DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

BDO Audit GDPR Services

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

ÚVODEM

K Obecnému nařízení o ochraně údajů („GDPR“) již bylo vydáno mnoho článků a složitých publikací pohlížejících na tuto problematiku často z jen z právního hlediska.

Nicméně, mnohým (či spíše většině) není stále jasné, jak účinně zajistit, aby do 25. května 2018 jejich organizace fungovala v souladu s GDPR. Jinými slovy je jasné, o co se jedná, stále ale zůstává mnoho otázek ohledně způsobu provedení.

V tomto Desateru navrhujeme realistický přístup k implementaci GDPR založený na našich vlastních zkušenostech a s přiměřenými náklady v rámci organizace.

KTERÝCH ORGANIZACÍ SE GDPR TÝKÁ?

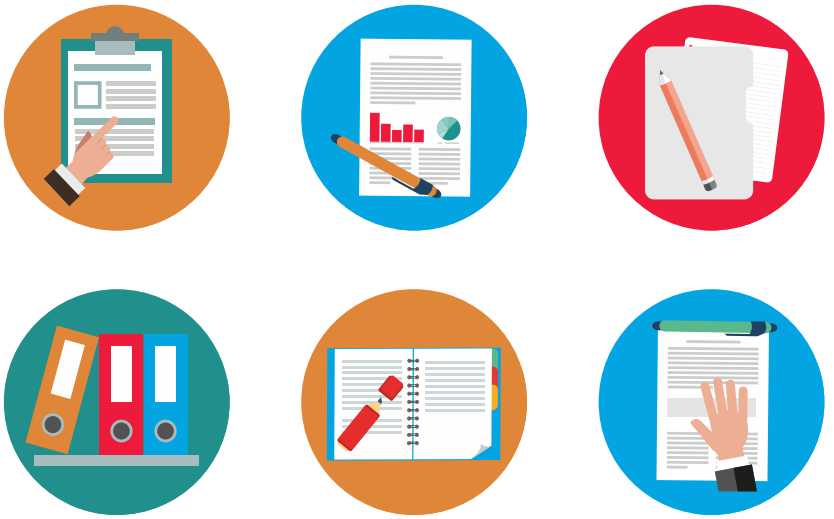
GDPR se v zásadě vztahuje na každého, kdo zpracovává osobní údaje. Vzhledem k tomu, že všechny organizace zpracovávají alespoň osobní údaje svých zaměstnanců, členů nebo spolupracovníků, GDPR se týká všech organizací bez ohledu na jejich velikost či důvod vzniku. Bude-li se však GDPR implementovat v malé organizaci co do počtu subjektu údajů a zpracovávaných osobních údajů, vynaložené úsilí by tomu mělo odpovídat.

Většina organizací však dnes spravuje řadu dalších osobních údajů: typickými případy jsou kontaktní údaje klientů v systému CRM a platební údaje klientů na internetových stránkách e-commerce.

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

Přestože pravidla GDPR jsou obsažena v právním aktu Evropské unie, jeho implementace má kromě právních aspektů také prvky organizační a IT prvky. Připravili jsme pro vás proto desatero zásad pro úspěšnou implementaci GDPR pokrývající všechny zmíněné oblasti:

1. STANOVTE ODPOVĚDNOST ZA OCHRANU OSOBNÍCH ÚDAJŮ V ORGANIZACI
2. PROMÍTNĚTE ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ DO KAŽDODENNÍ ČINNOSTI ORGANIZACE
3. ZVYŠUJTE POVĚDOMÍ V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ
4. VYTVOŘTE REGISTR OSOBNÍCH ÚDAJŮ
5. ZAVÁDĚJTE BEZPEČNOSTNÍ OPATŘENÍ S OHLEDEM RIZIKO
6. SE SOUHLASEM ZACHÁZEJTE S ROZVAHOU
7. BUĎTE OTEVŘENÍ OHLEDNĚ ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ
8. UPRAVTE SMLOUVY S DODAVATELI (ZPRACOVATELI OSOBNÍCH ÚDAJŮ)
9. KOMUNIKUJTE A PŘIPRAVTE SE NA SITUACE, KDY SE NĚCO NEPOVEDE
10. PROVĚŘTE, ZDA SE VÁS TÝKÁ POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ



DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

1.. Stanovte odpovědnost za implementaci GDPR v organizaci

Tak jako kapitán bezpečně vede svoji loď rozbouřenými vlnami, i projekt implementace GDPR si zaslouží zodpovědné řízení. S navigací může sice pomoct ten či onen externí odborník. O tom, kdy vyplout, kam až se vydat a kdy dorazit do přístavu, však může rozhodnout jen zástupce organizace mající potřebnou autoritu.

2. Promítněte zásady ochrany osobních údajů do každodenní činnosti organizace

Organizace musí přijmout a v každodenní činnosti uplatňovat zásady ochrany osobních údajů, které popisují, jak jsou data shromažďovány, používány a spravovány. Východiskem je osm hlavních zásad GDPR:

- **Zákonnost** - zpracovávat osobní údaje je možné pouze tehdy, pokud existuje
- alespoň jeden z právních titulů (důvodů) pro zpracování osobních údajů - souhlas, plnění smlouvy, plnění právní povinnosti, ochrana životně důležitých zájmů člověka, plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, oprávněné zájmy správce či třetí osoby.
- **Transparentnost** - všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků (viz níže).
- **Omezení účelem** - osobní údaje musí být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.
- **Minimalizace** - osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- **Přesnost** - osobní údaje musí být přesné a v případě potřeby aktualizované.

  Omezení uložení - osobní údaje musí být uloženy po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.

- **Bezpečnost** – organizace musí jí spravované osobní údaje chránit, ať už jde o informace v listinné nebo elektronické podobě. V praxi to znamená, že přístup k těmto informacím mají mít jen oprávněné osoby, informace budou dostupné v okamžiku jejich potřeby a bude zajištěna jejich správnost a úplnost.
- **Přístup založený na riziku** – organizace musí hodnotit zamýšlené činnosti a procesy zpracování z hlediska rizik, které z těchto činností a postupů plynou pro práva a oprávněné lidí, jejichž osobní údaje mají být zpracovávány. Praktickým dopadem je nutnost zpracovat analýzu rizik.

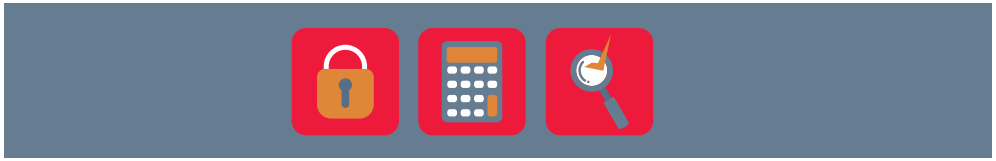
Organizace by měla zjistit dopad uvedených zásad do své činnosti a v případě nutnosti přehodnotit a upravit některé dosavadní postupy. Srozumitelně vyjádřené zásady zpracování osobních údajů v konkrétních politikách a směrnicích organizace rovněž mohou poskytnout zaměstnancům jasné pokyny k ochraně osobních údajů.

Pověřenec pro ochranu osobních údajů (viz níže) bude muset později ověřit, zda jsou pravidla skutečně dodržována.

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

3. Zvyšujte povědomí v oblasti ochrany osobních údajů

Jakmile jsou stanovena pravidla, musí být sděleny zaměstnancům, kteří osobní údaje zpracovávají (v zásadě všem administrativním pracovníkům). Tohoto cíle lze dosáhnout prostřednictvím videí, e-learningu, prezenčních školení, informačních schůzek, porad apod. – ty by měly být kombinovány s tipy a technikami pro zvyšování povědomí v oblasti bezpečnosti informací a kybernetické bezpečnosti.



4. Vytvořte registr osobních údajů

Aniž by měla organizace přehled o zpracovávaných osobních údajích, nemůže účinně kontrolovat nakládání s těmito údaji. Vytvoření registru osobních údajů tak představuje základ pro zajištění souladu s GDPR a poskytuje první pohled na druhy a množství osobních údajů v rámci organizace. V registru by mělo být zaznamenáváno:

Kategorie zpracovávaných osobních údajů

- Účel zpracování
- Kategorie osob, jejichž osobní údaje jsou zpracovávány (zaměstnanci, klienti atd.)
- Kde (v jakých systémech) a jak jsou údaje zaznamenávány
- Kdo zodpovídá za shromažďování, aktualizaci a likvidaci údajů
- Doba, po kterou jsou údaje uchovávány

Po sestavení prvotního přehledu je nutné zodpovědět následující otázky k ověření, zda je dodržováno osm základních zásad ochrany osobních údajů:

- Jaký je důvod pro zpracování údajů? Je opodstatněný?
- Je zpracování osobních údajů povoleno? Byla zaručena transparentnost, co se týče způsobu využití těchto údajů?
- Opravdu potřebujeme všechny tyto údaje? Uchováváme pouze údaje, které jsou nezbytné pro naše účely?
- Jak zajistíme, aby byly údaje přesné a aktuální?
- Jak dlouho budou údaje uchovány a je daná doba jejich uchování opravdu nezbytná?
- Jsou osobní údaje adekvátně zabezpečeny?

5. Zavádějte bezpečnostní opatření s ohledem riziko

Opatření přijatá k zajištění ochrany osobních údajů by měla být úměrná faktické citlivosti těchto údajů. Organizace by měla vždy brát v potaz potenciální újmu pro člověka, jehož osobní údaje zpracovává, v případě porušení povinností stanovených GDPR nebo zneužití těchto údajů.

Přístup založený na riziku umožňuje organizaci napnout síly směrem, kde je největší riziko. Pomáhá tak organizaci rozhodnout, kam alokovat omezené zdroje. Neznamená to však, že oblasti s nízkým rizikem by měly být organizací ignorovány.

Samotná bezpečnostní opatření jsou obvykle kombinací organizačních a IT opatření a nástrojů. Jedná se například o směrnice, prováděcí postupy, role, hesla, opatření proti škodlivému software (viry) atp. Ochranná opatření mohou být přijata na více úrovních:

- Bezpečnostní zásady a postupy
- Bezpečnost aplikací a služba Active Directory
- Zabezpečení IT infrastruktury
- Fyzická bezpečnost

BDO

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

6. Se souhlasem zacházejte s rozvahou

Souhlas je pouze jedním z právních titulů (důvodů), na kterém může být založeno zpracování osobních údajů. V zásadě by organizace měla uvažovat o souhlasu teprve tehdy, pokud není dán jiný z právních titulů pro zpracování. Na použití a podobu souhlasu jsou kladeny náročné požadavky a pro organizace není tak vždy lehké je naplnit. Nedodržení těchto požadavků může mít za následek i neplatnost souhlasu. V případě použití souhlasu proto ověřte, zda:

- Není dán jiný právní důvod pro zpracování osobních údajů
- Vyjadřuje-li se subjekt údajů ke zpracování osobních údajů a toto prohlášení se vztahuje i k jiným skutečnostem, že souhlas je od těchto jiných skutečností jasně odlišitelný
- Je souhlas informovaný, tedy jsou poskytnuty všechny relevantní informace požadované GDPR
- Je souhlas prokazatelný, tedy že organizace může bez pochybností prokázat, že jí byl souhlas řádně udělen

7. Buďte otevření ohledně zpracování osobních údajů

Důležitou zásadou ochrany osobních údajů je transparentnost vůči subjektům údajů (zaměstnancům, klientům apod.), a to ohledně způsobu shromažďování a použití osobních údajů. Od organizací bude požadováno, aby informovaly zúčastněné subjekty údajů zejména o následujících skutečnostech:

- Jaké osobní údaje jsou zpracováványNa základě čeho jsou zpracovávány
- Účely zpracování
- Doba uchovávání
- Sdílení údajů s třetími stranami
- Práva subjektů údajů

8. Upravte smlouvy s dodavateli (zpracovateli osobních údajů)

GDPR rozlišuje mezi správci, kteří určují účel a zdroje pro zpracování, a zpracovateli (dodavatelé, kteří zpracovávají data na žádost a podle pokynů správce). Příkladem je externí mzdová účetní, která zpracovává osobní údaje (výplatní pásky) jako zpracovatel na žádost svých klientů, správců osobních údajů.

GDPR vyžaduje, aby správce a zpracovatel (pracující na žádost správce) uzavřeli písemnou smlouvu. V této smlouvě musí být jasně definovány role a povinnosti týkající se ochrany osobních údajů. Mezi tyto povinnosti spadá např. závazek zajistit mlčenlivost nebo poskytnout součinnost správci pro splnění správcovy povinnosti reagovat na oprávněné žádosti subjektů údajů.

Bude stále důležitější, aby dodavatelé prokázali potenciálním i stávajícím klientům svou spolehlivost v oblasti ochrany údajů. To lze provést pomocí auditů připravenosti na GDPR, které dodavatelům umožní prokázat, že splňují všechny požadavky GDPR.

BDO

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

9. Komunikujte a připravte se na situace, kdy se něco nepovede

Úřad pro ochranu osobních údajů a případně také subjekty údajů budou muset být informovány o narušení ochrany osobních údajů. Pro tyto účely je vhodné zavést postupy pro případ bezpečnostního incidentu evidenci těchto incidentů. Podobný systém je často využíván bezpečnostními pracovníky organizace – a po několika malých úpravách může být použit i pro GDPR. V tomto systému musí být evidovány a analyzovány zjištěné incidenty. Cílem je vyhodnocení závažnosti incidentu – na základě tohoto se rozhodne, zda je třeba informovat Úřad pro ochranu osobních údajů a subjekty údajů.

V případě informování Úřadu pro ochranu osobních údajů o narušení ochrany údajů je nutné uvést:

- Co se stalo
- Jaké jsou pravděpodobní důsledky narušení osobních údajů
- Jaká opatření byla přijata ke zmírnění nepříznivých dopadů
- Odpovědnost organizace a výše případných pokut se bude odvíjet od toho, jaké úsilí organizace vynaložila k zabránění narušení osobních údajů, případně jaké kroky podnikla k vyřešení daného narušení.
- Zaměstnanci, kteří budou v případě bezpečnostního incidentu vykonávat definované činnosti, by k tomu měli být řádně proškoleni.

10. Prověřte, zda se vás týká pověřenec pro ochranu osobních údajů

GDPR vytváří novou pozici pověřence pro ochranu osobních údajů. Pověřenec odpovídá za kontrolu dodržování zásad GDPR v rámci organizace. Pověřenec by měl vedení organizace také dávat doporučení k zajištění souladu s GDPR. Pověřenec se může také vyjadřovat k posouzení vlivu na ochranu osobních údajů, účinnosti bezpečnostních opatření, návrhům dohod se zpracovateli. Kromě toho může mít řadu dalších stálých úkolů, jako je pořádání informačních schůzek týkajících se ochrany osobních údajů, prošetřování stížností v této oblasti a odpovídání na dotazy ohledně ochrany osobních údajů nebo prověřování bezpečnosti osobních údajů u třetích stran. Úřad pro ochranu osobních údajů může pověřence kontaktovat kvůli poskytnutí informací a pověřenec je povinen poskytnout součinnost.

Funkci pověřence musí zřídit všechny orgány veřejné moci a veřejné subjekty (např. obce, kraje, ministerstva). Jiné subjekty budou muset zřídit funkci pověřence, pokud je s jejich hlavní činností spojeno rozsáhlé zpracování osobních údajů. Do této kategorie budu spadat např. nemocnice, banky, pojišťovny, telefonní operátoři a další subjekty.

U ostatních organizací, které nesplňují uvedená kritéria, je zřízení funkce pověřence pro ochranu osobních údajů doporučováno jako příklad dobré praxe.

BDO

DESATERO ÚSPĚŠNÉ IMPLEMENTACE GDPR

KYBERBEZPEČNOST A GDPR

Kybernetické incidenty jsou jednou z hlavních příčin narušení ochrany údajů: hackeři mohou ukrást osobní údaje. Očekává se, že podobné útoky se stanou stále častějšími.

Dobrá kybernetická ochrana se tak stane důležitou součástí dodržování předpisů GDPR. Dokonalá ochrana bohužel neexistuje – techniky používané hackery jsou stále sofistikovanější a je prakticky nemožné se připravit na cokoliv, co by se mohlo stát. Je tedy třeba přijmout nejen preventivní opatření, ale také připravit plán pro případ, kdy hackeři bezpečnostní opatření obejdou.

V každém případě je důležité zajistit, aby byla zavedena "základní" opatření, jako je patch management, silná hesla, firewall, šifrování apod. Tak bude organizace schopna prokázat, že jednala s náležitou péčí, pokud dojde k narušení zpracovávaných osobních údajů. Žádná ochrana však není stoprocentní. Z tohoto důvodu stále více organizací uzavírá pojistky pro krytí kybernetických rizik.

PLÁN, JAK DOSÁHNOUT SOULADU S GDPR DO 25. KVĚTNA 2018

Vaše organizace ještě nepracuje na implantaci GDPR? Není žádný důvod k panice, protože nedávný průzkum provedený BDO Audit s.r.o. ukázal, že 54 % organizací se s GDPR teprve seznamuje a je na tom podobně jako vy. Znamená to však, že je čas konat.

Vše začíná posouzením souladu s GDPR, při němž jsou identifikovány nedostatky ve vztahu k GDPR – na základě toho je vypracován odpovídající akční plán.

Důležitou součástí je vytvoření počátečního registru osobních údajů ve vaší organizaci, který vám pomůže získat jasnou představu o úsilí, které bude nutné vyvinout pro splnění požadavků GDPR.

JAK VÁM MŮŽEME POMOCI?

GDPR vyžaduje kompetence a zdroje ve více doménách: organizační, právní a IT. Náš tým odborníků vám může pomoci v následujících oblastech:

- **Audit připravenosti na GDPR: obvykle jde o první krok k dosažení souladu s pravidly GDPR. Při posouzení je zjištěna současná situace, stejně jako nedostatky s ohledem na po6avkz stanovené GDPR. Na základě toho jsou stanoveny návrhy konkrétních opatření a je vypracován pragmatický akční plán.**
- **Podpora při implementaci GDPR: jakmile je plán stanoven, jeho různé prvky musí být provedeny na organizační, IT a právní úrovni. Můžeme vám pomoci s implementací těchto prvků.**
- **Pověřenec pro ochranu osobních údajů: tato pozice je k 25. květnu 2018 vyžadována pro mnoho organizací. Můžeme pro vás tuto roli zajistit.**
- **Vzdělávání v oblasti GDPR: připravíme pro vás a vaše zaměstnance semináře na míru nebo vám poskytneme náš akreditovaný e-learning, včetně testů a možnosti získat certifikát o absolvování kurzu.**

Zaujala vás naše nabídka? Prosím, kontaktujte naše specialisty.

Ondřej Šnejdar
Partner
+420 777 312 365
ondrej.snejdar@bdo.cz

Stanislav Klika
Senior Manager
+420 604 226 734
stanislav.klika@bdo.cz

BDO Audit s.r.o.
+420 241 046 221
Olbrachtova 1980/5
140 00 Praha 4

BDO