitimní účelya nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný | **účelnost** |
| přiměřené, relevantní a omezené na nezbytný rozsah ve vztahuk účelu, pro který jsou zpracovávány | **minimalizace údajů** |
| přesné a v případě potřeby aktualizované | **přesnost** |
| uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány | **časové omezení** |
| zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením | **integrita a důvěrnost** |

**Správcem** je fyzická nebo právnická osoba, která shromažďuje osobní údaje za určitým účelem.

**Zpracovatelem** je fyzická nebo právnická osoba, která zpracovává osobní údaje pro správce (např. osoba provádějící zpracování mezd).

Správce odpovídá za dodržení uvedených zásad a musí být schopen soulad s nimi doložit.

Základní zásady zpracování osobních údajů vyjadřují podstatu správného přístupu ke zpracování a ochraně osobních údajů. Na prvním místě stojí důraz kladený na účelnost zpracování. Správce musí vždy vědět, za jakým účelem, tj. proč osobní údaje zpracovává. Účel, případně účely musí být předem a jasně vyjádřené. V ideálním případě by tedy účely zpracování měly být uvedeny na předním místě vnitřní dokumentace, kterou správce zpracoval (například směrnice o ochraně a zpracování osobních údajů).

Právní úprava neposkytuje žádný přesný výčet použitelných účelů zpracování osobních údajů. Je tedy na každém správci, aby účel zpracování definoval sám.

## Subjekt údajů u zaměstnavatele

V zásadě se u běžných zaměstnavatelů bude jednat o tyto subjekty (fyzické osoby):

* ZAMĚSTNANCI
* UCHAZEČI O ZAMĚSTNÁNÍ
* KLIENTI
* OBCHODNÍ PARTNEŘI
* OSOBY VSTUPUJÍCÍ DO FIRMY

V dalším textu se budeme zabývat právě zaměstnanci a uchazeči o zaměstnání.

Základní právní rámec ochrany osobnosti vychází z ústavních předpisů a občanského zákoníku. Listina základních práv a svobod garantuje, že každý má právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a na ochranu svého jména. Každý má rovněž právo na ochranu před neoprávněným zasahováním do rodinného a soukromého života a každý je také chráněn před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Pro soukromoprávní vztahy obecně je pak právo na ochranu osobnosti, důstojnosti, soukromí a projevů osobní povahy zakotveno i v občanském zákoníku.

Ve vztahu k pracovněprávním vztahům jsou tato obecná pravidla konkretizována především zákoníkem práce a v konkrétní rovině ve vztahu ke zpracování a ochraně osobních údajů i v nařízení GDPR.

Právo na ochranu soukromí a osobních údajů zaměstnanců se v pracovněprávních vztazích do určité míry střetává s právem zaměstnavatele kontrolovat výkon práce, dbát na efektivní pracovní výkonnost zaměstnanců a chránit svůj majetek. Zaměstnavatelé bezpochyby musí mít v rukou určité konkrétní nástroje, s jejichž využitím budou tyto oprávněné zájmy a/nebo povinnosti naplňovat. Tyto dva proti sobě stojící zájmy je třeba vybalancovat tím, že zaměstnavatelé budou shromažďovat o zaměstnancích pouze ty údaje, které podle zákona musí, případně je nutně potřebují, to vše za dodržení pravidel stanovených příslušnými právními předpisy.

Zaměstnavatelé v pracovněprávních vztazích shromažďují o zaměstnancích informace a údaje, které mají povahu osobních údajů. Každý zaměstnavatel v důsledku této skutečnosti musí být považován za správce osobních údajů. Zaměstnavatelé pak také jako správci musí splňovat podmínky pro zpracování osobních údajů, zabezpečovat jejich ochranu a plnit další povinnosti v rámci zachovávání odpovědného přístupu ke zpracování osobních údajů.

Základní účel, na jehož základě zaměstnavatel jako správce zpracovává osobních údajů svých zaměstnanců, představuje samotné vedení personální agendy, které je nezbytnou součástí existence pracovněprávních vztahů, mimo jiné i vzhledem k povinnostem, které zaměstnavatelům vyplývají z právních předpisů. Účelem zpracování může být i racionální a odpovědný postup při obsazování volných pracovních míst, efektivní naplňování hlavní činnosti zaměstnavatele, propagace zaměstnavatele a public relations, zajištění bezpečnosti práce, zajištění pracovnělékařských služeb, odškodnění pracovních úrazů a nemocí z povolání či provádění kontroly dodržování režimu dočasně práce neschopného pojištěnce.

Zpracovávány pak mohou být jen ty osobní údaje, které jsou nezbytné pro naplnění stanoveného účelu. Osobní údaje mohou být zpracovávány jen po dobu, která je nutná pro dosažení účelu.

Pokud zaměstnavatel jako správce zpracovává některé osobní údaje svých zaměstnanců, ale neumí vysvětlit, proč zpracování provádí a k čemu tyto osobní údaje potřebuje, půjde o bezúčelné zpracování, které odporuje základním zásadám GDPR. Takovéto zpracování nemůže být prováděno, ani kdyby s ním zaměstnanec jako subjekt vyslovil souhlas.

Zpracování osobních údajů musí být zákonné. Má-li zaměstnavatel ke zpracování účel, musí se ještě vypořádat s tím, aby doložil některý z právních důvodů (titulů) zpracování. GDPR obsahuje taxativní (úplný) výčet právních titulů pro zpracování osobních údajů. Alespoň jeden z nich musí zaměstnavatel jako správce ke každému zpracování mít.

## Právní základ zpracování

Ve většině případů se bude jednat o plnění na základě jiného právního titulu, než je souhlas se zpracováním, a to konkrétně na základě

* **plnění smlouvy** nebo předsmluvních opatření

*pracovněprávní u zaměstnanců, obchodní u zákazníků, dodavatelů nebo odběratelů*

* **plnění právní povinnosti**

*daňové, sociálního zabezpečení a zdravotního pojištění, vyplývající ze zákoníku práce apod.*

* **oprávněného zájmu**

*např. identifikace osob vstupujících do podniku v nezbytném rozsahu*

Článek 6 nařízení k tomu stanoví: zpracování je zákonné, pouze pokud je splněna **nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu**:

|  |  |
| --- | --- |
|  | subjekt údajů **udělil souhlas** se zpracováním svých osobních údajů 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 údajů |
|  | zpracování je nezbytné **pro splnění právní povinnosti**, která se na správce vztahuje |
|  | zpracování je nezbytné **pro ochranu životně důležitých zájmů** subjektu údajů nebo jiné fyzické osoby |
|  | 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** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě |

Na prvním místě tedy figuruje ve výčtu právních důvodů pro zpracování souhlas subjektu, ačkoli ten bude v případě zaměstnanců (i jiných subjektů) při běžné činnosti firmy spíše **výjimečný**. Zaměstnavatel, který řádně ctí účelnost zpracování osobních údajů a zpracovává jen ty údaje, které potřebuje pro vedení personální agendy, mnohdy zjistí, že ve vztahu ke zpracovávaným osobním údajům od zaměstnanců žádný souhlas vůbec nepotřebuje. Bude-li přece jen v některých případech souhlas zaměstnanců vyžadovat, nesmí být formulace tohoto souhlasu součástí pracovní smlouvy, ani jiné smlouvy uzavírané se zaměstnancem, ale je zaměstnancem udělen na samostatné listině. Zaměstnanec musí být při předložení žádosti o souhlas se zpracováním poučen o tom, že není povinen souhlas udělit a případné udělení souhlasu je z jeho strany dobrovolné a svobodné.

Typickým právním titulem, na jehož základě provádějí zaměstnavatelé zpracování, je plnění právních povinností. Řadu osobních údajů zaměstnavatelé o zaměstnancích zpracovávají právě proto, aby dostáli svým povinnostem vyplývajícím ze zvláštních právních předpisů. Jde zejména o předpisy týkající se daní a pojistného na sociální zabezpečení a všeobecné zdravotní pojištění, dále pak o předpisy v oblasti zaměstnanosti, bezpečnosti práce a pracovnělékařských služeb:

* + 1. zákoník práce, zákon o zaměstnanosti a další právní předpisy v oblasti pracovního práva,
		2. zákon o specifických zdravotních službách a další právní předpisy v oblasti pracovnělékařských služeb,
		3. zákon o dani z příjmu a další daňové předpisy,
		4. právní předpisy v oblasti zdravotního, nemocenského a důchodového pojištění,
		5. občanský soudní řád, exekuční řád a insolvenční zákon.

Dalším často uplatňovaným právním titulem pro zpracování osobních údajů je plnění smlouvy, jejíž smluvní stranou je i subjekt údajů, tj. zaměstnanec. Zaměstnavatel jako správce zpracovává řadu osobních údajů právě proto, aby plnil své povinnosti vyplývající z pracovní smlouvy, dohody o pracovní činnosti nebo dohody o provedení práce či jiné smlouvy, kterou se zaměstnancem uzavřel (například kvalifikační dohoda, dohoda o odpovědnosti k ochraně hodnot svěřených zaměstnanci k vyúčtování), případně z kolektivní smlouvy sjednané s odborovou organizací.

Osobní údaje zaměstnanců lze zpracovávat i bez jejich souhlasu, pokud je to nezbytné pro účely oprávněných zájmů zaměstnavatele jako správce či třetí strany správce. Zaměstnanec je v takovém případě při získání údaje poučen o tom, pro jaký oprávněný zájem je zpracování nezbytné. Jde zejména o oprávněné zájmy zaměstnavatele spočívající v zajištění výkonu či provozu jeho činnosti, zajištění bezpečnosti a ochrany zdraví při práci či zajištění ochrany majetkových zájmů zaměstnavatele.

**Souhlas ke zpracování osobních údajů tedy v žádném případě nežádejte zbytečně, pokud ho nepotřebujete. Nevyhnete se tím případným problémům, spíše naopak.**

## Rozsah údajů

Stejně tak nežádejte zbytečně údaje, které nepotřebujete. Zvažte, zda veškeré údaje, které shromažďujete a uchováváte, jsou nezbytné k danému účelu a zda nejsou nadbytečné (typicky u uchazečů o zaměstnání – viz samostatná kapitola, strana 21).

Vyhněte se zpracování zvláštních kategorií osobních údajů, jako jsou biometrické či genetické údaje, pokud to není nezbytné, viz dále. Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.

K plnění povinností vyplývajících z právních předpisů potřebuje zaměstnavatel zpracovávat například následující osobní údaje:

* + jméno a příjmení,
	+ trvalé bydliště,
	+ faktické bydliště (místo pro doručování)
	+ datum narození,
	+ místo narození,
	+ rodné číslo,
	+ zdravotní pojišťovna,
	+ údaj o manželu či manželce a počtu vyživovaných dětí,
	+ státní příslušnost,
	+ probíhající srážky ze mzdy,
	+ trestněprávní bezúhonnost,

Pro plnění uzavřené smlouvy typicky zaměstnavatelé zpracovávají například

* + číslo bankovního účtu pro výplatu mzdy,
	+ členství v odborové organizaci – pokud bylo v kolektivní smlouvě dohodnuto, že bude zaměstnavatel provádět srážky ze mzdy k hrazení členských příspěvků a zaměstnanec o provádění těchto srážek požádal.

Jak už bylo uvedeno, pro zpracování výše uvedených osobních údajů zaměstnavatel **nemusí** ani **nemá od zaměstnanců získávat souhlas**. Nadbytečné vyžadování souhlasu se zpracováním tam, kde pro zpracování existuje jiný právní titul, musí být označeno za špatnou praxi, která dotčené subjekty uvádí v omyl a současně vypovídá o nesprávném přístupu zaměstnavatele ke zpracování osobních údajů.

**Podmínky vyjádření souhlasu** (článek 7. nařízení GDPR):

* 1. Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.
	2. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.
	3. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.
	4. Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.

Jakým konkrétním způsobem zaměstnavatel údaje o zaměstnancích získá, záleží víceméně na jeho uvážení a zavedené praxi. Obvyklým řešením je, že zaměstnavatel po vzniku pracovního poměru předloží zaměstnanci k vyplnění osobní dotazník, v němž zaměstnanec shora uvedené údaje vyplní. Je třeba dodat, že zaměstnanec je povinen zaměstnavateli údaje, které nutně potřebuje znát z důvodu plnění předepsaných povinností, pravdivě sdělit.

Zaměstnavatelé někdy získávají některé z výše uvedených osobních údajů zaměstnanců tím způsobem, že si pořídí fotokopii občanského průkazu zaměstnance. Kopie občanského průkazu nicméně vedle údajů, které zaměstnavatel nezbytně potřebuje, obsahuje například i fotografii zaměstnance, případně některé další údaje, pro jejichž zpracování nemá zaměstnavatel účel. Kromě zvláštních případů, v nichž by povinnost mít k dispozici kopii občanského průkazu vyplývala z právního předpisu, tedy bude pořízení a uchování kopie tohoto dokladu představovat bezúčelné zpracování osobních údajů. Zaměstnavatelé by se tedy měli této špatné praxe vyvarovat.

Zaměstnavatel v některých zvláštních případech musí o svých zaměstnancích znát a zpracovávat i osobní údaje, které patří mezi zvláštní kategorie podle Čl. 9 GDPR (podle dřívější terminologie se jednalo o citlivé osobní údaje). Například pokud zaměstnává osoby se zdravotním postižením, musí podle ustanovení § 80 písm. c) zákona o zaměstnanosti vést evidenci zaměstnávaných osob se zdravotním postižením, která musí obsahovat i údaj o důvodu, na jehož základě byl zaměstnanec uznán osobou se zdravotním postižením, tedy údaj o zdravotním stavu. Vzhledem k tomu, že se bude jednat o zpracování za účelem splnění právní povinnosti, nevyžaduje se ke zpracování zaměstnancův souhlas.

Je ovšem třeba upozornit na to, že v jiných případech, v nichž k tomu není dán bezprostřední účel a právní titul, by zjišťování údaje o zdravotním stavu zaměstnanců zaměstnavatelem představovalo nezákonné zpracování osobních údajů spadajících do zvláštní kategorie. Povahu citlivého údaje nicméně nemá informace o zdravotní způsobilosti, případně nezpůsobilosti zaměstnance k práci, kterou zaměstnavatel zjišťuje prostřednictvím lékařského posudku vydaného poskytovatelem pracovnělékařských služeb. Informace o zdravotní způsobilosti zaměstnance k výkonu práce totiž sama o sobě nijak konkrétně nevypovídá o zdravotním stavu.

Lékař smí jako výsledek prohlídky zaměstnance předat zaměstnavateli pouze tu informaci, zda zaměstnanec je či není zdravotně způsobilý k výkonu práce, případně zda smí práci vykonávat jen za určitých podmínek (úprava pracovní doby nebo omezení určitých činností apod.). Konkrétní informaci o zdravotním stavu či diagnóze může lékař sdělit jen přímo zaměstnanci, který se prohlídce podrobil.

V souvislosti s osobními a citlivými osobními údaji, které zaměstnavatelé o zaměstnancích smějí zjišťovat a zpracovávat, je třeba upozornit na ustanovení § 316 odst. 4 zákoníku práce, které obsahuje demonstrativní výčet informací, které zaměstnavatel od zaměstnanců nesmí zjišťovat – údaje o

1. těhotenství (pokud to není podstatné pro druh vykonávané práce),
2. rodinných a majetkových poměrech,
3. sexuální orientaci,
4. původu,
5. členství v odborové organizaci,
6. členství v politických stranách nebo hnutích,
7. příslušnosti k církvi nebo náboženské společnosti,
8. trestněprávní bezúhonnosti (pokud není zákonem stanovena jako podmínka výkonu práce).

Významné je, že ve vztahu k informacím uvedeným pod písmeny a), b) a h) zákon stanoví, že tyto údaje zaměstnavatel vyžadovat smí, stanoví-li to zákon nebo má-li k tomu zaměstnavatel věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li této povaze požadavek na dotčenou informaci přiměřený.

Jedním z údajů, ohledně jejichž zjišťování platí popsaná pravidla, je i údaj o trestněprávní bezúhonnosti. Pokud zvláštní zákon jako jeden z předpokladů pro výkon práce předepisuje podmínku bezúhonnosti, musí fyzická osoba ještě před vznikem pracovněprávního vztahu doložit splnění této podmínky výpisem z evidence Rejstříku trestů ne starším než 3 měsíce. Na možnost zaměstnavatele vyžadovat i od ostatních zaměstnanců výpis z evidence Rejstříku trestů je třeba usoudit na základě zjištění, zda jsou pro takový postup dány ospravedlnitelné věcné důvody a je-li požadavek na zjištění bezúhonnosti dané osoby přiměřený.

Dalším z údajů, který smí zaměstnavatel vyžadovat pouze při existenci vážných důvodů spočívajících ve vykonávané práci, je údaj o těhotenství zaměstnankyně. Vážný důvod ke zjištění takového údaje by byl dán zejména v případě, kdy by zaměstnavatel přijímal zaměstnankyni k výkonu práce na takové pracoviště, kde těhotná žena podle zvláštního předpisu (vyhláška č. 288/2003 Sb.) či na základě lékařského rozhodnutí nesmí pracovat.

Z ustanovení § 316 odst. 4 zákoníku práce také vyplývá, že zaměstnavatel nesmí od zaměstnanců vyžadovat údaj o jejich členství v odborové organizaci. Je ovšem třeba upozornit na to, že pouze prostřednictvím informace o tom, že alespoň tři zaměstnanci zaměstnavatele jsou členy odborové organizace, se zaměstnavatel může dozvědět, že u něj odborová organizace působí a musí vůči ní plnit povinnosti stanovené zákoníkem práce a dalšími právními předpisy. Chce-li tedy odborová organizace u zaměstnavatele realizovat svá oprávnění, musí mu prokázat, že u něj působí, tedy že alespoň tři zaměstnanci zaměstnavatele jsou jejím členem. Jakým způsobem to odborová organizace zaměstnavateli prokáže, záleží na ní samotné.

Zaměstnavatel, u kterého působí odborová organizace, nicméně nemůže vyžadovat informace o tom, kolik zaměstnanců je jejím členem a o jaké zaměstnance se jedná. Informaci o počtu zaměstnanců, kteří jsou členem odborové organizace, může zaměstnavatel vyžadovat snad jen v případě, kdy u něj působí více odborových organizací. Pokud totiž v tomto případě dojde ve vztahu mezi zaměstnavatelem a zaměstnancem k některé ze záležitostí, kde zákoník práce předepisuje zaměstnavateli povinnost projednat ji s odborovou organizací (například převedení na jinou práci nebo výpověď), má zaměstnavatel povinnost jednat s odborovou organizací, jíž je zaměstnanec členem. Pokud není zaměstnanec členem žádné odborové organizace, musí zaměstnavatel jednat s odborovou organizací s největším počtem členů, kteří jsou u zaměstnavatele v pracovním poměru, neurčí-li zaměstnanec jinak.

Pro tyto případy tedy zaměstnavatel potřebuje mít k dispozici informaci o tom, která odborová organizace sdružuje největší počet jeho zaměstnanců. Ani v tomto případě nemůže ovšem vyžadovat seznamy členů odborových organizací, neboť by tím porušil zákaz vyžadovat informaci o členství zaměstnanců v odborové organizaci. Nabízí se tedy například takový postup, kdy odborové organizace poskytnou zaměstnavateli informaci o tom, která sdružuje větší počet jeho zaměstnanců, prostřednictvím společného čestného prohlášení.

Informaci o členství zaměstnance v odborové organizaci zaměstnavatel nicméně zprostředkovaně zjistí tehdy, pokud bude v kolektivní smlouvě nebo jiné dohodě uzavřené zaměstnavatelem a odborovou organizací sjednáno, že bude zaměstnavatel provádět srážky z příjmu zaměstnance k úhradě členských příspěvků člena odborové organizace. Tento způsob placení příspěvků je ovšem vázán ještě na udělení souhlasu zaměstnancem, který tímto sám zaměstnavateli údaj o svém členství v odborové organizaci dobrovolně poskytne.

I v případě, kdy zaměstnavatel zpracovává jen nezbytné osobní údaje, musí dbát o to, aby zaměstnanec neutrpěl újmu na svých právech a aby nedošlo k neoprávněnému zásahu do soukromého života zaměstnanců a zneužití osobních údajů. Musí proto ke zpracování osobních údajů přistupovat odpovědně a kontinuálně dbát o zejména o účelnost a minimalizaci zpracování osobních údajů, jakož i o jejich zabezpečení a ochranu.

## Zvláštní kategorie osobních údajů

Zpracování zvláštních kategorií osobních údajů upravuje článek 9 nařízení GDPR, který zakazuje zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Zpracování je možné v některých případech, např.:

* subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů;
* zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
* zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
* zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
* zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí;
* zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.

Co se týče běžné činnosti, bude právním důvodem zpracování **plnění povinností v oblasti pracovního práva**. Pokud tomu tak není a např. evidenci příchodu a odchodu provádíte pomocí biometrického údaje, bude zapotřebí souhlas, stejně tak jako zdůvodnění, proč je nutné používat biometrický údaj k tomuto účelu.

# Analýza

## Postup

Podle nařízení GDPR musí mít někteří správci **pověřence pro ochranu osobních údajů**. Tato povinnost se zdaleka nedotýká každého podnikatele (správce) - kromě případů, kdy zpracování osobních údajů provádí orgán veřejné moci nebo veřejný subjekt je to tehdy, když hlavní činnosti správce nebo zpracovatele spočívají

* ve zpracování údajů, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů;
* nebo v rozsáhlém zpracování zvláštních kategorií údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů.

V případě, že Vaše firma nemá povinnost mít pověřence, **určete jednoho dva zaměstnance, kteří budou mít tuto oblast zahrnutou v pracovní náplni.** Tyto zaměstnance dostatečně vzdělejte.

Určený zaměstnanec nebo zaměstnanci **uspořádají několik schůzek**, a to za účasti osob, které si vytipují jako zástupce ze všech oddělení, kde se pracuje s osobními údaji (personalistika, seznamy dodavatelů a odběratelů, návštěvníci atd.). Na začátku to mohou být klidně všechna oddělení a za spolupráce osoby nebo osob z vrcholového managementu.

Ze všech jednání pořiďte co možná nejobsáhlejší **ZÁPIS**, který uchovejte, abyste posléze byli kontrolnímu orgánu schopni doložit, že jste se problematikou GDPR ve firmě dostatečně a opakovaně zabývali. Zdá se to jako formalita, je však dosti zásadní (a její naplnění není zase tak složité). Jinými slovy – vytvořte si obsáhlou dokumentaci ze všeho, co v souvislosti s nařízením GDPR děláte. Zápisy označte jako „porada k ochraně osobních údajů“ nebo podobně.

Cílem schůzek (a obsahem zápisů) bude **analýza** odpovídající na tyto otázky:

* + kde jsou v organizaci místa sběru osobních dat,
	+ jakých subjektů se týká,
	+ jaká je struktura těchto dat (o jaká data se v tom kterém případě konkrétně jedná),
	+ zda je potřeba ke zpracování dat souhlas subjektu dat,
	+ pokud ano, zda a jakým způsobem je získáván,
	+ jakým způsobem ta která data získáváte (formuláře listinné, online atp.),
	+ jaký je věcný obsah nástrojů získávání dat (např. formulářů),
	+ jak a kde se s daty pracuje (v jakém systému zpracování jsou dostupná v digitální podobě),
	+ kdo má oprávnění s daty manipulovat,
	+ kdo má přístup k jakým datům a na základě jakého oprávnění,
	+ jak jsou data uchovávána a chráněna,
	+ jaká jsou možná rizika zneužití,
	+ jak se bude postupovat v případě zneužití.

Vždy zaznamenejte a podle uvedených kritérií analyzujte **nejprve současný stav**.

**Smyslem analýzy** není nutně zjištění, že něco děláte špatně a musíte vše dělat jinak. Smyslem je zjistit, co děláte a jak to děláte, a na základě tohoto zjištění by mělo následovat doporučení, co a jak dělat nadále. To znamená, stanovení transparentních pravidel pro zpracování osobních údajů. Tedy nová tabulka, v níž bude uvedeno, co a jak budete zpracovávat, a nová jasně zaznamenaná pravidla pro toto zpracování.

Přitom zvažte zejména

* **zda skutečně veškeré údaje, které o subjektech shromažďujete, jsou nezbytné vzhledem k jejich účelu,**
* **zda nezískáváte nadbytečně souhlasy se zpracováním,**
* **zda subjekty údajů dostatečně informujete,**
* **zda údaje zbytečně nefigurují v některých databázích,**
* **zda je neuchováváte zbytečně dlouho,**
* **zda jsou dostatečně chráněny před zneužitím,**
* **jaké osoby k nim mají přístup a zda je to u všech potřebné.**

**Výsledkem bude přehled o pohybu dat týkajících se zaměstnanců, uchazečů o zaměstnání, a podobně i zákazníků, obchodních partnerů, či dalších osob.**

* Uveďte, zda je využíván **zpracovatel**, kdo to je, a jaké údaje jsou mu předávány.
* Uveďte skutečnost, zda jste či **nejste povinni jmenovat pověřence pro ochranu osobních údajů** (tuto povinnost předepisuje pro některé správce nařízení GDPR v článku 37). Jedná se o osobu, která má plnit funkci pomocníka či koordinátora ochrany osobních údajů a má také zabezpečovat komunikaci s dozorovými orgány, zejména Úřadem pro ochranu osobních údajů (roli pověřence může plnit i externí osoba).
* Uveďte, že podmínky nařízení GDPR pro povinné jmenování pověřence v rámci své obchodní a provozní činnosti nepovažujete za naplněné, protože Vaše hlavní činnosti nespočívají v rozsáhlém pravidelném a systematickém monitorování subjektů údajů ani ve zpracování zvláštních kategorií osobních údajů.
* Uveďte, jakým způsobem informujete subjekty údajů o zpracování informací.
* Zákazníka nebo smluvního partnera informujte o zpracování osobních údajů např. v obchodních podmínkách nebo na webových stránkách. Rovněž tak uchazeče o zaměstnání při odeslání osobních údajů prostřednictvím webového formuláře.
* Zaměstnance informujete o zpracování osobních údajů při uzavření smlouvy.
* Určitou část analýzy je nutné věnovat otázce zabezpečení. Sestavte přehled o tom, jaké je zabezpečení ochrany dat ve Vaší firmě, a zamyslete se nad tím, zda je potřeba provést nějaké změny (viz další část).

**Každý krok, který provádíte, zaznamenejte, uveďte, co jste zjistili a zda je potřeba provést nějaké opatření, nebo že není potřeba provést žádné opatření, protože jste v souladu s nařízením GDPR.**

**Zbytečně shromažďovaná data vyhoďte a zastavte jejich přísun. Přístup k těm potřebným omezte na nezbytný okruh zaměstnanců.**

**Proveďte analýzu souhlasů se zpracováním, které již v současné době získáváte, a prověřte, zda odpovídají výše uvedeným požadavkům, a také to, zda jsou potřebné, zda nemáte jiný právní základ pro zpracování dat.**

**Nepožadujte udělování souhlasů zbytečně, vyseparujte případné osobní údaje, které byste nezpracovávali za účelem splnění smlouvy nebo právní povinnosti, příp. oprávněných zájmů, a souhlas chtějte jenom v nezbytných případech.**

## Osobní data zaměstnanců

Sestavte si přehled, jaké údaje jsou shromažďovány, na jakém právním základě (nejčastěji plnění smlouvy / plnění právní povinnosti / oprávněný zájem / souhlas).

|  |  |  |  |
| --- | --- | --- | --- |
| **Osobní údaje** | **právní základ** | **místo uložení** | **zaměstnanci přicházející do styku** |
| jméno a příjmení | B/C smlouva, povinnost | osobní spis … |  |
| datum narození | B/C |  |  |
| rodné číslo | B/C |  |  |
| pohlaví | C |  |  |
| státní příslušnost | C |  |  |
| rodinný stav | C |  |  |
| počet dětí | C |  |  |
| vzdělání | B |  |  |
| adresy (bydliště, místo pobytu) | B |  |  |
| telefon | B |  |  |
| síťový identifikátor (e-mail, skype) | A/B |  |  |
| místo narození | C |  |  |
| číslo občanského průkazu | B |  |  |
| číslo řidičského průkazu | B/C |  |  |
| číslo cestovního pasu | B |  |  |
| bankovní spojení | B |  |  |
| zdravotní pojišťovna | C |  |  |
| předchozí zaměstnavatel | C |  |  |
| výpis z trestního rejstříku | C\* |  |  |
| kamerový záznam | F |  |  |
| zvukový záznam | F ? |  |  |
|  |  |  |  |
|  |  |  |  |
| **Zvláštní kategorie osobních údajů** |
| snímek obličeje (biometrický údaj) | A |  |  |
| otisk prstu (biometrický údaj) | A |  |  |
| podpis (biometrický údaj) | B |  |  |
| krevní skupina (genetický údaj) | ?? |  |  |
| zdravotní stav - způsobilost | B/C |  |  |
| zdravotní znevýhodnění - způsobilost | B/C |  |  |
| členství v odborech | C\* |  |  |
|  |  |  |  |
| **Údaje o členech rodiny** |  |  |  |
| jméno a příjmenímanžela/manželky |  |  |  |
| bydliště manžela/manželky |  |  |  |
| jméno a příjmení dítěte |  |  |  |
| datum narození dítěte |  |  |  |
|  |  |  |  |

 \* v některých případech

Tabulka obsahuje výčet nejčastějších dat zaměstnanců, upravte si ji podle potřeby. Informace o členství v odborech nesmí zaměstnavatel od zaměstnance vyžadovat, nicméně tato informace mu může být poskytnuta z iniciativy zaměstnance či odborové organizace, údaj o tom tedy přichází v úvahu např. tehdy, provádí-li zaměstnavatel srážku členského příspěvku.

Stejně tak některé další údaje přicházejí v úvahu pouze v zákonem vymezených případech (podkladem pro jejich shromažďování tedy bude právní povinnost).

Jednotlivé sloupce či údaje v tabulce, nebo její celkovou podobu, si můžete samozřejmě přizpůsobit a zahrnout další informace, můžete ji použít jenom pro inspiraci.

Cílem je získat **přehled**

* **jak jsou údaje uchovávány a ukládány (osobní spis - kartotéka, interní síť, mzdová či personální aplikace, archiv apod.),**
* **které organizační útvary mají přístup k osobním údajům, včetně jednotlivých pracovních pozic, jež jsou povinny/oprávněny s nimi při plnění pracovních povinností nakládat,**
* **jaký je způsob přístupu k osobním údajům pro jednotlivé pozice,**
* **jak jsou údaje zabezpečeny,**
* **jak dlouho jsou údaje uchovávány - např. po dobu pěti let po skončení pracovního poměru, nestanoví-li právní předpis jinak (mzdové listy).**

**Získáte tak celkový přehled o pohybu dat uvnitř firmy, týkající se zaměstnanců. Podobný postup bude následovat v případě dalších subjektů údajů.**

**Důležité je si uvědomit, že u zaměstnanců shromažďujete v drtivé většině pouze osobní data, která potřebujete k plnění smlouvy a/nebo zákonných povinností, příp. oprávněných zájmů. Nevyžadujte tedy od zaměstnanců zbytečné souhlasy se zpracováním.** Nejenže by to bylo nadbytečné, ale zřejmě také neplatné, vzhledem k větší či (v současné době nedostatku zaměstnanců) menší nerovnosti postavení smluvních stran a tedy existující pravděpodobnosti, že neudělení souhlasu může mít pro zaměstnance negativní důsledky.

Pokud přesto budete chtít uvést v pracovní smlouvě nebo smlouvě o pracích konaných mimo pracovní poměr zmínku o ochraně osobních údajů, je možné zvolit např. tuto formulaci:

*Zaměstnanec bere na vědomí, že zaměstnavatel zpracovává osobní údaje zaměstnance, uvedené v této smlouvě a souvisejících dokladech, které mu zaměstnanec sdělil při vzniku pracovněprávního vztahu nebo v jeho průběhu, a to výhradně za účelem plnění smlouvy, právních povinností a oprávněného zájmu účastníků smlouvy. Oprávněným zájmem je zejména ochrana majetku zaměstnavatele a zaměstnanců.*

*Osobní údaje jsou shromažďovány a dále zpracovávány pouze v rozsahu nezbytném pro výše uvedené účely.*

*Osobní údaje zaměstnavatel zpracovává po dobu trvání pracovněprávního vztahu. Po jeho skončení budou osobní údaje archivovány v souladu s příslušnými právními předpisy, a již nepotřebné údaje zlikvidovány.*

*Zaměstnanec má právo na přístup k jeho osobním údajům, které zaměstnavatel zpracovává, a další práva vyplývající ze zákona.*

## Osobní data uchazečů o zaměstnání

Zaměstnavatelé zpracovávají osobní údaje nejen o osobách, s nimiž již založili pracovněprávních vztah, ale také o uchazečích o zaměstnání. Zaměstnavatel zpracovává osobní údaje osob, které se u něj ucházejí o zaměstnání, za účelem efektivního výměru vhodného uchazeče, který odpovídá kvalifikačním a dalším požadavkům stanoveným zaměstnavatelem.

Uchazeč, který se přihlásil do výběrového řízení, ovšem předal zaměstnavateli své osobní údaje v souvislosti s tím, že projevil zájem o uzavření pracovní smlouvy. Jednání o smlouvě představuje samo o sobě právní titul pro zpracování, a tak se zpracováním osobních údajů pro účely průběhu výběrového řízení nemusí uchazeč udělit souhlas.

Je třeba upozornit na to, že uchazeči o zaměstnání poskytují zaměstnavateli své osobní údaje právě a jen pro účely probíhajícího výběrového řízení. Zaměstnavatelé mají někdy zájem na tom uschovat si životopisy neúspěšných uchazečů i po ukončení výběrového řízení pro účely případného dalšího výběrového řízení na obdobné volné pozice, které by se mohly objevit v budoucnu. Souhlas se zpracováním osobních údajů uchazeče o zaměstnání pro tyto účely nicméně dovodit nelze. Bude tedy nutné, aby subjekt údajů se zpracováním údajů obsažených ve svém životopisu pro účely případného dalšího výběrového řízení poskytl informovaný souhlas odpovídající podmínkám stanoveným v GDPR.

Zaměstnavatelé si při zpracovávání osobních údajů o uchazečích o zaměstnání musí dát pozor na zvláštní pravidla, která předepisují, jaké údaje smí a nesmí zaměstnavatel od uchazečů vyžadovat. Od uchazečů o zaměstnání může zaměstnavatel vyžadovat pouze takové údaje, které bezprostředně souvisí s uzavřením pracovní smlouvy. Tuto bezprostřední souvislost se vznikem pracovního poměru musí být tedy zaměstnavatel schopen dovodit u každého jednotlivého údaje, který od potencionálního zaměstnance vyžaduje. Nelze tedy automaticky říci, že všechny osobní údaje, které zaměstnavatel potřebuje zpracovat ve vztahu ke svým zaměstnancům, může vyžadovat i od uchazečů o zaměstnání.

Zaměstnavatelé poměrně často předkládají uchazečům o zaměstnání k vyplnění vstupní dotazník. Samo o sobě to pochopitelně není v rozporu se zákonem. Veškeré údaje, k jejichž vyplnění zaměstnavatel uchazeče předložením dotazníku vyplývá, musí mít nicméně bezprostřední souvislost s uzavřením pracovní smlouvy.

Prostřednictvím těchto pravidel právo sleduje zaprvé ochranu soukromí a osobních údajů zaměstnance a zadruhé se snaží předcházet diskriminaci a nerovnému zacházení s těmito osobami, ke kterému by mohlo dojít, pokud by se zaměstnavatel dověděl o určitých skutečnostech představujících potencionální diskriminační důvod.

*PŘÍKLAD*

*Pokud Vám uchazeči o zaměstnání sdělí data, která nepotřebujete (např. v e-mailu, v životopise), zbytečná data vyseparujte a zničte; e-mail si vytiskněte a smažte, nadbytečné údaje na listině začerněte nebo si naopak ty důležité přepište a původní listinu skartujte.*

*Stejně naložte s fotokopií občanského průkazu, pokud si ji pořídíte nebo pokud Vám je dodána.*

*Typická data, která nepotřebujete od uchazečů o zaměstnání, je rodné číslo nebo číslo občanského průkazu, údaj o počtu dětí.*

*Zaslané materiály od uchazečů o zaměstnání (životopis) zničte, anebo na základě souhlasu uchazeče uschovejte po krátkou dobu (předem stanovenou) za účelem možnosti oslovení uchazeče v budoucnu.*

## Zabezpečení

K zabezpečení osobních údajů musí zaměstnavatel zejména přijmout taková organizačně-technická opatření, která zajistí, že nedojde k neoprávněnému přístupu k osobním údajům. Právní úprava obsažená v GDPR nepředepisuje přesně, jak mají tato opatření vypadat. Důraz je kladen na zabezpečení ve vztahu k možnostem správce, souvisejícím nákladům, jakož i k rozsahu zpracování a riziku pro práva a svobody subjektů údajů.

Při stanovení a provádění technických a organizačních opatření k zajištění odpovídající úrovně zabezpečení se přihlíží k následujícím faktorům

- stav techniky;

- **náklady na provedení** (jde o to, aby byly přiměřené danému riziku);

- povaha, rozsah, kontext a účel zpracování;

- rizika pro práva a svobody fyzických osob.

Konkrétní podoba opatření přijatých k zajištění ochrany osobních údajů se bude odvíjet mimo jiné od způsobu, kterým zaměstnavatel osobní údaje zaměstnanců zpracovává. Jsou-li například obsaženy v písemné podobě v osobních dotaznících, které jsou založeny v osobních spisech zaměstnanců, musí být tyto osobní spisy uloženy na takovém místě a takovým způsobem, aby k nim měly přístup pouze oprávněné osoby. Pravidlem by tedy mělo být, že budou osobní spisy zamčeny s tím, že ke klíčům budou mít přístup pouze zaměstnanci, kteří přístup k osobním údajům ostatních zaměstnanců potřebují za účelem plnění svých pracovních povinností.

* **Sestavte se přehled ochrany osobních údajů** jak v listinné, tak digitální podobě. Uveďte, jaký je současný stav, a z toho vyjděte při stanovení případných opatření.
* Zamyslete se, jaké je riziko zneužití nebo úniku informací, jaké jsou způsoby, jak by k tomu mohlo dojít, a jaká přijmout opatření k zamezení takové situace. Určete osobu, které se budou hlásit případné **incidenty**, a jakým způsobem.
* Způsob ochrany není nijak závazně nařízením stanoven. **Uveďte**, že jste při posouzení zohlednili zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
* Zvažte využití některých cloudových služeb, což umožní dosažení pracovních dat např. i z domova, bez nutnosti přenášet je na pevných nosičích, což je vždy spojeno s možností jejich ztráty či krádeže).

Základem samozřejmě je zabezpečení pracovních počítačů (hesla, uzamykatelné prostory), zálohování dat.

Data v listinné podobě - zabezpečení šanonů a skříní v uzamykatelných prostorách nejlépe s bezpečnostními zámky, stejně tak případný archiv.

Současný archiv proberte a skartujte jeho nadbytečný obsah.

Nařízení GDPR jako příklad zabezpečení uvádí (článek 32)

1. pseudonymizaci a šifrování osobních údajů;
2. schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
3. schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
4. pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Souvisejícím opatřením směřujícím k zabránění zneužití osobních údajů by mělo být to, že zaměstnavatel upozorní zaměstnance s přístupem k osobním údajům na povinnost mlčenlivosti, kterou ve vztahu k veškerým osobním údajům mají. Zaměstnavatel rozhodně nic nezkazí ani tím, pokud uvedené zaměstnance k povinnosti mlčenlivosti zaváže ve zvlášť uzavřené dohodě.

Součástí zabezpečení budou **pravidelná školení** osob, které přicházejí do styku s osobními údaji. O proškoleních založte doklady ve složce GDPR.

**Výsledkem analýzy bude přehled o zabezpečení osobních dat a doporučení, zda a jak je potřebné udělat změny.**

# Zpracovatelé – dodavatelé služeb

Proveďte **revizi** formulářů obsahujících osobní data, obchodních smluv a smluv s dodavateli, kteří zpracovávají Vaše osobní údaje. Opět nezapomeňte na dokumentaci - uveďte, že jste to provedli, a co jste zjistili, zda je nebo není nutné provést změny.

S každým dodavatelem, kterému jakýmkoli způsobem předáváte osobní údaje zaměstnanců nebo zákazníků - fyzických osob, je nutné mít uzavřenu **smlouvu o zpracování osobních údajů**, která bude obsahovat níže uvedené předepsané náležitosti, anebo je nutné uvedené náležitosti inkorporovat do stávajících nebo nově uzavíraných smluv o dodávce služeb. Může jít o externí mzdovou účtárnu, IT nebo jiného dodavatele, který v rámci své činnosti disponuje s Vašimi osobními údaji (resp. s osobními údaji, které jste Vy shromáždili a za něž Vy nesete zodpovědnost).

Správce by měl využít pouze takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů (článek 28 nařízení). V písemné smlouvě mezi správcem a zpracovatelem musí být za tím účelem **stanoven**

* předmět zpracování
* doba trvání zpracování
* povaha a účel zpracování
* typ osobních údajů a kategorie subjektu údajů
* povinnosti a práva správce.

Kromě těchto skutečností ve smlouvě ve vztahu ke zpracování osobních údajů uveďte náležitosti dle článku 28 odst. 3 nařízení GDPR.

„Zpracovatel:

1. zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
2. zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
3. přijme všechna opatření požadovaná k zabezpečení zpracování podle článku 32 nařízení GDPR;
4. nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky. Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel;
5. zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III nařízení GDPR;
6. je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36 nařízení GDPR, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;
7. v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;
8. poskytne správci veškeré informace potřebné k doložení toho, že byly splněny stanovené povinnosti, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.“

# Záznamy zpracování a předchozí posouzení vlivu

Nařízení GDPR **neupravuje povinnost správců předem oznámit započetí zpracování osobních údajů** či jeho změnu Úřadu pro ochranu osobních údajů (ÚOOÚ). Namísto toho zavádí jiné povinnosti. Jedná se zejména o povinnost správců a zpracovatelů vést záznamy o činnostech zpracování (článek 30), a povinnost za stanovených podmínek provést posouzení vlivu na ochranu osobních údajů, a v návaznosti na to případně projít předchozí konzultací s dozorovým úřadem (článek 35 a 36).

Předmětem záznamové povinnosti **je vedení písemných záznamů** (i v elektronické podobě) o jednotlivých činnostech a úkonech zpracování osobních údajů, **jejich obsah je obdobný obsahu dřívější oznamovací povinnosti vůči ÚOOÚ**. Záznamy by měly sloužit pro přehled a průběžnou aktualizaci systému zpracování, tak pro případnou kontrolu dozorového úřadu (a prokázání souladu s nařízením GDPR). Lze konstatovat, že **obsahem** takového záznamu je v podstatě to, co je obsahem analýzy, popsané výše. S tím, že jednou za čas provedete aktualizaci.

**Povinnost vést záznamy** o zpracování osobních údajů se vztahuje na správce i na zpracovatele, kteří zaměstnávají 250 nebo více osob, nebo na správce a zpracovatele, u nichž zpracování představuje pravděpodobně riziko pro práva a svobody subjektů údajů, nebo u nichž není příležitostné, anebo zahrnuje zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či zvláštních kategorií osobních údajů.

Sami vidíte, že toto vymezení je poněkud nesmyslné – nejprve se stanoví podmínka minima 250 zaměstnanců, posléze však také parametr nikoli příležitostnosti a nikoli zpracování zvláštních kategorií osobních údajů, se kterými však přichází do styku všichni zaměstnavatelé (zdravotní stav - pracovnělékařské posudky, pracovní neschopnost). Zpracování osobních údajů u zaměstnavatelů také není tak zcela příležitostné, neboť osobní údaje zaměstnanců zpracovávají opakovaně. Počkejme si na praxi a výkladová stanoviska, nicméně i v této chvíli se musíme nějak zařídit. Lze zaujmout názor, že tvůrce nařízení bezpochyby věděl, že i zaměstnavatel zaměstnávající méně než 250 osob zpracovává trvale jejich osobní údaje, které jsou nezbytné pro plnění smlouvy a právních povinností, a že toto zpracování je stálé, nikoli tedy v pravém slova smyslu „příležitostné“ – přesto stanovil uvedenou hranici. Zpracování „běžných“ údajů zaměstnance bychom tak pro účel povinnosti vést záznamy nebrali v úvahu. Přitom přihlížíme také k tomu, co uvádí **recitál 13** k zamýšlenému záměru: *Řádné fungování vnitřního trhu vyžaduje, aby volný pohyb osobních údajů v Unii nebyl z důvodů souvisejících s ochranou fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán. Aby byla zohledněna specifická situace mikropodniků a malých a středních podniků, obsahuje toto nařízení odchylku pro organizace s méně než 250 zaměstnanci týkající se uchovávání údajů. Kromě toho jsou orgány a instituce Unie, členské státy a jejich dozorové úřady podporovány v tom, aby specifické potřeby mikropodniků a malých a středních podniků zohledňovaly při uplatňování tohoto nařízení.*

DPIA (*Data Protection Impact Assessment*) neboli **předchozí posouzení vlivu** zamýšleného zpracování osobních údajů na jejich ochranu bude vyžadováno, bude-li pravděpodobné, že určitý druh zpracování přinese vysoké riziko pro práva a svobody subjektů údajů. Jako příklad nařízení GDPR uvádí, že posouzení bude nezbytné mj. pro případy rozsáhlého zpracování citlivých údajů nebo systematického a rozsáhlého vyhodnocování osobních aspektů (např. profilování) jako podkladu pro určitá automatizovaná rozhodnutí – může se to tedy dotknout nemocnic či e-shopů. Dozorovými úřady členských států Evropské unie by navíc měly být sestaveny seznamy druhů operací podléhajících požadavku tohoto posouzení. Lze předpokládat, že u většiny zaměstnavatelů, konkrétně ve vztahu k jejich zaměstnancům, tato povinnost nevznikne, ledaže by zaměstnavatel například využíval nové technologie skýtající vysoké riziko pro práva zaměstnanců, např. různé monitorovací softwary.

Základem DPIA bude posouzení rizik a možných opatření pro jejich zmírnění. V případě, že by z tohoto posouzení vyplývalo, že zamýšlené zpracování přinese vysoké riziko, pokud by správce nepřijal příslušná opatření k jeho zmírnění, bude povinností správce předběžně konzultovat svůj záměr s dozorovým úřadem (ÚOOÚ).

Zamýšlí-li zaměstnavatel použít jakoukoliv **monitorovací technologii** nebo aplikaci původně třeba zaměřenou na ochranu před únikem dat, která by nicméně mohla sloužit ke sledování zaměstnanců, měl by zvážit přiměřenost zaváděných opatření, ale také kroky, které by omezily dopad těchto opatření na soukromí zaměstnanců. DPIA je tady na místě.

**Návrh zákona o zpracování osobních údajů (ZOOÚ)**, který nahradí stávající zákon o ochraně osobních údajů a implementuje nařízení GDPR do českého právního řádu s využitím povolených výjimek nebo upřesnění (viz kapitola 9), k tomu stanoví, že **pokud právní předpis ukládá nějakou povinnost, jejíž součástí je i zpracování osobních údajů (např. zaměstnavatel musí zpracovávat osobní údaje pro účely sociálního pojištění), nemusí správce provádět posouzení vlivu na ochranu osobních údajů, neboť by to bylo nadbytečné a představovalo nadměrnou zátěž, protože by to nemohlo vést k nesplnění uložené povinnosti.**

**Zvažte, zda jste správcem, na kterého by dopadaly výše uvedené povinnosti. V analýze uveďte, zda ano nebo ne – a proč. Důležité je podchytit, že jste se touto otázkou zabývali, a došli jste k názoru, že uvedené povinnosti nemáte** (popř. máte), s odůvodněním uvedeným v této kapitole.

# Práva subjektu údajů

Subjekt údajů by měl být poučen o právech, která mu v souvislosti se zpracováním jeho osobních údajů náleží (články 12-22 nařízení GDPR). Kromě stávajících práv

* práva na přístup k vlastním osobním údajům a **informacím** o jejich zpracování,
* práva na opravu či omezení zpracování,
* práva na výmaz osobních údajů,
* práva vznést námitku proti zpracování osobních údajů a
* práva nestát se předmětem automatizovaného rozhodování,

náleží subjektům údajů také další práva, jako třeba právo na výmaz (právo být zapomenut) - je v nařízení GDPR podrobně upraveno v návaznosti na dříve přijatou judikaturu soudních institucí Evropské unie. Jedná se o povinnost správce zlikvidovat osobní údaje, je-li naplněn jeden z vymezených důvodů (článek 17 nařízení GDPR). Zaměstnavatel tak bude povinen vymazat osobní údaje zaměstnance např. v případě, kdy osobní údaje již nebude potřebovat pro původní účely zpracování. Právo na výmaz však není bezvýjimečné, a zaměstnavatel si vyhodnotí, zda nebo do jaké míry se v konkrétním případě uplatní některá z výjimek.

Obsah informace upravuje článek 13 (informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů - tedy od toho, koho se osobní informace týkají) a 14 (ostatní).

Lze konstatovat, že u údajů, které zpracováváte na základě smlouvy (pracovněprávní nebo jiné), je subjekt, který Vám je poskytuje, zároveň informován o tom, jaké údaje poskytuje a k jakému účelu (a na jakém právním základě).

* Pokud provádíte profilování zákazníků, vložte do svých pravidel ochrany osobních údajů souhlas zákazníka s profilováním podle GDPR (článek 4 bod 11 a článek 7 GDPR) a zajistěte souhlas zákazníka s těmito podmínkami.
* U objednávky budete mít zaškrtávací políčko pro všeobecné obchodní podmínky a vedle toho zaškrtávací políčko pro pravidla ochrany osobních údajů (obě políčka samostatně).
* Zpracováváte osobní údaje potenciálních zákazníků pro účely marketingu? Pokud ano, máte souhlas s marketingem v souladu s GDPR?
* Zasíláte stávajícím zákazníkům newslettery? Zákazník musí mít možnost odhlásit se z odběru v každém emailu. Odhlášení by nemělo být podmíněné žádným složitým úkonem a mělo by být možné na jedno kliknutí s okamžitou platností.

# Ohlašování případů porušení zabezpečení

Nově je dle nařízení GDPR (článek 33) každý správce povinen ohlásit dozorovému úřadu (ÚOOÚ) jakýkoliv případ porušení zabezpečení osobních údajů, tzv. "data breaches" – např. útok hackerů nebo jiné případy úniku nebo zničení osobních údajů - **s výjimkou případu, kdy je nepravděpodobné, že by porušení představovalo riziko pro práva a svobody subjektů údajů**. Správce je povinen učinit ohlášení bez zbytečného odkladu, nejpozději do 72 hodin od zjištění jednotlivého případu. Je-li navíc pravděpodobné, že porušení zabezpečení osobních údajů představuje vysoké riziko pro práva a svobody subjektů údajů, je správce povinen případ porušení oznámit také dotčeným subjektům údajů, tedy dotčeným zaměstnancům a/nebo klientům, a to za použití jasných a jednoduchých jazykových prostředků (článek 34 nařízení GDPR). Součástí oznámení je mj. informace o povaze porušení zabezpečení osobních údajů, jeho pravděpodobné důsledky a popis následně správcem přijatých nebo navržených opatření k řešení situace. Oznamovací povinnost přitom zjednodušeně řečeno nevzniká v případech přijetí dostatečných předběžných opatření (např. šifrování nebo pseudonymizace údajů) nebo následných opatření (článek 34 odst. 3 nařízení GDPR). Vyžadovalo-li by oznámení nepřiměřené úsilí, subjekty údajů mohou být informovány pomocí veřejného oznámení nebo podobného opatření.

**Seznamte se s tím, jakým způsobem postupovat v případě porušení zabezpečení. Určete zaměstnance, u kterého se budou případy porušení hlásit.**

# Zákon o zpracování osobních údajů

Upravuje některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou obecným nařízením upraveny nebo se umožňuje či předpokládá jejich úprava vnitrostátní úrovni. Mezi ně patří např. aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu, vědeckého nebo historického výzkumu nebo pro statistické účely.

Zákon by měl obsahovat kromě jiného výjimky z poučovací a informační povinnosti správce, ochranu zdroje a obsahu informací, výjimky z práv na opravu, na výmaz a na omezení zpracování osobních údajů, omezení práva na námitku, a další výjimky ve speciálních případech.

Pro představu lze načrtnout několik navržených ustanovení:

§ 7 stanoví způsobilost dítěte pro souhlas se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku.

§ 9 upravuje možnost oznámení formou změny výchozí evidence: je-li správce povinen oznámit příjemci provedenou opravu, omezení zpracování nebo výmaz osobních údajů, může tak učinit změnou osobních údajů v evidenci, pokud příjemci pravidelně zpřístupňuje její platný obsah.

§ 10 obsahuje výjimku z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů - správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.

Jmenování pověřence pro ochranu osobních údajů určuje navržený § 14 kromě orgánů veřejné moci také orgánům zřízeným zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu.

Novinářská zpracování nebo užití pro účely akademického, uměleckého nebo literárního projevu upravuje § 16 (17) a následující.

Návrh obsahuje dále také speciální ustanovení o ochraně osobních údajů při jejich zpracování za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, a zajišťování obranných a bezpečnostních zájmů České republiky.

Návrh zákona o zpracování osobních údajů je obsahem sněmovního tisku 138/0, podané pozměňovací návrhy tisk 138/12, doprovodný zákon pak tisk 139/0 a podané pozměňovací návrhy k němu 139/11. Oba návrhy jsou v současné době (konec října 2018) v Poslanecké sněmovně před 3. čtením.

# Propojení článků a recitálů GDPR

|  |  |  |  |
| --- | --- | --- | --- |
| článek | recitál | článek | recitál |
| **1** | **1 až 13** | **45** | **103 až 107** |
| **2** | **14 až 21** | **46** | **108, 109** |
| **3** | **22 až 25** | **47** | **110** |
| **4** | **26 až 37** | **49** | **111 až 116** |
| **5** | **39** | **51** | **117 až 119** |
| **6** | **40 až 50** | **52** | **118, 120** |
| **7** | **32, 33, 42, 43** | **53** | **121** |
| **8** | **38** | **55** | **122** |
| **9** | **51 až 56** | **56** | **124 až 128** |
| **11** | **57** | **57** | **123, 132** |
| **12** | **58, 59** | **58** | **129** |
| **13** | **60 až 62** | **60** | **124 až 128, 130, 131** |
| **14** | **60 až 62** | **61** | **133** |
| **15** | **63, 64** | **62** | **134** |
| **16** | **65** | **63** | **135** |
| **17** | **65, 66** | **64** | **136** |
| **18** | **67** | **66** | **137, 138** |
| **20** | **68** | **68** | **139** |
| **21** | **69, 70** | **69** | **139** |
| **22** | **71, 72** | **70** | **139** |
| **23** | **73** | **75** | **140** |
| **24** | **74 až 77, 83** | **77** | **141** |
| **25** | **78** | **78** | **143** |
| **26** | **79** | **79** | **145** |
| **27** | **80** | **80** | **142** |
| **28** | **81** | **81** | **144** |
| **30** | **13, 39, 82** | **82** | **146, 147** |
| **32** | **74 až 77, 83** | **83** | **148, 150, 151** |
| **33** | **75, 85, 87, 88** | **84** | **149, 152** |
| **34** | **75, 86, 87, 88** | **85** | **153** |
| **35** | **75, 84, 89 až 93** | **86** | **154** |
| **36** | **94 až 96** | **88** | **155** |
| **37** | **97** | **89** | **156 až 163** |
| **38** | **97** | **90** | **164** |
| **39** | **97** | **91** | **165** |
| **40** | **98, 99** | **92** | **166 až 170** |
| **42** | **100** | **94** | **171** |
| **44** | **101, 102** | **95** | **173** |