Příprava na GDPR krok za krokem

Mgr. Radomír Pivoda

Brno, 11. 4. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

GDPR

- Co je GDPR a jak se na něj připravit.
- Jaká data zpracováváme v rámci společnosti?
- Provádíme zpracování v souladu se zákonem?
- A bude současný stav vyhovovat GDPR?
- Jaká opatření přijmout?
- Co nám hrozí, když se nepřipravíme?

CO JE TO „GDPR“ - DŮVODY VZNIKU

- 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 pohybu těchto údajů
- Nařízení EU – přímo aplikovatelné
- Účinnost 25. 5. 2018
- Neobsahuje přechodná ustanovení

CO JE TO „GDPR“ - DŮVODY VZNIKU

- Data jako nezbytnost a riziko zároveň
- Preventivní a sjednocená úprava
- Zastaralá a nejednotná úprava napříč EU
- Nemožnost legislativně stíhat tempo technologického rozvoje (internet of things, cloudová řešení, big data, BYOD)

VZTAH GDPR A ZÁKONA č. 101/2000 Sb.

- Nařízení neruší zákon č. 101/2000 Sb.
- Návrh novely zákona č. 101/2000 Sb. publikován v srpnu 2017
- Nařízení v mnohém nahrazuje zákon
- Český zákon bude nadále upravovat:
  - některé aspekty týkající se Úřadu pro ochranu osobních údajů
  - dílčí záležitosti nutné k dotvoření rámce ochrany osobních údajů, které nejsou Obecným nařízením upraveny nebo které Obecné nařízení umožňuje upravit na vnitrostátní úrovni
  - aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby

ZÁKLADNÍ ZMĚNY SPOJENÉ S GDPR

- Rovnocenná vymahatelnost v celé EU
- Stejné sankce
- Spolupráce dozorových orgánů
- Rozšíření definice osobních údajů
- Nová práva subjektů údajů
- Oznamovací povinnost v případě narušení bezpečnosti údajů

SANKCE

- Až 20 milionů Euro nebo 4% z celosvětového obratu skupiny (vyšší z obou možností)
- Nebezpečí žalob ze strany fyzických osob (nárok na náhradu škody v případě hmotné či nehmotné újmy)
- Ztráta důvěry a reputační riziko

SANKCE A RIZIKA

- Výše sankce se stanovuje podle řady faktorů:
  - Povaha
  - Závažnost
  - Délka porušování
  - Počet poškozených subjektů a míra škody
  - Kroky podniknuté správcem či zpracovatelem ke zmírnění škod
  - Kategorie osobních údajů dotčené porušením

OSOBNÍ ÚDAJ

- Veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě
- Údaj, který umožňuje identifikovat konkrétní osobu, je osobním údajem
- To, co je u jedné fyzické osoby osobním údajem, protože ji to jasně identifikuje, nemusí být osobním údajem pro další fyzickou osobu
- Osobním údajem může být jeden údaj nebo i více údajů, které teprve dohromady umožňují konkrétní osobu určit

NEJČASTĚJŠÍ OBECNÉ OSOBNÍ ÚDAJE

- jméno
- adresa
- pohlaví
- věk
- datum narození
- místo narození
- rodné číslo
- osobní stav
- zdravotní znevýhodnění
- fotografický záznam
- video záznam
- audio záznam
- e-mailová adresa
- telefonní číslo
- IP adresa
- různé identifikační údaje vydané státem: číslo občanského průkazu, číslo řidičského průkazu, číslo cestovního pasu a další...
- vzdělání
- příjem ze zaměstnání (mzda, plat), příjem z důchodu

ZVLÁŠTNÍ OSOBNÍ ÚDAJE

Zpracování citlivých osobních údajů podléhá přísnějšímu režimu, než je tomu u obecných údajů.

- údaje o rasovém či etnickém původu (národnost), NE státní občanství
- politické názory, NE členství v politické straně nebo hnutí, NE členství v komunistické straně před rokem 1989 (dle ÚS)
- náboženské vyznání
- filozofické vyznání
- členství v odborech
- zdravotní stav - údaje o tělesném nebo dušením zdraví, o poskytnutí zdravotních služeb
- sexuální orientace
- trestní delikty
- pravomocná odsouzení

GENETICKÉ A BIOMETRICKÉ ÚDAJE

- Genetické údaje:
- DNA, RNA
- krevní skupina
- Rh faktor krve
- jiné

- Biometrické údaje:
- snímek obličeje,
- otisk prstu,
- snímek oční duhovky,
- snímek sítnice,
- podpis
- hlas (zabarvení)

ÚDAJE NEPOŽÍVAJÍCÍ OCHRANY

- Údaje o právnických osobách, orgánech veřejné moci a institucích
- Údaje zemřelých osob
- Údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter
- Anonymizované údaje - nelze ani nepřímo přidělením dalších identifikátorů určit subjekt údajů

OSOBNÍ ÚDAJE DĚTÍ

- Kategorie citlivých osobních údajů
- Hranice věku dítěte podle GDPR – 16 let
- Návrh novely zákona č. 101/2000 Sb. - **věk dítěte pro souhlas se zpracováním jeho osobních údajů je navržen na 13 let**
- Souhlas platný pouze tehdy, pokud je vyjádřen nebo schválen zákonným zástupcem

SPRÁVCE OSOBNÍCH ÚDAJŮ

- Každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování.
- Nutnost řádného právního důvodu zpracování
- Povinnosti:
  - dodržování zásad zpracování
  - dodržování povinností upravených nařízením
  - zabezpečení údajů

ZPRACOVATEL

- Fyzická nebo právnická osoba, která jménem správce zpracovává osobní údaje
- Může provádět jen takové operace, kterými jej správce pověřil
- Zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům, jejichž zpracováním jej správce pověřil – jinak je v pozici správce
- Vztah spolupracovníků a společnosti / činnost externích dodavatelů
- Činnost spolupracovníků - smlouva o obchodním zastoupení + Pravidla pro nakládání a ochranu osobních údajů

PRÁVNÍ TITUL ZPRACOVÁNÍ

- Plnění smlouvy, jejíž smluvní stranou je subjekt údajů
- Opatření před uzavřením smlouvy na žádost subjektu údajů
- Splnění právní povinnosti
- Ochrana životně důležitých zájmů
- Splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněný zájem příslušného správce (přednost základních práv a svobod)
- Souhlas

SOUHLAS

- **Svobodný, konkrétní, informovaný a jednoznačný** projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů
- Povinnost správce doložit, že subjekt údajů udělil souhlas se zpracováním svých údajů
- Aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen
- Souhlasem nesmí být podmíněno plnění smlouvy, včetně poskytnutí služby, kde zpracování OÚ není pro plnění smlouvy nutné
- Souhlas nemá být součástí obchodních podmínek / standardizovaných formulářů

ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- Zákonnost, korektnost a transparentnost
- Účelové omezení
- Minimalizace údajů
- Přesnost
- Omezení uložení
- Integrita a důvěrnost
- Odpovědnost

PRÁVA SUBJEKTU ÚDAJŮ

- právo na přístup
- právo na opravu
- právo na výmaz
- právo být zapomenut
- právo na omezení zpracování
- právo na přenositelnost údajů
- právo vznést námitku

PRÁVO NA PŘÍSTUP

- Možnost ověřit si zákonnost zpracování údajů (Ověření identity!)
- Právo vědět a být informován o:
  - účelech zpracování,
  - kategorii dotčených osobních údajů,
  - příjemcích nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
  - plánované době, po kterou budou osobní údaje uloženy,
  - existenci práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
  - právu podat stížnost u dozorového úřadu,
  - veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
  - skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

PRÁVO OPRAVU

- Subjekt údajů má právo na doplnění neúplných osobních údajů
- Možnost poskytnout dodatečné prohlášení
- Správce by měl zajistit podmínky pro to, aby žádosti na opravu mohly být podávány online, zejména v případě zpracování osobních údajů elektronickými prostředky (opět problém s ověřením identity)
- Nutnost přijetí mechanismu k ověření identity subjektu údajů
- Zajištění opravy osobních údajů uchovávaných v elektronické podobě jako „scan“

PRÁVO NA VÝMAZ

- Nové pravidlo podle GDPR
- Povinnost správce bez zbytečného odkladu vymazat osobní údaje, pokud je dán jeden z těchto důvodů:
  - Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány
  - Subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování
  - Osobní údaje byly zpracovány protiprávně
  - Právní povinnost stanovená právem Unie nebo členským státem

PRÁVO BÝT ZAPOMENUT

- Rozšíření práva na výmaz
- Provedení přiměřených kroků, včetně technických opatření, k vymazání veškerých odkazů na osobní údaje a jejich kopie
- Správce má povinnost zlikvidovat osobní údaje, pokud jsou splněny podmínky – viz právo na výmaz

PRÁVO NA OMEZENÍ ZPRACOVÁNÍ

- Nové pravidlo podle GDPR
- Dočasný přesun vybraných údajů do jiného systému zpracování
- Znepřístupnění vybraných osobních údajů nebo dočasné odstranění zveřejněných údajů z internetových stránek
- Skutečnost, že zpracování osobních údajů je omezeno, by měla být v systému jasně vyznačena.
- Blokace v jednotlivých IT systémech společnosti

PRÁVO NA PŘENOSITELNOST ÚDAJŮ

- Nové pravidlo podle GDPR
- Splnění dvou podmínek, které musí nastat současně:
  - 1. zpracování je založeno na souhlasu nebo na smlouvě
  - 2. je prováděno automatizovaně
- Povinnost správce předat subjektu údajů všechny o něm zpracovávané informace ve strukturovaném, běžně používaném, strojově čitelném formátu
- Zjednodušení předání osobních údajů jinému správci

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

- Záznamy, které budou správci podle GDPR povinni vést o zpracování a na žádost je zpřístupnit dozorovému orgánu
- Náhrada za oznamovací povinnost
- Písemně nebo v elektronické formě
- 250 zaměstnanců, nebo „nikoliv příležitostné zpracování zvláštních kategorií osobních údajů“

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

- Záznamy obsahují:
  - jméno a kontaktní údaje (společného) správce, zástupce správce a pověřence pro ochranu OÚ;
  - účely zpracování;
  - popis kategorií SÚ a kategorií OÚ;
  - kategorie příjemců, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
  - informace o případném předání OÚ do třetí země nebo mezinárodní organizaci;
  - plánované lhůty pro výmaz jednotlivých kategorií údajů;
  - obecný popis technických a organizačních bezpečnostních opatření

PSEUDONYMIZOVANÉ ÚDAJE

- U pseudonymizovaných údajů je možné určit, koho se údaje týkají, ale jen s použitím dodatečných informací.
- Příklad:
  - Jméno a příjmení nahrazeno číselným kódem, správce zvlášť uchovává soubor se jménem, příjmením a tímto číselným kódem. Kdo má přístup k oběma souborům zároveň, je schopen určit, ke komu se informace o věku a vzdělání vztahují.
- Existence dvou oddělených souborů

DOPADY DO IT

- Opatření proti neoprávněnému přístupu a zneužití dat
  - Zamezení možnosti datových extraktů zaměstnanci, kteří je nepotřebují k výkonu své práce.
  - Kontrola nad odesíláním OÚ e-mailem
- Správa šifrovacích klíčů – vnitřní předpis
- Shadow IT

DOPADY DO IT

- Vnitřní předpis vyžadující pravidelnou změnu přístupových hesel
- Základní pravidla pro heslo:
  - alespoň osm znaků (prolomení za 9 vteřin)
  - nesmí obsahovat smysluplné slovo
  - nesmí být spojeno s informacemi o uživateli (např. rodné či telefonní číslo)
  - obsahuje malá i velká písmena
  - obsahuje číslice a speciální znaky (např. !, ?, _, # apod.)
  - heslo obsahující 10 znaků, malá a velká písmena, číslice a speciální znaky – prolomení za více než 3 týdny

PŘÍPRAVA NA NAŘÍZENÍ

- Diagnostika organizace (vstupní analýza)
  - Časový harmonogram
  - Identifikace procesů a systémů
  - Identifikace rozsahu zpracování osobních údajů
- Analýza stávajícího stavu zpracování osobních údajů
  - Právní audit
  - Datový a bezpečnostní audit
  - Procesní audit
  - Analýza rizik
- Ustanovení pověřence (DPO)
  - Lze i jeden pověřenec pro více organizací (viz dále)

POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

- „Data Protection Impact Assessment“
- Pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob
- Povinnost provést před zahájením zpracování
- Správce si vyžádá posudek pověřence pro ochranu osobních údajů
- Možnost „předchozí konzultace“ s ÚOOÚ

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- Nová pracovní pozice podle nařízení
- Vhodné využít již při implementaci
- Musí být jmenován na základě profesních kvalit, odborných znalostí práva a praxe v oblasti ochrany údajů
- S přihlédnutím k organizační struktuře a velikosti správce může být jmenován jediný pověřenec pro několik orgánů nebo subjektů

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- Nová pracovní pozice podle nařízení
- Vhodné využít již při implementaci
- Musí být jmenován na základě profesních kvalit, odborných znalostí práva a praxe v oblasti ochrany údajů
- S přihlédnutím k organizační struktuře a velikosti správce může být jmenován jediný pověřenec pro několik orgánů nebo subjektů

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- Může být zaměstnancem správce či zpracovatele, nebo na základě smlouvy o poskytování služeb
- V souvislosti s plněním svých úkolů není správcem propuštěn ani sankcionován
- Může plnit i jiné úkoly a povinnosti, pokud nedojde ke střetu zájmů
- Kontaktní osoba pro styk s ÚOOÚ
- Nemůže zastávat pracovní místo, na kterém by stanovoval účely a prostředky zpracování osobních údajů
- Pověřenci nenesou osobní odpovědnost za nedodržování GDPR

OSVĚDČENÍ

- Předpokládá se zavedení mechanismů pro vydávání:
  - Osvědčení o ochraně osobních údajů
  - Pečetí a známek dokládajících ochranu osobních údajů
- pro účely prokázání souladu s nařízením
- Získáním osvědčení se nesnižuje odpovědnost správce
- Platné na dobu nejvýše 3 let
- Obdoba certifikací ISO
- Nařízení ani zákon zatím blíže neupravuje

PRÁVO SUBJEKTU ÚDAJŮ NA SOUDNÍ OCHRANU

- Žalovaným vždy konkrétní správce nebo zpracovatel
- Právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy
- Organizace (resp. i statutární zástupce) je odpovědná i za porušení, které nezavinila - objektivní odpovědnost
- Zpracovatel odpovědný, když:
  - poruší povinnost přímo uloženou nařízením
  - jedná nad rámec zákonných pokynů správce či v rozporu s nimi

NARUŠENÍ BEZPEČNOSTI ÚDAJŮ

- Oznamovací povinnost
- Nově musí správce ohlásit únik či ohrožení zabezpečení osobních dat ÚOOÚ nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl
- Hlášení incidentu:
  - popis opatření, která správce přijal nebo navrhl
  - popis povahy daného případu
  - popis pravděpodobných důsledků porušení zabezpečení osobních údajů
  - jméno a kontaktní údaje jo a kontaktní údaje DPO
- Povinnost informovat osoby a subjekty, kterých se únik týká
  - Pokud je pravděpodobné, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob

VNITŘNÍ PŘEDPISY

- Vyřizování stížností
- Ochrana osobních údajů
- Ochrana dat
- Systém řízení rizik
- Směrnice o IT bezpečnosti
- Vnitřní předpis o uchovávání osobních údajů potenciálních a stávajících klientů, které provádí spolupracovníci mimo kontrolu společnosti.

KAMEROVÝ SYSTÉM

- Důvody pro instalaci – účel zpracování
  - Bezpečnost
  - Ochrana majetku
  - Prevence vandalismu
  - Zamezení přístupu cizích osob
- Zakázaný účel – sledování zaměstnanců a dalších fyzických osob
- Monitorované prostory – právo na soukromí
- Kamera se záznamem
  - Uchovávání záznamu
  - Zabezpečení záznamu / pravidla pro přístupu k záznamu

KAMEROVÝ SYSTÉM

- Zpracování může probíhat bez souhlasu, pokud je to nezbytné pro účely oprávněných zájmů správce či třetí strany
- Srozumitelné informování subjektů o zpracování údajů
- Informace o monitorování objektu musejí být uvedeny na přehledných místech
- Povinnost uvádět/evidovat:
  - kontakt na provozovatele systému
  - účel zpracování
  - kategorie dotčených osobních údajů a jejich příjemce
- Pouze data nezbytná pro daný účel (zásada minimalizace dat)
- Vhodná technická a organizační opatření
  - proces pravidelného testování, posuzování a hodnocení účinnosti

DODAVATELÉ

- Písemná forma smluv
- Revize stávajících smluv – doplnění odpovědnosti za svěřené osobní údaje
- Přístup dodavatelů = třetích osob k osobním údajům
- Závazek mlčenlivosti
- Pozor na zpracování DIČ u dodavatelů – fyzických osob

OSOBNÍ ÚDAJE ZAMĚSTNANCE

- Titulem pro zpracování osobních údajů zaměstnanců je plnění pracovní smlouvy a plnění právních povinností
- Před uzavřením pracovního poměru
  - Životopis od uchazeče o zaměstnání – nezbytnost pro uzavření smlouvy
  - Nutnost souhlasu pro zařazení do databáze
  - Souhlas v případě, že životopis poskytla 3. strana (agentury)
  - Screening sociálních sítí
  - Black list
- Souhlas pro Marketingové účely

OSOBNÍ ÚDAJE ZAMĚSTNANCE

- Během trvání pracovního poměru
  - Intranet, vstupové karty, webové stránky – oprávněný zájem
  - PR materiály – nutnost souhlasu
- Monitoring zaměstnanců
  - Proporcionalita / oprávněný zájem
  - Povinnost informovat subjekt údajů
  - Aktualizace vnitřních předpisů

OSOBNÍ SPIS ZAMĚSTNANCE

- Obsah určuje zaměstnavatel
- Pouze písemnosti nezbytné pro výkon práce v pracovněprávním vztahu
- Nelze pořizovat kopie libovolných dokladů, ani se souhlasem nebo je nutné zamezit zpracování údajů o třetích osobách (např. rodný list)

OSOBNÍ ÚDAJE ZAMĚSTNANCE PO SKONČENÍ PRACOVNÍHO POMĚRU

- Archivace dle zákona
- Uschování odůvodněno předpokladem vzájemného uplatňování nároků z pracovněprávního vztahu
- Postupná likvidace složky po uplynutí lhůt pro archivaci:
  - Životopis – ztrácí relevanci ukončením pracovního poměru
  - Stejnopisy evidenčních listů (3 roky)
  - Účetní podklady (5 let)
  - Záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti (6 let)
  - Mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění (30 let)

MARKETING

- Dříve získané souhlasy nevyhovující standardům GDPR je nutné získat znovu
- Všechny registrované adresy je nově nutné verifikovat tzv. double opt-inem pro ověření správné identity příjemce
  - potvrzení zadané e-mailové adresy zasláním e-mailu s potvrzovacím odkazem
- Zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu
  - Marketing vlastních produktů a služeb stávajícím zákazníkům
  - Cílená reklama v klientské zóně na webových stránkách, klasický dopis
  - Souhlasem podmíněny pokročilé marketingové aktivity - sledování a vyhodnocování aktivity na webových stránkách a obohacování údajů o zákaznících z dalších zdrojů (např. ze sociálních sítí) za účelem lepšího cílení reklamy

MARKETING

- Při každém dalším obchodním sdělení možnost jednoduchým způsobem zdarma zasílání nabídek odmítnout
- Telefonní marketing podléhá souhlasu vždy
- Povinnost ukončit a v budoucnu neprovádět zpracování, které je souhlasem podmíněno, včetně likvidace údajů, pro jejichž zpracování nemá správce jiný právní základ
- Povinnost ukončit zasílání obchodních sdělení elektronickou poštou osobám, jejichž kontakt správce získal při prodeji zboží či služby, ale nemá jejich souhlas, ani jim neumožnil zasílání obchodních sdělení snadno odmítnout.
- Neplatnost souhlasů z nakoupených databází
- Cookies

ŽIVOTNÍ CYKLUS DOKUMENTU

- Příjem + třídění – zapisování + označování – oběh a vyřizování – odesílání – ukládání - archivace – vyřazování
- Archivace – vlastní archiv / spisová služba
- Skartace – přímo v rámci společnosti / externí dodavatel
- Nikdy likvidace dokumentů vyhozením do tříděného odpadu

ZÁVĚREČNÉ SHRNUTÍ

- Proveďte důkladnou inventuru
- Posuďte, kdo má k datům přístup
- Ověřte si bezpečnost dat
- Zvažte výběr vhodného pověřence
- Aktualizujte vnitřní předpisy a procesy
- Vzdělávejte personál

Děkuji za pozornost!

Tento seminář pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz