Jak chránit osobní data v elektronickém a digitalizovaném účetnictví?

Stanislav Klika

PŘEDSTAVENÍ PREZENTUJÍCÍHO

STANISLAV KLIKA

Senior manažer
Česká republika

M: +420 604 226 734

E-mail: stanislav.klika@bdo.cz

- Vnitřní kontrola a řízení rizik
- Interní audit a profesní rozvoj interních auditorů
- Kybernetická bezpečnost a GDPR

CO JSOU OSOBNÍ ÚDAJE?

Osobní údaje

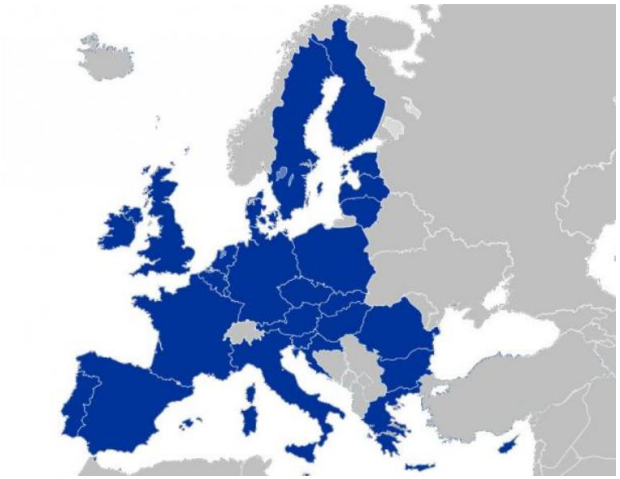
- Osobním údajem je jakákoliv (každá) informace (bez ohledu např. na kvalitu nebo pravdivost této informace).
- Tato informace se musí vztahovat k fyzické osobě.
- Fyzická osoba musí být těmito údaji či na jejich základě identifikovatelná a odlišitelná od jiných fyzických osob. Mohou tedy nastat dvě situace:
  - Lze utvořit přímý vztah mezi údajem a fyzickou osobou – jde o přímou identifikaci (určenost)
  - Správce nebo zpracovatel disponuje údajem, který však nepostačuje k tomu, aby mohl na základě tohoto údaje provést přímou identifikaci fyzické osoby. Má však možnost si opatřit další údaj a spojit jej s původním údajem a fyzickou osobu tak identifikovat – jde o nepřímou identifikaci (určitelnost).

SOUČASNÝ STAV V ČLENSKÝCH STÁTECH EU

Směrnice 95/46/ES

- Nakládání s osobními údaji je v současnosti v Evropské unii upraveno směrnicí 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců a v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

- Každý členský stát EU má svoji národní právní úpravu, která směrnici implementuje



NOVÁ PRÁVNÍ ÚPRAVA

Obecné nařízení o ochraně osobních údajů (GDPR)

- 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – „GDPR“)

- Posílit právo fyzických osob na ochranu údajů a zároveň usnadnit volný pohyb osobních údajů v rámci jednotného digitálního trhu EU

NOVÉ POVINNOSTI

GDPR stanoví nové povinnosti a zpřísňuje stávající

- Větší důraz na odpovědnost správce
- Detailnější požadavky na úpravu vztahu správce a zpracovatele
- Rozšíření práva na přístup k osobním údajům a práva být zapomenut
- Nové právo na přenositelnost osobních údajů
- Povinnost vést záznamy o zpracování - konec oznamovací povinnosti
- Povinnost vypracovat posouzení vlivu na ochranu osobních údajů
- Pověřenec pro ochranu osobních údajů
- Přísnější požadavky na udělování souhlasu se zpracováním a výslovné právo odvolat souhlas
- Vyšší nároky na bezpečnostní opatření a kontrolní mechanismy

HROZBA VYSOKÝCH SANKCÍ

GDPR stanoví vyšší sankce než stávající právní úprava

- Dosavadní právní úprava: § 44 – 46 ZOOÚ
  - Nejvyšší pokuta za spáchání správního deliktu právnickou osobou jako správcem nebo zpracovatelem, pokud tím ohrozí větší počet osob nebo poruší povinnosti při zpracování citlivých údajů činí 10 000 000 Kč (kvalifikované skutkové podstaty v § 45 odst. 2 ZOOÚ)
- V případě méně závažného porušení pokuta až do výše 10 mil. EUR nebo u podniku až 2 % celkového ročního světového obratu
- V případě závažnějšího porušení pokuta až do 20 mil. EUR nebo u podniku až 4 % celkového ročního světového obratu
- Udělením pokuty není dotčeno právo subjektů údajů na náhradu škody

PŘÍPRAVA NA GDRP V ČR

Návrh zákona o zpracování osobních údajů

- Adaptační zákon pro GDPR
- Implementace směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů
- Vnější připomínkové řízení ukončeno
- Důležitá pravidla
  - Věk dítěte pro souhlas se zpracováním os. údajů v souvislosti s nabídkou služeb informační společnosti: od 13 let
  - Veřejný subjekt: ministerstva a další ústřední orgány státní správy a jim podřízené úřady, veřejné sbory, ozbrojené sbory, veřejné školy, kraje, obce, komory, soudy (kromě soudního rozhodování), ČNB, NKÚ, Veřejný ochránce práv atd.

JAK ZAJISTIT SPLNĚNÍ POVINNOSTÍ PODLE GDPR A VYHNOUT SE SANKCÍM?

Kde začít?

- Termín pro splnění povinností se blíží mílovými kroky (25. května 2018)
- Organizace by měly učinit vše podstatné k zajištění přípravy na GDPR co nejdříve, a to i s ohledem na plánování zdrojů k pokrytí výdajů na zajištění souladu
- Změny prováděné na poslední chvíli mohou znamenat dodatečné náklady

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

1) Úprava odpovědnosti v organizaci

Je úprava odpovědnosti v souvislosti se zpracováním osobních údajů dostatečná?

- Riziko
  - Rizika související s ochranou osobních údajů nebudou řízena a cílů v oblasti ochrany osobních údajů nebude dosaženo
- Řešení
  - Vnitřní dokumentace (vnitřní předpisy) obsahuje jednoznačné a adresné povinnosti a odpovědnost v souvislosti s ochranou osobních údajů

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

2) Pravidla v oblasti IT

Je úprava pravidel v oblasti IT (např. politiky přístupů nebo správy hesel, včetně zavedení technických opatření vynucujících uplatnění těchto pravidel) dostatečná ?

- Riziko
  - Dojde k narušení osobních údajů
- Řešení
  - Vnitřní dokumentace, organizační a technická opatření

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

3) Plnění informační povinnosti

Je informační povinnost vůči subjektům údajů plněna (povinnost poskytovat informace o kategoriích zpracovávaných osobních údajů, účelech zpracování, příjemcích údajů a o právech subjektů údajů)?

- Riziko
  - Např. neplatnost souhlasu se zpracováním osobních údajů, pokuta za přestupek, poškození reputace
- Řešení
  - Rozsah poskytovaných informací odpovídá stanovenému rozsahu informační povinnosti, úprava informačních klauzulí u souhlasů, smluv a na webu

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

4) Registr zpracovávaných osobních údajů

Existuje registr zpracovávaných osobních údajů, který obsahuje alespoň kategorie zpracovávaných osobních údajů, kategorie subjektů údajů, povahu a účely zpracování, místo, kde jsou osobní údaje shromažďovány, odpovědnost za jednotlivé fáze zpracování osobních údajů, lhůty, po které mají být osobní údaje zpracovávány a právní tituly opravňující správce k jejich zpracování?

- Riziko
  - Zaměstnanci nebudou mít dostatečné informace pro řízení rizik souvisejících s ochranou osobních údajů, cílů v oblasti ochrany osobních údajů nebude dosaženo
- Řešení
  - Vytvoření registru osobních údajů

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

5) Práce se souhlasy

Je práce se souhlasy se zpracováním osobních údajů prováděna správně (správné vymezení, kde je souhlas nezbytný ke zpracování osobních údajů a kde je zpracování osobních údajů odůvodněno jiným právním titulem, např. smlouvou, oprávněnými zájmy atd., jasné odlišení textu souhlasu od smluvních ujednání, plnění informační povinnosti zejm. konkrétní vymezení účelu, pro který budou osobní údaje zpracovávány)?

- Riziko
  - Neplatnost souhlasu, pokuta za přestupek
- Řešení
  - Souhlas se používá, pokud neexistuje jiný právní titul, souhlas je odlišen od smluvních ujednání

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

6) Úprava smluv mezi správce a zpracovateli

Je úprava smluv mezi správcem a zpracovateli osobních údajů dostatečná (např. existuje ujednání o zárukách součinnosti zpracovatele v souvislosti s vyřízením požadavků subjektů údajů uplatněných u správce těchto údajů)?

- Riziko
  - Narušení osobních údajů, neschopnost reagovat na oprávněné požadavky subjektů údajů, pokuta za přestupek, poškození reputace
- Řešení
  - Písemné ujednání mezi správcem a zpracovatelem obsahuje náležitosti stanovené GDPR

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

7) Postupy pro uchování a likvidaci osobních údajů

Je nastavení postupů pro uchování a likvidaci osobních údajů dostatečné, zejm. s ohledem na zásadu minimalizace osobních údajů a omezení uložení osobních údajů?

- Riziko
  - Uchování osobních údajů, které nejsou nezbytné pro účely zpracování, pokuta za přestupek
- Řešení
  - Skartační lhůty a skartační příznaky jsou přiřazovány s ohledem na účely zpracování osobních údajů

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

8) Zvyšování povědomí zaměstnanců

Je zajištěno zvyšování povědomí zaměstnanců v oblasti ochrany osobních údajů a jejich zabezpečení (např. zajištění školení)?

- Riziko
  - Zaměstnanci nebudou mít dostatečné informace týkající se povinností v oblasti ochrany osobních údajů a tyto povinnosti nebudou dodržovány, cílů v oblasti ochrany osobních údajů nebude dosaženo
- Řešení
  - Vstupní a periodické školení zaměstnanců

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

9) Postupy pro případ narušení ochrany osobních údajů

Existují postupy pro případ narušení ochrany osobních údajů?

- Riziko
  - Následky narušení osobních údajů nebudou zmírněny, vyšší pokuta, reputační riziko
- Řešení
  - Tvorba psaných postupů, seznámení zaměstnanců s vnitřními postupy

DESATERO ÚSPĚŠNÉ PŘÍPRAVY NA GDPR

10) Postupy pro komunikaci s ÚOOÚ

Existují postupy pro komunikaci s Úřadem pro ochranu osobních údajů?

- Riziko
  - Riziko vyšších sankcí
- Řešení
  - Tvorba psaných postupů, seznámení zaměstnanců s vnitřními postupy

Děkuji za pozornost.

Společnosti skupiny BDO působící v České republice jsou zřízeny v souladu s českými právními předpisy, jsou členem BDO International Limited (společnosti s ručením omezeným registrované ve Velké Britanii) a jsou součástí mezinárodní sítě nezávislých členských firem BDO.

www.bdo.cz