HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

NOVÁ PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ

MĚNÍME VIZE
VE SKUTEČNOST

www.komora.cz

Výhrada: *Cílem dokumentu je poskytnutí základních informací pro podnikání. Hospodářská komora ČR objektivně nemůže převzít odpovědnost za naprostou správnost, úplnost a aktuálnost jí poskytovaných informací. Hospodářská komora ČR postupuje s odbornou péčí, ale neodpovídá za škodu vzniklou v souvislosti s poskytnutými informacemi.*

OBSAH

ÚVOD

25. května 2018 začnou platit nová pravidla ochrany osobních údajů. Konkrétně vstoupí v účinnost nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů), kterým se zrušuje směrnice 95/46/ES (dále „**GDPR**“).

Jak se mají firmy připravit? Kolik je to bude stát? A týká se nová regulace opravdu každého? Na tyto a další otázky přinášíme odpovědi v naší nové příručce, v níž na příkladu imaginární společnosti Nebojsa s.r.o. ilustrujeme praktické dopady nové právní úpravy.

PROČ VZNIKLO GDPR?

Jako reakce na technologický pokrok v oblasti informačních a komunikačních technologií. Dnes se osobní údaje zpracovávají daleko komplexněji a používají se nové metody, např. profilování či automatizované zpracování osobních údajů. GDPR tak především posiluje ochranu dat občanů.

PROČ BY SE MĚLA SPOLEČNOST NEBOJSA S.R.O. ZABÝVAT GDPR?

- Má 10 000 zákazníků, především fyzických osob.
- Zaměstnává 10 zaměstnanců.
- Provozuje e-shop s knihami.
- Používá CRM a interní databázi kontaktů.
- Je správcem osobních údajů.
- Osobní údaje pro ni zpracovává externí firma (zpracovatel).
- Mzdovou agendu zaměstnanců zpracovává externí firma.

Všechny výše zmíněné činnosti spadají do pole působnosti GDPR, proto je nutné, aby se Nebojsa s.r.o. včas připravila.

Jak pracovat s příručkou?

Příručka je pro lepší přehlednost rozdělena do dvou částí. První část přináší přehled hlavních pilířů úpravy GDPR. Druhá část je zaměřená prakticky, aby firmy, v našem modelovém případě společnost Nebojsa s.r.o., věděly, jaké kroky učinit pro implementaci pravidel GDPR.

ČÁST PRVNÍ

ZÁKLADNÍ INFORMACE

Dne 25. května 2018 nahradí GDPR v českém právním řádu zákon č. 101/2000 Sb., o ochraně osobních údajů (dále „zákon o ochraně osobních údajů“ nebo „zákon“).

Je tedy rozdíl mezi nařízením EU a zákonem?
Jak nařízení EU, tak zákon stanoví práva a povinnosti přímo adresátům, v našem případě tedy přímo společnosti Nebojsa s.r.o., jejím zaměstnancům a zákazníkům. Nařízení EU má však přednost před zákonem. Je tzv. přímo aplikovatelné a závazné pro všechny členské státy EU. Ty si nemohou upravit pravidla odlišně. Proto je třeba zákon o ochraně osobních údajů upravit tak, aby byl v souladu s GDPR.

Právní úpravu ochrany osobních údajů tvoří GDPR a zákon o ochraně osobních údajů.

HLAVNÍ ZNAKY GDPR

- Je jednotně aplikovatelné v celé EU.
- Rozšiřuje pojem osobních údajů.
- Zpřesňuje souhlas se zpracováním osobních údajů.
- Vyžaduje vyšší technickou a organizační bezpečnost správců a zpracovatelů.
- Při rozsáhlém a systematickém zpracování osobních údajů požaduje jmenování pověřence na ochranu osobních údajů (DPO - Data Protection Officer).
- Zavádí novou povinnost - vést záznamy o činnostech zpracování.
- Při rizikových zpracováních osobních údajů požaduje předchozí provedení posouzení vlivu na ochranu osobních údajů (DPIA - Data Protection Impact Assessment) a případně též konzultaci s Úřadem na ochranu osobních údajů (dále „**ÚOOÚ**“).
- Posiluje stávající práva fyzických osob (občanů, zákazníků) a zakládá práva nová – právo být zapomenut či právo na přenositelnost údajů, např. při změně banky.
- Porušení ochrany dat musí být oznámeno do 72 hodin ÚOOÚ a v některých případech i fyzické osobě.
- Zavádí nepoměrně vyšší sankce za porušení ochrany osobních údajů - oproti dosavadní maximální částce 10 mil. Kč bude možné uložit sankce až do výše 20 mil. eur nebo 4 % celosvětového obratu podniku.

BUDE OPRAVDU VŠECHNO JINÉ?

Při srovnání právní úpravy zákona o ochraně osobních údajů s GDPR se ukazuje, že nové pojmy nejsou žádnou revolucí. V mnoha případech se jedná o upřesnění spíše než o zpřísnění:

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Osobní údaje - jakákoliv informace týkající se určeného nebo určitelné fyzické osoby. Fyzická osoba se považuje za určenou nebo určitelnou, jestliže ji lze přímo či nepřímo identifikovat **zejména** na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.	**Osobní údaje** - veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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.
Citlivý údaj - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě fyzické osoby a genetický údaj fyzické osoby; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci fyzické osoby.	**Citlivé údaje** - jsou speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob.
Anonymní údaj - takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určené nebo určitelné fyzické osobě.	**GDPR se nevztahuje na anonymní data.**
Oznamovací povinnost – ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů před zpracováním osobních údajů.	**Tato povinnost bude zrušena.**
Likvidace osobních údajů – správce, nebo na základě jeho pokynu, zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti fyzické osoby	**Právo být zapomenut –** subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se dané fyzické osoby týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat.
Přístup subjektu údajů k informacím – požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.	**Právo na přístup –** fyzická osoba má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.
Ochrana práv subjektů údajů – je-li žádost fyzické osoby shledána oprávněnou, správce	**Právo na opravu –** fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil

nebo zpracovatel odstraní neprodleně závadný stav.	nepřesné osobní údaje, které se jí týkají. S přihlédnutím k účelům zpracování má fyzická osoba práva na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.
Toto právo není v zákoně upraveno.	**Právo na přenositelnost údajů** – fyzická osoba má právo získat osobní údaje, které se jí týkají, jež poskytla správci ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.
Tato povinnost není v zákoně upravena.	**Posuzování vlivu na ochranu osobních údajů** – pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro právo a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.
Tato povinnost není v zákoně upravena.	**Pověřenec pro ochranu osobních údajů** – správce a zpracovatel jmenují pověřence pro ochranu osobních údajů.
Tento časový údaj není v zákoně uveden.	**Porušení ochrany dat** – jakékoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu.
Sankce – max. do výše 10 000 000 Kč (nebyla nikdy uložena).	**Sankce** – 10 000 000 EUR nebo do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, 20 000 000 EUR nebo do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok.

DŮLEŽITÉ POJMY

- ***Osobní údaje*** = veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.

Prvky osobních údajů:

- obecné: jméno, pohlaví, věk, datum narození, osobní stav, občanství, IP adresa;
- organizační: pracovní nebo osobní adresa, telefonní číslo, email, ověřovací identifikační údaje;
- citlivé osobní údaje: speciální kategorie - ještě více zpřísněna - rasový původ, politické názory, genetické údaje (např. DNA), biometrické údaje (např. otisk prstu).

Z působnosti GDPR jsou vyloučeny anonymizované údaje a údaje zemřelých osob.

- ***Fyzická osoba*** = každý, jehož osobní údaje jsou zpracovávány, typicky zákazník, klient.

Společnost Nebojsa s.r.o. zpracovává osobní údaje svých zaměstnanců a zákazníků.

- ***Správce*** určuje účel a prostředky zpracování osobních údajů. Jedná se o OSVČ nebo právnickou osobu, která nabízí zboží a služby rezidentům EU a při své činnosti zpracovává osobní údaje.

Správcem osobních údajů je samotná právnická osoba, tedy společnost Nebojsa s.r.o.

- ***Zpracovatel*** zpracovává osobní údaje pro správce.

Zpracovatelem je externí společnost, která zpracovává mzdovou agendu pro společnost Nebojsa s.r.o.

- ***Zpracování*** = operace nebo soubor operací s osobními údaji prováděných pomocí či bez pomoci automatizovaných postupů, jako je:

  - **Shromažďování** - sběr dat, získávání či vytěžování dat z různých zdrojů (dotazníky, přihlášky, veřejné rejstříky atd.)
  - **Zaznamenání** - zápis dat (údajů) do předem definovaných polí
  - **Uspořádání** - zvolený způsob organizace dat
  - **Strukturování** – zápis dat podle předem definovaných standardů
  - **Uložení** – zapsání dat do souboru či dokumentu, požadavek na uchování dat
  - **Přizpůsobení nebo pozměnění** – upravení dat dle potřeby
  - **Vyhledání** - nalezení správných údajů dle zadaného požadavku či kritéria
  - **Nahlédnutí** – možnost podívat se na požadované informace bez možnosti získání papírové či elektronické formy výstupu
  - **Použití** – aplikování dat dle potřeby
  - **Zpřístupnění přenosem** – zaslání/předání elektronickou formou (e-mail, internet)
  - **Šíření nebo jiné zpřístupnění** – poskytnutí dat veřejnosti papírovou či elektronickou formou
  - **Seřazení či zkombinování** – třídění/zobrazení dat dle zadaného kritéria či vytažení dat z více zdrojů a složení dle pravidel
  - **Omezení** – získání či poskytnutí pouze určitých dat
  - **Výmaz nebo zničení** – zrušení záznamu či poškození nosiče dat, vymazání osobních dat z databáze

POZOR! Nevztahuje se na zpracování osobních údajů:

- v rámci činností fyzické osoby v čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, tedy bez jakékoliv souvislosti s profesní nebo obchodní činností (např. vlastní seznam telefonních a dalších kontaktů ve smart phonu);

- příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonů trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

KDY JE ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOULADU SE ZÁKONEM?

Níže uvádíme 3 nejdůležitější podmínky:

➢ **jde o zpracování, k němuž správce/zpracovatel získal souhlas**

Nebojsa s.r.o. získává souhlas se zpracováním osobních údajů od zákazníků pomocí předdefinovaného „zaškrtávacího políčka" na webovém formuláři objednávky zboží. Nebojsa s.r.o. má zpracování osobních údajů zákazníků (jméno, příjmení, adresa bydliště, e-mail) řádně nahlášené u ÚOOÚ.

POZOR!
S příchodem GDPR se ohlašovací povinnost vůči ÚOOÚ ruší, protože se zpřísňují požadavky na zpracování osobních údajů. Souhlas se zpracováním osobních údajů musí být dán svobodně a ke konkrétnímu účelu. Tento účel musí být jednoznačně specifikován a musí být prokazatelně doložen po celou dobu zpracování.

➢ **zpracování osobních údajů je nezbytné pro splnění smlouvy**

Nebojsa s.r.o. má uzavřenou se zákazníkem smlouvu na koupi zboží. Výslovný souhlas se zpracováním osobních údajů není potřeba dávat do smlouvy, protože osobní údaje obsažené ve smlouvě jsou nezbytné pro splnění smluvní povinnosti.

➢ **zpracování je nezbytné pro splnění právní povinnosti**

Nebojsa s.r.o. jako zaměstnavatel zpracovává osobní údaje zaměstnanců. Tyto údaje musí Nebojsa s.r.o. shromažďovat z důvodu zákonné[1] povinnosti vést mzdovou a personální agendu (např. jméno a příjmení zaměstnance, rodné číslo, datum narození, mít informaci o tom u jaké zdravotní pojišťovny je zaměstnanec veden, osobní hodnocení zaměstnance, mzdy). Nebojsa s.r.o. tyto údaje zpracovává po určité období a v určitém rozsahu.

[1] *Zvláštní právní předpisy, které zaměstnavateli ukládají povinnost zpracovávat osobní údaje ke stanoveným účelům:*
- *zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů*
- *zákon č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů*
- *zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů*
- *zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů*
- *zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů*

JAKÁ PRÁVA MÁ FYZICKÁ OSOBA, TYPICKY ZAKÁZNÍK?

PRÁVO NA PŘÍSTUP

- Právo získat potvrzení, zda osobní údaje jsou či nejsou zpracovány. Jsou-li zpracovány, právo získat ke svým údajům přístup.
- Právo vědět k jakému účelu jsou data zpracovávána, právo být informován o kategorii dotčených osobních údajů (zda jde o osobní či citlivá data), kdo bude příjemcem osobních údajů, na jakou dobu budou data zpracována, jak podat stížnost u ÚOOÚ. Informace o tom, zda dochází k automatizovanému zpracování včetně profilování. Profilováním se obecně rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě. V praxi k němu běžně dochází např. při žádosti o úvěr, kdy banka hodnotí bonitu klienta pro účely poskytnutí úvěru.

Příklad Na společnost Nebojsa s.r.o. se obrátí prostřednictvím e-mailu její zákazník Pavel Antonín, že by rád viděl kopie svých objednávek zboží od začátku svojí registrace. Zaměstnanec obchodního oddělení společnosti Nebojsa s.r.o. nejprve kontaktuje zákazníka a ověří, že požadavek opravdu přišel od Pavla Antonína. Následně se obrátí na svého kolegu z IT oddělení, aby dohledal veškeré objednávky, které společnost eviduje u Pavla Antonína. Po vyhledání veškerých objednávek zaměstnanec obchodního oddělení posoudí, zda jde opravdu o relevantní informace, které si pan Pavel Antonín vyžádal a následně mu je elektronicky poskytne.

POZOR!
Právem na přístup nesmí být dotčena práva ostatních osob např. obchodní tajemství.

PRÁVO NA OPRAVU

- Při podezření na nesprávnost údajů právo požádat o nápravu a povinnost správce zajistit opravu bez zbytečného odkladu.

Příklad Klientka se vdala a je vedena u společnosti Nebojsa s.r.o. pod svým rodným příjmením. Požádá prostřednictvím e-mailu společnost Nebojsa s.r.o. o opravu příjmení. Ta bez zbytečného odkladu údaj ve své databázi opraví.

PRÁVO BÝT ZAPOMENUT

Správce bez zbytečného odkladu vymaže osobní údaje, pokud:

- osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány;
- zákazník odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování;
- osobní údaje byly zpracovány protiprávně;
- pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí v souvislosti s nabídkou služeb informační společnosti.

Rozšířením je **právo na výmaz**, tedy provedení přiměřených kroků, včetně technických opatření, k vymazání veškerých osobních údajů, včetně záloh a automatických obnov IT systémů.

Příklad: Klientka Alice Nováková požádá e-mailem společnost Nebojsa s.r.o., aby dohledala veškerá data, která o ní společnost vede. Zaměstnanec společnosti Nebojsa s.r.o. pan Jáchym ověří, že požadavek přišel opravdu od paní Alice Novákové a následně se obrátí na kolegu z IT oddělení. Kolega z IT prověří evidenci i zálohové systémy a nalezená data předá panu Jáchymovi. Ten zkontroluje, že se data opravdu týkají klientky a následně je elektronicky (např. ve formátu pdf.) předá paní Alici Novákové. Ta po prohlédnutí dat uplatní právo „být zapomenut" a požádá o výmaz

1. *svého hodnocení u zakoupené knihy – požadavek je akceptován a hodnocení smazáno;*
2. *všech svých objednávek – požadavek je zamítnut z důvodu povinnosti vést účetní záznamy;*
3. *osobních údajů souvisejících s jejím předchozím částečným pracovním úvazkem u společnosti Nebojsa s.r.o. – požadavek je zamítnut z důvodu povinnosti zaměstnavatele vést mzdovou a personální agendu;*
4. *své fotky, která byla použita pro marketingové účely jednoho z produktů společnosti Nebojsa s.r.o. – tento požadavek je přijat a fotka smazána.*

PRÁVO NA PŘENOSITELNOST[2]

Zákazník má právo získat své osobní údaje ve **strukturovaném, běžně používaném a strojově čitelném formátu**. Přenositelnost pak znamená povinnost správce předat osobní údaje zákazníka novému správci, zpravidla konkurenci. Toto právo posiluje postavení zákazníků, jelikož jim usnadní přesouvání, kopírování nebo přenášení osobních údajů z jednoho IT prostředí do druhého.

Příklad: Klientka Alice Nováková požádá e-mailem společnost Nebojsa s.r.o., aby veškeré tituly u ní zakoupených knih převedla společnosti Knihy s.r.o. Zaměstnanec společnosti Nebojsa s.r.o. ověří a vyhledá všechny zakoupené tituly knih a předá je ve formátu XML společnosti Knihy s.r.o.

JAKÉ POVINNOSTI MAJÍ FIRMY?

PORUŠENÍ OCHRANY DAT MUSÍ BÝT OZNÁMENO DO 72 HODIN

Správce/zpracovatel musí ohlásit únik či ohrožení zabezpečení osobních dat ÚOOÚ nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl.

Ohlášení musí přinejmenším obsahovat:

- popis povahy daného případu porušení zabezpečení osobních údajů (např. hackerský útok na internetové bankovnictví);

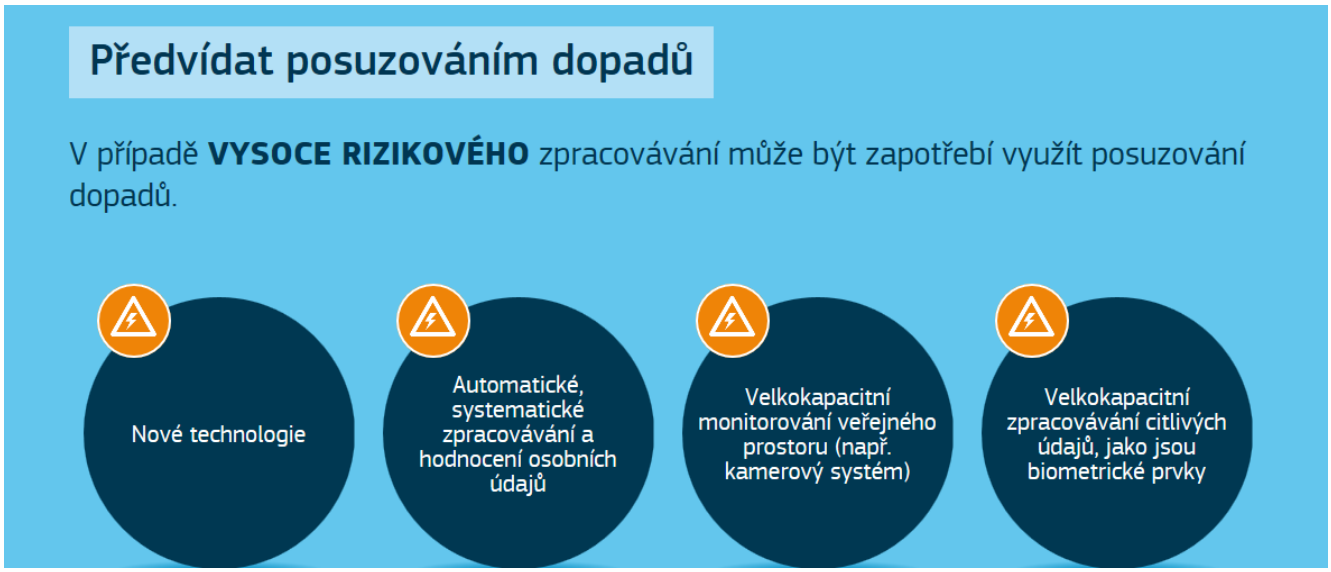
[2] Vodítka k právu na přenositelnost údajů jsou na stránkách www.uoou.cz.

- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů (např. pravděpodobnost neoprávněného přístupu k bankovním účtům);
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů (např. dočasné zablokování internetového bankovnictví a výzva klientům k bezodkladné změně hesel).

POZOR!
Jakmile se správce/zpracovatel dozví o porušení zabezpečení osobních údajů, musí včas informovat ÚOOÚ a v některých případech i fyzickou osobu/zákazníka.

POVINNOST POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ[3]

Firmy budou muset posoudit dopady v případě vysoké rizikovosti zpracování osobních údajů:



Zdroj: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

POZOR! Úřad pro ochranu osobních údajů připravuje seznam operací zpracování, které podléhají požadavkům posouzení vlivu.

Příklad: Pokud by společnost Nebojsa s.r.o. chtěla zpracovávat věrnostní program pro své zákazníky, na základě kterého by docházelo k profilování zákazníků podle počtu zakoupených knih a podle druhu knižních titulů, měla by nejprve zpracovat posouzení vlivu na ochranu osobních údajů. Musela by zároveň přijmout taková opatření, aby dodržela zásadu minimalizace zpracování osobních údajů a transparentnosti.

[3] Posuzování vlivu na ochranu osobních údajů je proces, který má popisovat zpracování, posuzovat nezbytnost a přiměřenost zpracování a napomáhat zvládnutí rizik pro práva a svobody fyzických osob vyplývajících ze zpracování osobních údajů.

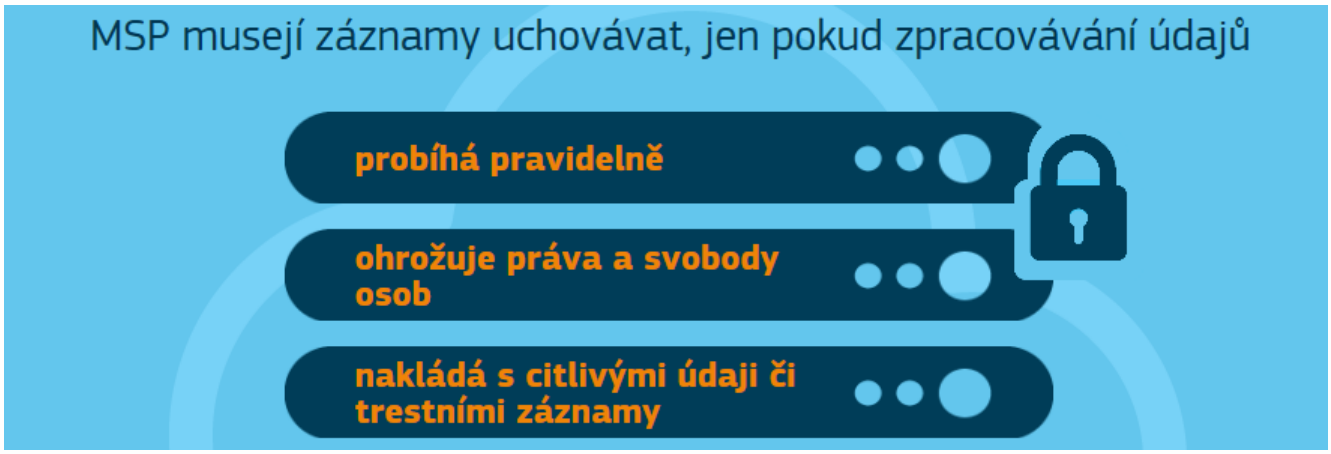
POVINNOST VÉST ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Každý správce a zpracovatel povede záznamy o činnostech zpracování, za něž odpovídá.

Záznamy obsahují:

- název a kontaktní údaje správce/právnické osoby;
- důvod zpracování údajů;
- popis kategorií subjektů údajů a osobních údajů;
- kategorie organizací, které údaje obdrží;
- přenos údajů do jiné země či organizace;
- lhůtu pro odstranění údajů;
- popis bezpečnostních opatření uplatňovaných při zpracovávání.

Výjimky z povinnosti vést záznamy o činnostech zpracování mají malé a střední podniky, které zaměstnávají méně než 250 zaměstnanců.

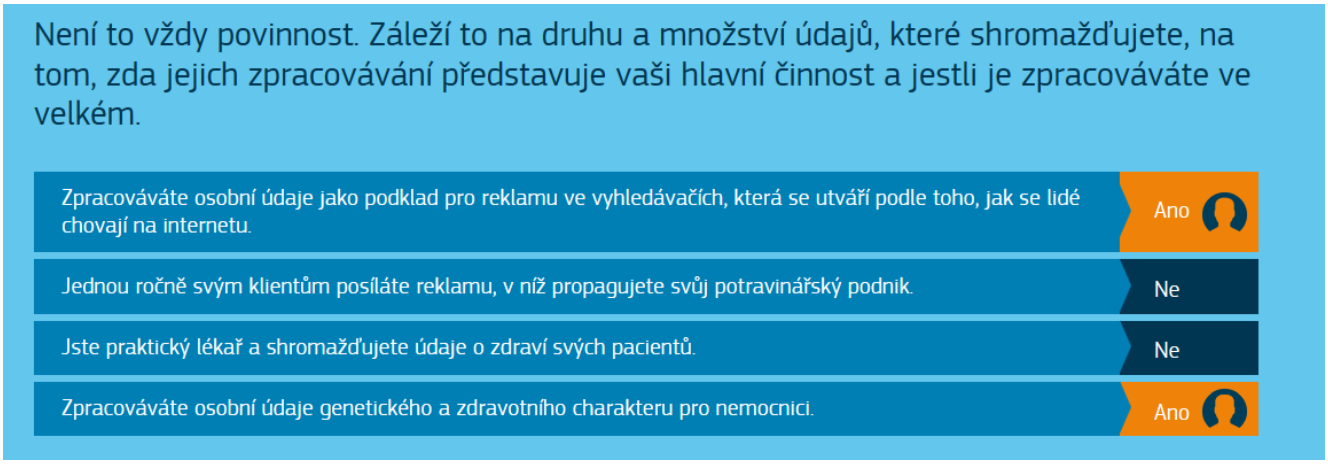


Zdroj: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

Výše uvedená výjimka se tedy nevztahuje na malé a střední podniky, jestliže jejich zpracování pravděpodobně představuje riziko pro práva a svobody fyzických osob, zpracování není příležitostné nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Příklad: I přesto, že má Společnost Nebojsa s.r.o. pouze 10 zaměstnanců, musí zpracovávat záznamy o činnostech, neboť zpracovává osobní údaje, které zahrnují profilování zákazníků (viz bod výše povinnost posouzení vlivu na ochranu osobních údajů).

POVINNOST JMENOVAT POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ[4]?



Zdroj: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

Úkolem pověřence je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z GDPR.

Povinnost jmenovat pověřence nastává ve třech případech:

1. Zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů).
2. Hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů.
3. Hlavní činností správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

POZOR! Za hlavní činnosti lze považovat klíčové operace směřující k dosažení cílů správce. Aby se jednalo o hlavní činnost podnikatele, musí být osobní údaje zpracovávány rozsáhle a musí souviset se základními činnostmi právnické osoby. Jde o veškeré aktivity podnikatele, kdy je zpracování osobních dat nedílnou součástí činnosti podnikatele.

Příklady rozsáhlého zpracování[5]:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice;
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové průkazky);
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost;
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky;
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy;
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb.

[4] Vodítka k pověřencům pro ochranu osobních údajů jsou na stránkách www.uoou.cz.
[5] Vodítka k pověřencům pro ochranu osobních údajů, která jsou k dispozici na stránkách www.uoou.cz.

Požadavky na osobu pověřence:

- Znalosti v oboru práva a praxe v oblasti ochrany osobních údajů
  i. Národní i evropská legislativa
  ii. Orientace v podnikání a vnitřním uspořádání správce

Úkoly pověřence:

- shromažďovat informace za účelem zjišťování zpracovatelských činností;
- analyzovat a prověřovat právní soulad zpracovatelských činností;
- informovat, radit a vydávat doporučení správci nebo zpracovateli;
- poskytovat poradenství/posudku při posuzování vlivu na ochranu osobních údajů a monitorování jeho uplatňování.

POZOR! Pověřenec nenese osobní odpovědnost za nedodržování GDPR. Odpovědnost za dodržení povinností leží na firmě.

Příklad: Společnost Nebojsa s.r.o. je pouze malou společností s vyhraněným sortimentem zboží a zpracovává osobní údaje zákazníků (jméno, příjmení, adresa bydliště, e-mail) pouze za účelem prodeje zboží. Nemusí tedy mít pověřence pro ochranu osobních údajů.

JAKÉ HROZÍ FIRMÁM SANKCE PŘI PORUŠENÍ POVINNOSTÍ?

GDPR zavádí oproti stávající právní úpravě několikanásobně vyšší pokuty - oproti dosavadním maximálně 10 mil. Kč bude možné uložit sankce až do výše 10 mil., resp. 20 mil. eur nebo 2%, resp. 4 % celosvětového obratu podniku. Aplikuje se vždy přísnější varianta.

Při udělení pokuty se posuzuje řada faktorů:

- povaha, závažnost a délka trvání porušení povinností;
- úmysl či nedbalost správce/zpracovatele;
- kroky podniknuté ke zmírnění škod;
- míra odpovědnosti správce či zpracovatele;
- veškeré relevantní předchozí porušení;
- míra spolupráce s ÚOOÚ;
- kategorie osobních údajů;
- způsob, jakým se ÚOOÚ dozvěděl o porušení.

Kromě sankcí mohou hrozit právnickým osobám žaloby podané fyzickými osobami s nárokem na náhradu způsobené újmy (např. únik údajů o sexuální orientaci).

POZOR!

- Maximální výše pokuty může být udělena jak malým podnikatelům, tak velkým národním korporacím.

Zdroj: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

ČÁST DRUHÁ

CO MUSÍ FIRMA UDĚLAT, ABY BYLA PŘIPRAVENÁ NA GDPR?

Znovu si připomeňme, že každá firma musí chránit práva zákazníků, zaměstnanců, zkrátka všech osob, které jí poskytují své osobní údaje. Jak tohoto cíle firma dosáhne, je v zásadě na ní. Důležitý je výsledek, tedy ochrana a zabezpečení údajů. Pravidla GDPR dopadají na firmu jako celek, nikoli pouze na některá oddělení, typicky IT či právní. Dotýkají se každého, kdo ve firmě pracuje s osobními údaji.

Přípravu na GDPR je vhodné rozdělit do několika etap:

1. ANALYTICKÁ ČÁST – INTERNÍ AUDIT

V této fázi je nezbytné zmapovat, jak se ve firmě zachází s osobními údaji.

Je nutné zjistit:

- jaký druh osobních údajů se zpracovává (např. citlivé údaje, údaje dětí);
- kdo s nimi pracuje (např. zaměstnanci jednotlivých odborů, externí dodavatelé);
- kde jsou uloženy (např. CRM, jiná elektronická či papírová evidence);
- na základě jakého právního titulu se osobní údaje zpracovávají (např. souhlas, smluvní povinnost, zákonné povinnosti);
- k jakému účelu jsou data zpracovávána (např. mzdová či personální agenda, marketingové služby);

- po jakou dobu jsou data zpracovávána (např. zda společnost osobní data smaže po ukončení projektu);
- kde a jak se osobní údaje archivují (např. externí úložiště, cloudové služby).

Prakticky je třeba do interního auditu zapojit jak vedení firmy, tak všechny odpovědné osoby.

Harmonogram auditu může být následující:

- úvodní porada vedení firmy - představení problematiky a rozsahu GDPR;
- vytvoření GDPR týmu – zástupci všech oddělení, která pracují s osobními údaji;
- audit jednotlivých oddělení;
- zpracování získaných informací;
- vytvoření závěrečné zprávy pro vedení společnosti s upozorněním na rizika a navržení praktických opatření.

Příklad: Společnost Nebojsa s.r.o. pro vypracování základní analýzy sestavila tým složený z právníka, zaměstnance IT, obchodu, marketingu a ekonomického oddělení. Při interním auditu se zjistilo, že obchodní oddělení zpracovává databázi zákazníků, která je přístupná všem zaměstnancům a obsahuje neaktuální data. Obchodní oddělení zpracovává osobní údaje zákazníku na základě souhlasu, který je uveden na jejich internetových stránkách. Oddělení marketingu si vede svojí vlastní databázi, kde má uvedené osobní údaje zákazníků pro marketingové účely. Oddělení marketingu zpracovává osobní údaje na základě souhlasu se zpracováním osobních údajů. Ekonomické oddělení zpracovává osobní údaje zaměstnanců a předává je externí firmě, která zajišťuje vedení mzdové a personální agendy. Tyto údaje jsou zpracovány na základě zákonné povinnosti zaměstnavatele.

2. PRAKTICKÁ ŘEŠENÍ

Na základě vypracované analýzy by měl návrh řešení obsahovat:

- **úpravu vnitřních norem a procesů společnosti:**
  - úprava vnitřních dokumentů;
  - zajistit školení zaměstnanců, kteří nakládají s osobními údaji;
  - připravit se na případné zpracování posouzení vlivu na ochranu osobních údajů;
  - zajistit potřebnou dokumentaci k záznamům o činnostech zpracování;
  - nastavit řešení bezpečnostních incidentů;
  - připravit se na zvláštní podmínky při zpracování osobních údajů dětí.
- **určení, zda společnost potřebuje pověřence pro ochranu osobních údajů**

  GDPR nestanoví žádné podmínky pro vzdělání či certifikování pověřence. Důležité je, aby měl znalosti a praktické zkušenosti v oblasti ochrany osobních údajů.
- **zajištění bezpečnosti zpracování osobních údajů**
  - osobní údaje musí být zabezpečeny podle kategorie např. osobní a citlivé údaje;
  - v závislosti na kategorii zpracování osobních údajů nutno vyhodnotit možná rizika;

- připravit postupy pro případné porušení ochrany dat. Nově musí být tato povinnost oznámena do 72 hodin Úřadu pro ochranu osobních údajů a v některých případech i dotčené fyzické osobě;
- zavedení technických opatření jako např. pseudonymizace (osobní údaje fyzické osoby jsou označeny číslem/kódem, přičemž spojovací číslo je vedeno odděleně od osobních údajů) a šifrování osobních údajů (postup, který převádí informace do nečitelné podoby na základě klíče/šifry). Nejde však o povinné podmínky zpracování osobních údajů, jde o bezpečnostní prvky, které mohou pomoci správci či zpracovateli osobních údajů.

3. REALIZAČNÍ FÁZE

Po výběru vhodných řešení přichází jejich implementace do života firmy. Efektivitu a praktičnost přijatých opatření je třeba pravidelně ověřovat, a to jak technickou úroveň, tak pravidelné školení zaměstnanců. Největším rizikem bezpečnosti ochrany dat je totiž lidský faktor. Pokud se podaří eliminovat tato rizika, je velká pravděpodobnost, že firma zvládne přechod na GDPR bez nepřiměřené zátěže a velkých nákladů. Výsledkem bude ochrana dat jak zevnitř, tak před případnými vnějšími útoky.

ZÁKLADNÍ DOPORUČENÍ

1. REVIDOVAT SOUHLASY SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Doporučujeme revidovat a podrobněji upravit souhlas se zpracováním osobních údajů, aby byl každý zákazník konkrétně informován, k jakému účelu poskytuje svoje osobní data. Takto revidovaný souhlas bude potřeba zajistit u nového zákazníka. U stávajících zákazníků je možné využívat již udělené souhlasy, pokud budou odpovídat výše uvedeným podmínkám.

Základem je jednoduchá a srozumitelná komunikace. Zákazník musí vědět, **kdo** zpracovává jeho osobní údaje (nutná identifikace podnikatele), musí vědět, **proč** jeho osobní údaje zpracovává (například za účelem nákupu zboží), **jak** dlouho je bude uchovávat (podnikatel by měl smazat data, se kterými nepracuje) a **kdo další** získá jeho osobní údaje (externí firma).

Chtěli bychom upozornit, že nejsou dostatečné souhlasy se zpracováním osobních údajů získané automatizovaným způsobem, např. pomocí předvyplněného „zaškrtávacího políčka“.

POZOR! Jestliže zpracováváte osobní údaje dětí ze sociálních sítí, ověřte jejich věk. Pro děti mladší 13, resp. 16 let (záleží na národní úpravě, v ČR to bude zřejmě 16 let) je nutný souhlas rodičů.

2. REVIDOVAT SMLOUVY

Doporučujeme revidovat smluvní vztahy mezi správcem (např. zaměstnavatel) a zpracovatelem (externí firmou). Smlouva musí jasně nastavit povinnosti a odpovědnost za případnou škodu každé ze smluvních stran. V případě outsourcingu doporučujeme mít smluvně upraveno, že

externí dodavatel zpracovává osobní údaje v souladu se všemi obecně závaznými právními předpisy, neboť přímá odpovědnost za řádné zpracování osobních údajů.

3. NEEXISTUJE GDPR EXPERT

Vždy půjde o týmovou práci lidí napříč celou firmou. GPDR není záležitostí jedince. V případě, že nemáte k dispozici odborníky ve všech oborech, je možné se obrátit na externí poradce. Již dnes je na trhu řada společností, které nabízejí řešení pro zajištění souladu s GDPR. Doporučujeme však vždy důkladně zvážit, i s ohledem na finanční zatížení, zda všechny nabízené služby jsou nezbytné (např. není potřeba mít certifikovaného pověřence osobních údajů).

ZÁVĚR

Osobní data jsou cenným aktivem každého podnikatele. Tvoří důležitou součást know-how a pro úspěšné podnikání je jejich ochrana v životním zájmu firmy. V poslední době totiž dochází stále častěji k neoprávněným únikům a krádežím dat, a to ve všech sektorech (od e-shopů přes banky až po státní správu). Proto lze nová pravidla, která přináší GDPR, vnímat pozitivně. Přiměje firmy, aby si „udělaly doma pořádek“:

- získaly jasný přehled o osobních datech, která vlastní;
- zlegalizovaly data, která spravují neoprávněně;
- zbavily se dat, která nepotřebují;
- nastavily procesy, které zabrání úniku dat a vzniku škod.

ZDROJE

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pobytu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

- Internetové stránky:

- http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=en
- www.uoou.cz
- https://www.uoou.cz/obecne-narizeni-eu-gdpr/ds-3938/p1=3938
- http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52946
- www.komora.cz

Vydala Hospodářská komora České republiky
Odbor legislativy, práva a analýz
Florentinum, Na Florenci 2116/15
110 00 Praha 1
tel.: +420 266 721 300
e-mail: office@komora.cz
www.komora.cz
Rok vydání: listopad 2017