

GDPR

NOVÁ PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ

Petr Daněk

GDPR

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“).

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 VAŠE FIRMA ZABÝVAT GDPR?

- 🕒 Má 10 000 zákazníků, především fyzických osob.
- 🕒 Zaměstnává 10 zaměstnanců.
- 🕒 Provozuje e-shop.
- 🕒 Používá CRM (Customer relationship management - řízení vztahů se zákazníky) a interní databázi kontaktů.
- 🕒 **Je správcem osobních údajů.**
- 🕒 Osobní údaje pro ni zpracovává externí firma (zpracovatel).
- 🕒 **Mzdovou agendu zaměstnanců zpracovává externí firma.**

GDPR

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.

GDPR

- ⌚ 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.
- ⌚ 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 obrátu podniku.

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 - údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, biometrické údaje, údaje o sexuální orientaci a trestních deliktech či pravomocném odsouzení osob.

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

DŮLEŽITÉ POJMY

🕒 **Fyzická osoba** = každý, jehož osobní údaje jsou zpracovávány, typicky zákazník, klient. Správce 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 a při své činnosti zpracovává osobní údaje.

Správce osobních údajů je samotná společnost (PO) nebo OSVČ (FO podnikající)

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

Např. zpracovatelem je externí společnost, která zpracovává mzdovou agendu

DŮLEŽITÉ POJMY

- **Zpracování**

- 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 i 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

DŮLEŽITÉ POJMY

- **Zpracování**

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 v smart fonu);

🕒 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

➤ zpracování osobních údajů je nezbytné pro splnění smlouvy

Správce 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

Správce jako zaměstnavatel zpracovává osobní údaje zaměstnanců. Tyto údaje musí správce shromažďovat z důvodu zákonné 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).

Správce – zaměstnavatel tyto údaje zpracovává po určité období a v určitém rozsahu.

KDY JE ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOULADU SE ZÁKONEM

- jde o zpracování , k němuž správce/zpracovatel získal souhlas

Správce získává souhlas se zpracováním osobních údajů od zákazníků podepsáním souhlasu se zpracováním osobních údajů nebo např. pomocí předdefinovaného „zaškrťovacího políčka“ na webovém formuláři objednávky zboží.

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.

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.

Příklad: Obrátí se na vás prostřednictvím e-mailu váš zákazník, že by rád viděl kopie svých objednávek zboží od začátku svojí registrace. Nejprve kontaktujte zákazníka a ověřte, že požadavek opravdu přichází od tohoto zákazníka. Následně dohledáte veškeré objednávky(zakázky), které u něj evidujete. Poté posoudíte, zda jde opravdu o relevantní informace, které si zákazník vyžádal a následně mu je elektronicky poskytnete.

POZOR!

Právelem na přístup nesmí být dotčena práva ostatních osob např. obchodní tajemství.

JAKÁ PRÁVA MÁ FYZICKÁ OSOBA, TYPICKY ZAKÁZNÍK

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 u vás vedena pod svým rodným příjmením. Požádá-li o opravu příjmení, údaj bez zbytečného odkladu ve své databázi opravíte.

JAKÁ PRÁVA MÁ FYZICKÁ OSOBA, TYPICKY ZAKÁZNÍK

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.

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

JAKÁ PRÁVA MÁ FYZICKÁ OSOBA, TYPICKY ZAKÁZNÍK

PRÁVO NA PŘENOSITELNOST

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: Klient vás požádá o výpis dpt hodnot, typu čoček nebo obruby a předání těchto informací jiné společnosti. Pozor zde by mohlo jít v případě dpt hodnot o citlivé informace a je nutné si vyžádat souhlas klienta s předáním těchto informací. (V tomto případě - pokud to bude možné- je jednodušší tyto informace předat přímo klientovi ať s nimi naloží dle svého.

JAKÉ MAJÍ POVINNOSTI FIRMY

POVINNOST POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ - DPIA

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

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

Společnosti či instituce jej budou muset vypracovat, pokud provádějí systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování. Typickým příkladem je činnost bank, pojišťoven, leasingových či jiných finančních institucí. Algoritmickým posouzením informací o klientovi vyhodnocují jeho situaci za účelem nabídky služby.

Příklad: Pokud byste chtěli zpracovávat věrnostní program pro své zákazníky, na základě kterého by docházelo k profilování zákazníků podle počtu zakoupených druhů či typů zakoupených druhů produktů, měli by nejprve zpracovat posouzení vlivu na ochranu osobních údajů. Musíte zároveň přijmout taková opatření, aby dodržela zásadu minimalizace zpracování osobních údajů a transparentnosti.

JAKÉ MAJÍ POVINNOSTI 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 bankovníctví);
- 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 citlivým údajům);
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů (např. dočasné zablokování internetového připojení..)

POZOR!

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

JAKÉ MAJÍ POVINNOSTI FIRMY

POVINNOST VÉST ZÁZNAMY O ČINNO STECH ZPRACOVÁNÍ

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

Záznamy obsahují:

- název a kontaktní údaje správce/právnícké 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.

JAKÉ MAJÍ POVINNOSTI FIRMY

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

Výše uvedená výjimka se 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.

I přesto, že máte ne více než 10 zaměstnanců, musíte zpracovávat záznamy o činnostech, neboť zpracováváte citlivé osobní údaje, které zahrnují údaje o zdravotním stavu (viz odstavec výše).

JAKÉ MAJÍ POVINNOSTI FIRMY

POVINNOST JMENOVAT POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

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.

JAKÉ MAJÍ POVINNOSTI FIRMY

Příklady rozsáhlého zpracování

- 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.

JAKÉ MAJÍ POVINNOSTI FIRMY

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 nenesení osobní odpovědnost za nedodržování GDPR. Odpovědnost za dodržení povinností leží na firmě.

Příklad: Pokud jste pouze malou společností s vyhraněným sortimentem zboží a zpracováváte osobní údaje zákazníků (jméno, příjmení, adresa bydliště, e-mail) pouze za účelem prodeje zboží. Nemusíte mít pověřence pro ochranu osobních údajů.

JAKÉ HROZÍ FIRMÁM SANKCE PŘI PORUŠENÍ POVINNOSTI

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 obrátu 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 podnikajícím osobám (PO, OSVČ) 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.

CO MUSÍ FIRMA UDĚLAT, ABY BYLA PŘIPRAVENA 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.

CO MUSÍ FIRMA UDĚLAT, ABY BYLA PŘIPRAVENA NA GDPR

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.

CO MUSÍ FIRMA UDĚLAT, ABY BYLA PŘIPRAVENA NA GDPR

Na základě vypracované analýzy by měl návrh řešení obsahovat:

➤ úpravu vnitřních norem a procesů společnosti:

🕒 **úprava vnitřních dokumentů -smlouvy, souhlasy ;**

🕒 **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.

CO MUSÍ FIRMA UDĚLAT, ABY BYLA PŘIPRAVENA NA GDPR

- 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.

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 „zaškrťovacího políčka“.

POZOR! Jestliže zpracováváte osobní údaje dětí ze sociálních sítí pro marketingové účely, 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.

ZÁKLADNÍ DOPORUČENÍ

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.

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/>
 - 🕒 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

www.zkcoo.cz/gdpr

VZORY DOKUMENTŮ KE STAŽENÍ

- Záznamy správce o činnostech zpracování osobních údajů
 - Vnitřní směrnice o ochraně osobních údajů
 - Seznámení a poučení zaměstnance
 - Smlouva o zpracování os. Údajů
- Souhlas se zpracováním osobních údajů a poučení
 - Mlčenlivost zaměstnance

DĚKUJI ZA POZORNOST

danek@zkcoo.cz