NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016

GDPR

Martina Macek

GDPR – co nás čeká

- Nařízení vstoupí v platnost 25 května 2018.
- Za jeho nedodržení mohou být uvaleny astronomické pokuty a to až 20 milionů euro nebo až 4 % celosvětového ročního obratu.

GDPR – předmět a cíle nařízení

- Toto nařízení stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů.
- Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů.
- Volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán.

GDPR – věcná působnost nařízení

- Toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

GDPR – věcná působnost nařízení

- Toto nařízení se nevztahuje na zpracování osobních údajů prováděné: a) při výkonu činností, které nespadají do oblasti působnosti práva Unie; b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU; c) fyzickou osobou v průběhu výlučně osobních či domácích činností; d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

GDPR – Místní působnost nařízení

- Toto nařízení se vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni.
- Toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí: a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie.

GDPR – Místní působnost nařízení

- Toto nařízení se vztahuje na zpracování osobních údajů správcem, který není usazen v Unii, ale na místě, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného.

GDPR – základní definice nařízení

- **Osobní údaj** – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“); 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.

GDPR – základní definice

- **Zpracování** – jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

GDPR – základní definice

- **Správce** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;
- **Zpracovatel** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
- **Původce** – každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán;

GDPR – zákonnost zpracování

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;

GDPR – zákonnost zpracování

- 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.

GDPR – Práva občanů (subjektů údajů)

- Jedním z největších dopadů nařízení je výrazné posílení práv občanů neboli tzv. subjektů údajů. Těmito právy jsou zejména práva na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a v neposlední řadě právo vznést námitku.

GDPR – Práva občanů (subjektů údajů)

- Jako občané máme tato práva ke všem údajům, které má správce o nás k dispozici, tj. i k tzv. nestrukturovaným údajům, které mohou tvořit přílohy e-mailů nebo které jsou uloženy na různých interních a externích úložištích.
- Právo na přístup dává občanům zejména možnost ověřit si zákonnost zpracování jejich údajů. Je téměř absolutním právem subjektu údajů, s výjimkou případů stanovených článkem 23, který dává členským státům EU možnost omezit toto právo v zájmu národní a veřejné bezpečnosti, obrany a soudních řízení.

GDPR – Práva občanů (subjektů údajů)

- Příkladem práv na přístup je informace o zdravotním stavu subjektu, přístup k údajům ve své zdravotní dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích.
- Každý občan tedy bude mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, znát období, po které budou údaje uchovávány a znát příjemce jeho osobních údajů.

GDPR – Práva občanů (subjektů údajů)

- Novým právem podle GDPR je právo na to, aby správce bez zbytečného odkladu vymazal naše osobní údaje, pokud je dán jeden z těchto důvodů:
  - Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
  - Občan odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování.
  - Občan vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
  - Osobní údaje byly zpracovány protiprávně.
  - Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí.
  - Pokud není dána právní povinnost stanovená právem Unie nebo členským státem.

GDPR – povinnosti pro instituce a firmy

- Nařízení nově zavádí princip zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.
- Uplatnění principu zodpovědnosti bude představovat nemalé časové a finanční investice. Ty se budou týkat zejména oblastí:
  - Implementace záměrné a nezbytné ochrany dat.
  - Vypracování posouzení vlivu na ochranu osobních údajů, v angličtině DPIA neboli Data Protection Impact Assessment.
  - Jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer).

GDPR – povinnosti pro instituce a firmy

- Zavedení tzv. pseudonymizace osobních údajů.
- Vedení záznamů o činnostech zpracování.
- Konzultace s dozorovým orgánem před samotným zpracováním osobních údajů.

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

GDPR – povinnosti pro instituce a firmy

- Dalším principem spadajícím do oblasti zodpovědnosti je povinnost správců nebo zpracovatelů vést záznamy o činnostech zpracování, za které zodpovídají. Každý správce a zpracovatel bude povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány.

GDPR – povinnosti pro instituce a firmy

- Tyto záznamy o činnostech musí obsahovat následující informace:
  - Jméno a kontaktní údaje správce a zpracovatele včetně jména DPO,
  - účely zpracování,
  - popis kategorií subjektů údajů a kategorií osobních údajů,
  - kategorie příjemců, kterým byly nebo budou údaje zpřístupněny,
  - informace o mezinárodním předávání osobních údajů,
  - lhůty pro výmaz jednotlivých kategorií údajů,
  - popis technických a organizačních opatření.
- Výjimky z povinnosti vést záznamy o činnostech zpracování lze uplatnit pro organizaci s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje u nich riziko pro práva a svobody osob a tyto organizace nezpracovávají citlivé údaje.

DPO – Pověřenec pro ochranu osobních údajů

- Povinnost jmenovat pověřence nastává ve třech případech, pokud:
  - zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů),
  - hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů,
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

- Podle nařízení může být jediný pověřenec jmenován i pro několik státních orgánů, institucí či firem, které mají podobnou organizační strukturu.

DPO – Pověřenec pro ochranu osobních údajů

- Příklady rozsáhlého zpracování osobních údajů:
  - 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,
  - zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky,
  - zpracování obsahových, provozních či lokalizačních dat poskytovatelem telefonních a internetových služeb.

DPO – Pověřenec pro ochranu osobních údajů

- Příklady zpracování, která nejsou rozsáhlá:
  - Zpracování údajů o pacientech jednotlivým lékařem,
  - zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů jednotlivým právníkem.

- Pověřenci nenesou osobní odpovědnost za nedodržování GDPR. Nařízení jasně stanoví, že jsou to správci nebo zpracovatelé, kteří musí zajistit a být schopni doložit, že zpracování je prováděno v souladu s GDPR. Právní soulad v oblasti ochrany dat je odpovědností správce nebo zpracovatele.

DPO – Pověřenec pro ochranu osobních údajů

- Mezi profesní předpoklady zvažované při jmenování pověřence patří: vědomosti z oblasti národní a evropské legislativy a praxe v oboru ochrany osobních údajů a důkladná znalost GDPR. Užitečná je znalost chodu organizace, která je správcem. Pověřenec by také měl mít dostatečnou znalost prováděných operací zpracování, stejně jako informačních systémů a technického zabezpečení dat.

DPO – Pověřenec pro ochranu osobních údajů

- Mezi klíčové oblasti metodické a poradní působnosti pověřence patří aplikace zásad zpracování (kapitola II Obecného nařízení), implementace práv subjektů údajů (kapitola III), záměrná a standardní ochrana osobních údajů podle čl. 25, záznamy o činnostech zpracování podle článku 30, zabezpečení zpracování podle článku 32, oznamování porušení tohoto zabezpečení podle článků 33 a 34 nebo hodnocení dopadů podle článku 35. Zapojení pověřence od počátku plánování nového zpracování osobních údajů usnadní dodržení všech povinností správce.

GDPR – sankce

- GDPR zavádí několikanásobně vyšší pokuty, než jsme byli doposud zvyklí. Jejich maximální výše je 20.000.000 eur nebo 4 % z celkového ročního obratu společnosti (vyšší z obou možností) a bude záviset na řadě faktorů, jako je např. povaha, závažnost a délka porušování, počet poškozených občanů a míra škody, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, kategorie osobních údajů dotčené porušením a řada dalších.

GDPR – sankce

- Maximální výše pokuty může být udělena jak menší společnosti s několika zaměstnanci, tak velké nadnárodní korporaci, pokud neučiní kroky nezbytné k uvedení do souladu s principy a povinnostmi vyplývajícími z GDPR.

- Kromě udělení těchto správních pokut mohou být správci či zpracovatelé osobních údajů navíc vystaveni žalobám podaným fyzickými osobami s nárokem na náhradu škody v případě hmotné či nehmotné újmy. V neposlední řadě jsou společnosti vystaveny ztrátě důvěry a reputačním rizikům způsobeným nesprávným zacházením s osobními údaji.

GDPR a spisová služba

- Zpracovávání osobních údajů musí být zákonné a musí splňovat účel, který je podepřen právní úpravou, tedy že shromažďování osobních údajů odpovídá tomuto účelu, je vedeno v rozsahu, který mu odpovídá, a osobní údaje jsou zpracovávány korektně a zákonným a transparentním způsobem.

  - **Vhodné provedení auditu spisové služby, zda tomu tak opravdu je.**

GDPR a spisová služba

- Osobní údaje jsou uchovávány pouze po dobu nezbytnou, odpovídající účelu zpracování.
  - Doporučuje se, aby původce dokumentů provedl revizi spisových a skartačních plánů, zejména pak skartačních lhůt, zda odpovídají lhůtám uvedeným v právních předpisech, jsou-li pro konkrétní typy dokumentů lhůty stanoveny, ostatním typům dokumentů stanoví přiměřené skartační lhůty, které budou odpovídat požadavkům na délku uchovávání dokumentů po jejich vyřízení pro úřední potřebu a současně požadavkům veřejného zájmu.

GDPR a spisová služba

- Používaný eSSL je schopen splňovat kromě jiného všechny nároky na ochranu osobních údajů.
  - Původci musí zabezpečit dokumenty obsahující osobní údaje proti přístupu neoprávněných osob, a to včetně vlastních zaměstnanců. Musí proto využívat zejména nástroje pro omezení přístupu k dokumentům a jejich metadatům obsahujícím osobní údaje a přístup umožnit pouze oprávněným osobám, a to při všech operacích s takovými dokumenty a metadaty, a zaznamenávat historii nahlížení do dokumentů a metadat obsahujících osobní údaje.

GDPR a spisová služba

- Používaný eSSL musí umožnit naplnit povinnosti správce údajů vůči subjektu údajů dle čl. 13, 14,15,16, 18, 19, 20 a 21 GDPR ve lhůtách stanovených v čl. 12 GDPR.
  - Každá fyzická osoba je oprávněna požádat původce dokumentů podle čl.15 nařízení 2016/679 o informaci, jaké údaje o něm v dokumentech zpracovává, pro jaký účel a v jakém rozsahu, na základě jakého titulu (viz článek 6 nařízení) je zpracovává a po jakou dobu budou uloženy.
  - Původce také musí informovat subjekt údaj o případném úmyslu předat osobní údaje do třetí země (mimo prostor EHS a mimo státy se srovnatelnou zárukou ochrany osobních údajů) nebo mezinárodní organizaci (čl. 13 GDPR).

GDPR a spisová služba

- Nastavené procesy musí umožňovat zároveň povinnost uchovávat dokumenty a umožnit výběr archiválií podle zákona č. 499/2004 Sb. versus „právo na výmaz/právo být zapomenut“ podle čl. 17 GDPR.
  - Žádá-li fyzická osoba o provedení výmazu osobních údajů podle čl. 17, pak původce dokumentů musí rozlišit, jakým způsobem jsou dokumenty s osobními údaji zpracovávány. Jsou-li dokumenty zpracovávány v eSSL tázající fyzickou osobu upozorní, že výmaz ze systémů eSSL (či spisové služby vedené analogově) ve smyslu ustanovení článku 17 odst. 3 nařízení 2016/679 je možné provést teprve po uplynutí skartačních lhůt dokumentů a jejich zařazení do procesu výběru archiválií, a to pouze u těch dokumentů, které nebudou příslušným archivem vybrány jako archiválie. V případě výběru za archiválie původce dokumenty s osobními údaji a jejich metadata předá k uložení do příslušného archivu a v systému spisové služby po skončení skartačního řízení a uplynutí lhůt pro podání odvolání dokumenty a jejich metadata smaže. Další uchovávání osobních údajů je podle GDPR zákonné „pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, nebo pro určení, výkon nebo obhajobu právních nároků“ (srovnej odst. 65 preambule GDPR).

GDPR – závěrečné shrnutí nutných kroků

- Analýza činností původce souvisejících s informacemi (zejména pak s osobními údaji); zjištění agend a systémů, ve kterých se vyskytují osobní údaje (vedení seznamu o činnostech zpracování); možnost využít obdobnou analýzu provedenou v organizaci z důvodu zákona o kybernetické bezpečnosti.
- Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.).

GDPR – závěrečné shrnutí nutných kroků

- Stanovení postupů a politiky ochrany – analýza přístupových oprávnění, bezpečnosti uložení (dokumentů, spisů, systémů, informací).
- Proškolení zaměstnanců: správná správa hesel, řádné návyky zaměstnanců, nastavení odpovědnosti, procesy při ukončení pracovního / služebního poměru, pracovní náplně odpovídající práci s osobními údaji atp. (GDPR se netýká „jen personalistů“!).

GDPR – závěrečné shrnutí nutných kroků

- Revize pracovních smluv se zaměstnanci, doplnění doložky o ochraně osobních údajů.
- Revize spisového řádu (doplnit všechny evidence vedené u původce) a revize spisového a skartačního plánu (provést revizi skartačních lhůt z hlediska zákonného zmocnění a skutečné provozní potřebnosti).
- Revize výkonu spisové služby, ISSD a dalších evidencí s osobními údaji a přijetí opatření.

GDPR – závěrečné shrnutí nutných kroků

- Ověření správy dat a jejich záloh (v případě externího dodavatele prověření smluv a ošetření ochrany osobních údajů ve smlouvách).
- Příprava procesů včetně šablon odpovědí a nastavení lhůt vyřízení podání, která přijdou podle GDPR (čl. 12 až 22 a 34 GDPR).
- Stanovení postupů pro detekování bezpečnostních incidentů a řešení porušení zabezpečení (kdo odpovídá za nahlášení incidentu, kam oznamuji, komu atp.).

Institut pro správu dokumentů

„Jen profesionálové s odpovídající kvalifikací umožní důvěryhodnou a konkurence schopnou správu dokumentů.“

DĚKUJI ZA POZORNOST.