GDPR v kostce
12 kroků k implementaci
pro oblast cestovního ruchu

Holubová advokáti s.r.o.
Za Poříčskou bránou 21
18600 Praha 8

+420 224914050
info@holubova.cz

Co je to GDPR?

GDPR (General Data Protection Regulation) je nové Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů).

- GDPR bude účinné od 25. 5. 2018 a nahrazuje stávající Směrnici Evropského parlamentu a Rady 95/46/ES, která byla transponována do zákona č. 101/2000 Sb., o ochraně osobních údajů. Tento zákon bude taktéž zrušen a nahrazen novým.

- GDPR je oproti směrnici účinné přímo, není třeba jej implementovat, je postaveno na stejných principech jako směrnice, ale jde více do hloubky, má širší teritoriální působnost a stanoví mnohem vyšší sankce za jeho nedodržování.

- GDPR upravuje ochranu osobních údajů fyzických osob jakožto subjektů údajů, přiznává jim četná práva a naopak zpracovatelům osobních údajů ukládá tomu odpovídající povinnosti.

- GDPR má širší dosah, vztahuje se na správce či zpracovatele osobních údajů se sídlem v Evropské Unii, ale také se sídlem mimo EU, pokud působí na trhu EU, resp. zpracovávají osobní údaje občanů států EU.

- GDPR rozšiřuje a zpřesňuje definici osobních údajů, mezi které spadá i IP adresa, email nebo soubor cookies.

- GDPR klade více požadavků na udělení souhlasu se zpracováním osobních údajů, souhlas musí být dán v jasné, srozumitelné a aktivní formě.

- GDPR dává fyzickým osob mnoho práv. Mají např. právo na přístup ke svým osobním údajům, právo na přenositelnost údajů mezi správci, právo na opravu, právo vznést námitku proti zpracování nebo právo být zapomenut.

- GDPR úkoluje správce, aby zavedli vhodná technická a organizační opatření a postupy, aby každé zpracování osobních údajů splňovalo požadavky GDPR a zaručovalo ochranu práv subjektů.

- GDPR stanoví i jiné povinnosti pro správce osobních údajů. Ti jsou v některých případech povinni provádět posouzení dopadu na ochranu osobních údajů nebo jmenovat pověřence pro ochranu osobních údajů.

- GDPR stanovuje vysoké sankce. Za jeho porušení může být uložena pokuta až 20 mil. EUR nebo pokuta ve výši 4 % celkového ročního obratu společnosti, podle toho, co je vyšší.

Jak se připravit na GDPR ve 12 krocích?

1) Zvyšte povědomí o GDPR mezi klíčovými osobami

- zvyšte povědomí o GDPR mezi klíčovými osobami, zejména mezi obchodním vedením společnosti a IT oddělením
- určete, kdo bude za implementaci GDPR ve Vaší společnosti odpovědný, příp. stanovte tým
- zahrňte GDPR do rozpočtu pro rok 2018

2) Zjistěte, jaké osobní údaje zpracováváte

- zdokumentujte procesy, ve kterých získáváte osobní údaje
- zjistěte, jak tyto údaje dále zpracováváte

3) Zhodnoťte, zda tyto všechny údaje potřebujete a zda je smíte zpracovávat

- u každého osobního údaje, který sbíráte, zhodnoťte, zda jej opravdu potřebujete
- u každého osobního údaje určete právní důvod zpracování podle GDPR

4) Upravte texty a proces získávání souhlasu se zpracováním

- pokud nenaleznete jiný právní důvod zpracování osobních údajů, zajistěte souhlas subjektu údajů se zpracováním
- souhlas musí být u každého osobního údaje svobodný, aktivní, srozumitelný
- odvolat souhlas musí být tak jednoduché jako ho poskytnout
- typickým příkladem pro oblast cestovního ruchu bude souhlas se zasíláním obchodních sdělení

5) Při získávání souhlasu se zpracováním se zaměřte na děti

- pokud Vaše služby cílí na děti, a to online, zaveďte verifikaci věku dětí
- zjistěte, zda nepotřebujete souhlas zákonného zástupce

6) Zajistěte všechna práva subjektů údajů

- zjistěte, zda jste schopni zajistit, a to zejména po technické stránce, všechna práva, která subjekt údajů, zejm. zákazník má
- pokud ne, zaveďte takové procesy, s jejichž pomocí budete schopni své povinnosti splnit

7) Zajistěte, aby subjekt údajů o svých právech věděl

- poučte své zákazníky a zaměstnance o jejich právech na ochranu osobních údajů, jde např. o
  - právo na přístup, opravu a výmaz
  - právo zabránit přímému marketingu
  - právo zabránit automatizovanému rozhodování a profilování
  - právo na přenositelnost osobních údajů
- cestovní kanceláře mohou toto poučení o právech zařadit do všeobecných obchodních podmínek

8) Ukládejte bezpečně a stanovte, co budete dělat v případě narušení bezpečnosti zpracování

- zjistěte, kam v současnosti ukládáte osobní údaje či dokumenty, které je obsahují
- zhodnoťte, jaké je nebezpečí úniku dat, příp. zlepšete zabezpečení

9) Ujasněte si, komu předáváte osobní údaje

- hotely, delegáti, přepravní společnosti, účetní, daňoví poradci, IT společnosti, těm všem cestovní kanceláře zpravidla předávají osobní údaje
- zhodnoťte, zda k tomu máte právní důvod, příp. souhlas
- zjistěte, zda subjekt údajů o předání ví

10) Pokud poskytujete osobní údaje mimo země EU, zjistěte, zda tyto země zajišťují odpovídající ochranu

- Pokud poskytujete osobní údaje do třetích zemí, jste povinni zajistit, aby ochrana osobních údajů byla srovnatelná s ochranou v EU
- Např. pokud ubytováváte zákazníky v hotelech v Thajsku, musíte prověřit, jaká je tamní ochrana osobních údajů, příp. zajistit ochranu jinak

11) Určete, zda spadáte do kategorie správců, kteří mají další povinnosti

- někteří správci musí vést záznamy o zpracování osobních údajů
- někteří správci musí pro aktuální a nově zaváděné procesy vypracovat tzv. dopadovou analýzu (DPIA)
- někteří správci musí jmenovat tzv. pověřence pro ochranu osobních údajů (DPO)

12) Pokud působíte mezinárodně, určete příslušný úřad

- pokud máte pobočky v jiných zemích, určete příp. zvolte příslušný dozorový úřad, pod který budete spadat
- Vemte v potaz, že každý dozorový úřad může mít trochu jiný přístup k GDPR

Jak Vám můžeme pomoci?

První fáze – před účinností GDPR

1. Školení pro klíčové osoby a zaměstnance

Rozsah školení (lze přizpůsobit na míru)

- základní definice, pojmy a principy GDPR
- práva a povinnosti vyplývající z GDPR
- návod, jak splnit požadavky GDPR a vyhnout se tak sankcím
- diskuze a odpovídání na dotazy

2. Analýza stávajícího stavu

- posouzení zpracovávání osobních údajů, zejména s ohledem na formu získání souhlasu ke zpracování a zajištění informační povinnosti ve vztahu k subjektům údajů
- identifikace zjištěných nedostatků ve zpracovávání
- návrh řešení a změn pro zajištění souladu s GDPR

3. Úprava textů souhlasů, podmínek a další dokumentace

Dle potřeby

- úprava smluvní a další dokumentace dle požadavků GDPR
- spolupráce na přípravě změn vnitřních procesů a technických řešení ve spolupráci s interními či externími IT techniky
- právní konzultace s osobami odpovědnými za implementaci GDPR v podniku
- komunikace s Úřadem pro ochranu osobních údajů
- sledování a zapracování výkladových stanovisek

Druhá fáze – po 25. 5. 2018

4. DPIA, DPO a soulad s GDPR

- průběžná aktualizace a hodnocení souladu s GDPR

Dle potřeby

- zpracovávání „Posouzení dopadu na ochranu osobních údajů“ (DPIA), který by měl obsahovat systematický popis zamýšleného zpracování, posouzení rizik z hlediska práv a svobod subjektů údajů, provedení testu proporcionality vč. posouzení, zda je zpracování ve vztahu k účelům zpracování nezbytné

- konkrétní podoba zajištění souladu s GDPR v návaznosti na závěry analýzy, nezbytné úpravy právní dokumentace, vnitřních procesů a technických řešení

- výkon funkce pověřence pro ochranu osobních údajů (DPO)