JSEM ODPOVĚDNÝ ZA **IMPLEMENTACI GDPR** V MÉ ORGANIZACI – Jak mám postupovat?

Obecné nařízení o ochraně osobních údajů

GDPR. CO TO JE?

GDPR neboli Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů je přelomová nová legislativa, přinášející zásadní posílení ochrany osobních údajů a řadu nových povinností nebo změny stávajících povinností pro všechny správce a zpracovatele.

GDPR bylo přijato 27. 4. 2016 a začne platit od 25. 5. 2018.

V souvislosti s postupující výstavbou sítí nové generace dochází i k radikálnímu zvyšování objemu dat přenesených novými sítěmi. S pohybem a zpracováním údajů, zejména osobních, souvisí i vysoce aktuální problematika ochrany těchto údajů.

Nepodceňujte zapojení kolegů z různých oddělení do zpracování dotazníku, budete překvapeni, kolik nových informací se dovíte při osobním rozhovoru, a které nejsou v dotazníku uvedeny.

Zpracováváte osobní data podle zákona č. 101/2000 Sb.?

NE — **ANO**

Pamatujte, že neznalost zákona neomlouvá, poučte se.

NĚKTERÉ Z NEJDŮLEŽITĚJŠÍCH DOPADŮ GDPR

1. Bude zapotřebí realizovat nákladné a náročné změny ve vašich informačních systémech a interních procesech z následujících důvodů:
   - GDPR rozšiřuje nutnost aktivního souhlasu subjektů údajů i na oblasti, kde to nyní není zapotřebí
   - klade důraz na zvýšení zabezpečení dat, zejména prostřednictvím šifrování či pseudonymizace
   - zpřísňuje stávající a zavádí nová práva subjektů údajů (např. právo na přístup, právo na výmaz, přenositelnost osobních údajů aj.), jejichž realizace je technicky náročná
   - musíte provést změny ve vaší interní organizační struktuře, např. zavést tzv. pověřence pro ochranu osobních údajů neboli data protection officer(a), DPO, zavést principy tzv. „privacy by design“, např. nezbytné posuzování vlivu jakýchkoliv významnějších opatření nebo projektů na ochranu osobních údajů.
2. Musíte změnit smlouvy s vašimi dodavateli – zpracovateli osobních údajů, protože GDPR významně mění postavení zpracovatelů osobních údajů a zvyšuje rozsah jejich povinností a odpovědnosti.
3. Musíte proškolit zaměstnance o nových povinnostech a pravidlech.
4. GDPR je doprovázeno dalšími regulačními opatřeními EU, zejména v oblasti platebních služeb tzv. PSD2 nebo nyní finalizovaným nařízením o e-privacy. Z této další legislativy EU vyplývají další konkrétní úkoly pro dotčené organizace, neboť tato regulační opatření doplňují GDPR, nepřekrývají se s ním.
5. GDPR zavádí mnohonásobné zpřísnění sankcí – pokuty v milionech EUR namísto milionů Kč – s tím, že s ohledem na tlak na jednotný výklad GDPR v rámci EU nelze vyloučit výrazný nárůst udělovaných pokut.
6. Ještě větší rizika než sankce představuje v případě nesouladu činnosti organizace s GDPR poškození dobrého jména organizace v celoevropském měřítku. Pořádek v oblasti ochrany osobních údajů je v kybernetickém světě samozřejmým požadavkem. Část soukromé i veřejné sféry využije implementaci GDPR k tomu, aby se prezentovala svým zákazníkům jako „bezpečný digitální partner“.

*V rámci reportingu zkuste **využít v maximální míře moderní technologii**, která vám umožní:*
- *definovat role, skupiny, organizační strukturu;*
- *v rámci číselníků sledovat jednotlivé agendy i typy zpracování;*
- *načítat data z aplikací a ty dále dle nastavených procesů zpracovat;*
- *definovat reporty a procesy na základě rolí, skupin a organizační struktury;*
- *veškeré dokumenty archivovat a opatřovat elektronickým podpisem;*
- *k dokumentům na konci procesu vytvářet souhrnnou zprávu;*
- *případně data pro regulátory odesílat přímo datovou schránkou.*

UDĚLEJTE INTERNÍ AUDIT

Implementaci GDPR nejlépe začnete, když si uděláte pořádek v osobních údajích, které zpracováváte, podle stávajícího zákona č. 101/2000 Sb. v platném znění.

Proveďte interní audit buď vlastními silami nebo externími poradci. Interní audity dnes nabízí řada advokátních kanceláří i konzultačních firem.

Inspirujte se jednoduchým dotazníkem[1)]

1. **Jaká zpracování provádíte, zejména v personální a klientské agendě?**
   - Osobní údaje jsou zpracovávány manuálně anebo automatizovaně?
2. **Proč a na základě jakého právního titulu osobní údaje zpracováváte?**
   - k plnění úkolů uložených zákonem – např. vedení agendy sociálního zabezpečení
   - k jiným účelům, zejména plnění smlouvy, plnění podnikatelského záměru na základě souhlasu subjektu údajů, s využitím veřejných zdrojů, pro ochranu práv správce apod.
   - Splňuji požadavky pro zákonné zpracování?
   - Udal jsem dostatečný důvod pro shromáždění osobních údajů?
3. **V jakém rozsahu se osobní údaje shromažďují?**
   - Provádím zpracování dat podle účelu, který jsem specifikoval?
   - Jsou shromážděná data adekvátní, přesná a účelná?
4. **V jakém termínu se osobní údaje likvidují?**
   - Uchovávám osobní data pouze po dobu nezbytně nutnou?
5. **Jakým způsobem se osobní údaje aktualizují?**
   - Jsou shromážděná data přesná a aktualizovaná dle potřeby?
6. **Komu mohou být osobní údaje zpřístupněny?**
7. **Kdo je za dodržení interní normy týkající se výše uvedených bodů odpovědný?**
8. **Kdo je odpovědný za komunikaci se subjekty údajů?**
   - Mám k dispozici proceduru k určení práv subjektů dat s ohledem na jejich data, která zpracovávám?
9. **Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému přístupu k osobním údajům, jejich změně, zničení nebo ztrátě?**
   - Chráním dostatečně osobní údaje?
10. **Jaká interní dokumentace řeší výše uvedené body?**

1) Dotazník byl zpracován s p. prof. Telcem.

NA ZÁKLADĚ ODPOVĚDÍ NA OTÁZKY PRO AUDIT SI PŘIPRAVTE INTERNÍ SYSTÉM NEBOLI REPORTING.

Budou ho tvořit tyto 4 oblasti tvořené **přehledy** a **dokumenty**.

1. **Detailní přehled zpracování osobních údajů** ve vaší organizaci podle jednotlivých agend (např. personální), který bude obsahovat následující části:

   Typy zpracování osobních údajů podle **účelu** zpracování
   - Jaké kategorie subjektů údajů se zpracování týká (např. klienti, potenciální klienti, …)
   - Právní tituly ke každému zpracování (např. se souhlasem subjektů údajů)
   - Délka zpracování osobních údajů v závislosti na účelu zpracování
   - Uplatňování práv subjektů údajů (např. právo na přístup k osobním údajům)
   - Archivace a následná likvidace osobních údajů
   - Jsou údaje předávány nebo zpřístupňovány třetím osobám?
   - Informační systémy zpracovávající osobní údaje a jejich provázanost
   - Zásady zabezpečení osobních údajů ve vztahu k příslušné agendě
2. **Seznam všech povinností**
3. **Seznam odpovědností jednotlivých osob ve vztahu k povinnostem**
4. **Seznam všech úkolů**
   - průběžné úkoly, tj. ty, které zajistí compliance do budoucna
   - jednorázové úkoly, což je zejména řešení tzv. kostlivců ve skříni nalezených při interním auditu.

Po zpracování interního systému byste měli být schopni rozdělit reporty:

A) **monitorovací**, které vám umožní se přesvědčit, že vše ve vztahu ke zpracování osobních údajů jde normálně

B) reporty **událostní**, které vás informují, že nastalo něco, co vyžaduje vaši akci (např. havárie informačního systému, zpracovávajícího osobní údaje)

Vraťte se k přehledům, zpracovaným jako výstup interního auditu a nové povinnosti do nich zapracujte.

Ověřte si, jak váš **interní systém** a metodika funguje. Pokud jste si je nastavili správně, měli byste snáze rozpoznat nutné změny ve vašem **reportingu**, jaké nové reporty potřebujete a jak musíte změnit ty stávající.

ZPRACUJTE SEZNAM NOVÝCH POVINNOSTÍ.

Nové povinnosti vyplývají nejen z GDPR, ale např. i ze schvalovaného Nařízení na ochranu soukromí, které má podle EK platit od stejného okamžiku jako GDPR.

Musíte se naučit:
- zavést nové mechanismy pro přeshraniční přenos dat v rámci EU a mimo ni včetně přípravy tzv. Binding Corporate Rules nebo jiných právních nástrojů
- jak řešit nová pravidla pro cookies
- jak najít správného pověřence (tzv. Data Protection Officer), a jestli ho vaše organizace potřebuje
- jak správně využívat online reklamu a zda je možné využívat online profilování
- jak je třeba změnit smlouvy se zpracovateli osobních údajů
- jak realizovat právo být zapomenut za co nejnižších nákladů
- jaké nové postupy uplatnit při zjištěném porušení zabezpečení zpracovávaných osobních údajů
- a řadu dalších povinností.

POVZBUZENÍ NA ZÁVĚR

GDPR není jen spousta práce a snahy řešit otevřené otázky, ale taky obchodní příležitost. Jednak je opravdu potřeba si udělat pořádek v oblasti zpracování osobních údajů. Tím, že ochrana osobních údajů prostupuje jako digitální krev celým systémem internetové ekonomiky, udělání si pořádku v této oblasti znamená povýšit svoje podnikání na vyšší úroveň.

Další příležitost, kterou GDPR přináší, je ve vztahu k zákazníkům. Vzniká možnost dát do popředí to, co se zatím příliš neukazovalo – že organizace dbá na práva svých zákazníkům k osobním údajům a že je opravdu chrání a pečuje o ně. To je zpráva, která by se měla vrátit ve zvýšení počtu zákazníků a jejich důvěry. Implementace GDPR je tak věcí marketingových oddělení stejně jako IT nebo firemních právníků.

SDRUŽENÍ PRO INTERNETOVÝ ROZVOJ

Zpracoval a upravil SPIR (Sdružení pro internetový rozvoj) se souhlasem autora,
Mgr. Zbyňka Loebla, LLM, vedoucí práva ICT a of counsel, PRK Partners s.r.o. advokátní kancelář.
Původně vyšlo v NEXT GENERATI@N Telekomunikace 2017-01.
www.spir.cz

verze 01