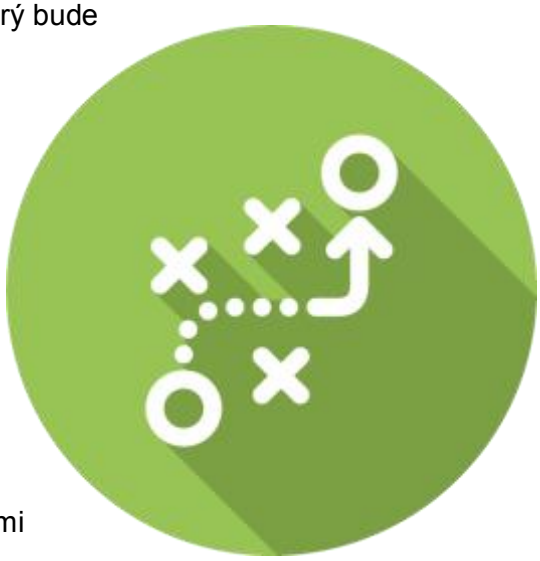
Harmonogram implementace GDPR

Obecné nařízení EU o ochraně osobních údajů (GDPR) nabude účinnosti dne 25. 5. 2018. Abyste dodrželi všechna pravidla a podmínky stanové GDPR, je dobré se dostatečně připravit a s Nařízením se podrobně seznámit. Tento článek by vám měl pomoci se v procesu přípravy zorientovat a stanovit si vlastní postup, který bude aplikovatelný na Vaší společnost či organizaci.



Dříve než se blíže podíváme na jednotlivé etapy přípravy na GDPR, je nutné říci, že ještě před samotným zahájením přípravy je nutné, aby si společnost ujasnila a definovala, v jaké roli je vůči osobním údajům, které zpracovává. Podle toho zda jste správce či zpracovatel, se liší Vaše povinnosti. Proces přípravy by také kromě přesně vymezených fází, měl mít stanovený svůj časový rámec, rozpočet a vymezenou odpovědnost mezi jednotlivými zúčastněnými osobami.

Fáze přípravy

1. Přípravná fáze;
2. Analýza a zmapování současného stavu;
3. GAP analýza (včetně analýzy firemní dokumentace);
4. Dopadová analýza;
5. Definice cílového stavu, návrhy a implementace změn;

Přípravná fáze

Tato fáze především obsahuje vypracování plánu, jak bude příprava na GDPR vypadat, co vše se bude muset zrevidovat (jak rozsáhlá je dokumentace organizace) a popřípadě změnit. Také je potřeba stanovit rozpočtový rámec na přípravu a sestavit tým lidí, kteří přípravu na GDPR budou provádět. V rámci dostatečné efektivity je potřeba, aby v tomto týmu byli i kromě řadových pracovníků, také zástupci vedení společnosti (především střední a vyšší management). V případě, že budete jmenovat Pověřence pro ochranu osobních údajů (DPO), je velice žádoucí, aby i tato osoba byla součástí týmu již v přípravné fázi.

Analýza a zmapování současného stavu

Úplně prvním úkonem je detailní zmapování a rozbor toho, kde všude a jakými prostředky se zpracovávají osobní údaje ve Vaší společnosti (IT systémy, fyzické dokumenty, HR oddělení a další) a to včetně osob, které mají k osobním údajům přístup (platí i pro pouhé nahlížení). Velmi důležité je také zmapování základních činností, které se s údaji provádí (sběr, evidence, aktualizování, odstraňování, popřípadě i profilování). Pro co nejdetailnější zmapování veškerých toků osobních údajů, je nejefektivnější si zodpovědět šest základních otázek, které se zpracování osobních údajů týkají – co, jak, kdo, kdy, o kom a proč:

1. **CO** – Zjistit jaké všechny osobní údaje máte a vytvořit seznam všech doposud zpracovávaných osobních údajů (například jméno, příjmení, rodné číslo, bydliště, číslo kreditní karty, IP adresa a další), tyto údaje poté specifikovat a popřípadě je rozdělit ještě do kategorie zvláštních (citlivých) údajů nebo údajů týkajících se dětí. Dále zaznamenat zdroje osobních údajů, tedy kdo mi údaje poskytl (sám subjekt osobních údajů, vlastní evidence, veřejné registry, třetí strany a jiné);
2. **JAK** - Jakými prostředky se zpracovávají, shromažďují a ukládají osobní údaje ve Vaší společnosti (IT systémy, fyzické dokumenty, HR oddělení a další). Měly by být popsány nejen nástroje pro zpracovávání a ukládání, ale také samotné postupy zpracovávání;
3. **KDO** – Které osoby primárně osobní údaje zpracovávají a současně mají zodpovědnost za jejich aktuálnost a správnost. Kterým osobám mohou být osobní údaje zpřístupněny, včetně důvodů zpracování, stanovení podmínek, způsobů a doby zpracování;
4. **KDY** – Zmapování časového charakteru zpracovávání osobních údajů – Kdy byly osobní údaje získány, jak často dochází k aktualizacím dat, po jak dlouho dobu jsou data uchovávána, včetně mechanismů k určení těchto lhůt;
5. **O KOM** – Identifikace subjektu údajů, tedy fyzické osoby, jejichž osobní údaje jsem zpracovával nebo budu zpracovávat. Touto identifikací dojdeme také k tomu, které všechny osoby mají právo na získávání, opravu, předávání, aktualizaci či výmaz svých osobních údajů;

6. **PROČ** - Tedy určení *účelu zpracování* (proč či za jakým účelem chcete osobní údaje subjektu zpracovávat) a následně zejména *právního titulu* pro zpracování (souhlas subjektu údajů se zpracováním; plnění uzavřené smlouvy; plnění právní povinnosti stanovené zákonem; oprávněný zájem správce na zpracování; veřejný zájem správce nebo životně důležitý zájem).

Dalším nezbytným krokem je analýza procesů, tedy identifikace a popis všech konkrétních činností, které se s osobními údaji provádí a jakými způsoby se údaje zpracovávají. Musí také dojít k revizi všech stávajících souhlasů a smluv, které máte vzhledem k subjektům údajů v držení tak, aby byly v souladu s legislativou GDPR (a byly opětovně odsouhlaseny či dodatkovány), chcete-li je používat i po 25. květnu 2018.

GAP analýza (včetně analýzy firemní dokumentace)

V rámci této analýzy by správce měl provést hloubkovou analýzu a revizi veškeré své dokumentace (smlouvy, podmínky, kodexy, směrnice a další), a to i vzorové, včetně revize souhlasů, jejich získávání a systému uchovávání. Poté by měly být vygenerovány požadavky, které správce musí splnit a postup pro jejich naplňování. Mělo by také dojít k porovnání současné právní úpravy ochrany osobních údajů ve společnosti s GDPR a stanovení nutných a potřebných změn. Je také možné, že budete muset upravit i již uzavřené smlouvy, v takovém případě doporučujeme namísto obnovování celých smluv uzavírání příslušných dodatků. Kontrolou by také měly projít všechny smlouvy, kde dochází k vymezení pravomocí mezi správcem a zpracovatelem (především vymezení odpovědnosti jednotlivých aktérů). V rámci GAP analýzy byste neměli opomenout zanalyzovat i oblast automatizovaného zpracovávání a předávání osobních údajů do třetích zemí.

Dopadová analýza

V rámci této analýzy by především mělo dojít k popsání jednotlivých dopadů přípravy na GDPR na jednotlivá oddělení a segmenty společnosti, včetně stanovení a posouzení rizik. Nařízení totiž stanovuje podmínku, aby správce přizpůsobil organizační a technická opaření tomu, jak vysokou míru rizika zpracovávání osobních údajů představuje pro práva a svobody jednotlivce. V rámci souhrnné analýzy rizik, by se společnosti měli především zaměřit na:

- Vypracování dokumentu Posouzení vlivu na ochranu osobních údajů;
- Míru pravděpodobnosti obdržení pokuty od dozorového orgánu;
- Rizika, která mohou postihnout subjekty údajů;
- Odpovědnost vyplývající z občansko-právních sporů;
- Riziko zhoršení reputace či renomé společnosti;
- Možnost výskytu pracovně-právních sporů;

Měla by tak býti vypracována analýza ohledně zabezpečení informací a osobních údajů, a to včetně všech informačních systémů, cloudových řešení či fyzického uložení dokumentů. Současně by také měla být provedena analýzu vlivu požadavků na GDPR na IT systémy, která ukáže, jak má společnost nastavené informační systémy a jiná technologická řešení a zda jsou dostačující pro GDPR.

Definice cílového stavu, návrhy a implementace změn

V této fázi přípravy na GDPR byste již měli přesně znát současný stav Vaší společnosti v oblasti zabezpečení osobních údajů. Teď musíte všechny zanalyzované poznatky porovnat s požadavky GDPR, odhalit mezery a stanovit postup úprav a změn. Abyste získali přesné informace o tom, jaké všechny konkrétní změny budou muset být provedeny, můžete provést analýzu rozdílů nebo-li rozdílovou analýzu, které identifikuje nutné kroky k tomu, abyste vše měli v souladu s GDPR. Postup reálné přípravy na požadavky GDPR dle výsledků analýz může být proveden v těchto krocích:

- Kontrola současných informačních systémů, zda splňují veškeré požadavky GDPR.
- Stanovení požadavků na změny.
- Stanovení možných mezer a nedostatků, které mohou vzniknout během tvorby a implementace nových systémů a postupů.
- Provést zkušební test a na základě zpětné vazby doladit či změnit nefunkční oblasti.

V rámci této poslední fáze by také mělo dojít k implementaci jednotlivých procesů, které zajistí dodržování GDPR. Na tuto část přípravy si stanovte dostatečný časový rámec, včetně dostačujících finančních zdrojů a personálních kapacit. Měli byste dostatečnou pozornost věnovat především těmto pravidlům GDPR:

- Zajištěná tvorby záznamů o činnostech zpracování – Dokumentace veškerých činností, které se provádějí v rámci zpracování osobních údajů.
- Dostatečné zajištění práv subjektů údajů – Musíte být schopní garantovat všechna práva, které mu Nařízení přiznává (právo na přístup k osobním údajům, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost, právo vznést námitku…).

Během této poslední fáze byste také již měli mít jasno, zda se na Vás vztahuje povinnost jmenovat Pověřence na ochranu osobních údajů – povinnost ho jmenovat, je stanovená v těchto případech zpracování osobních údajů:

- Provádí-li-ho orgány veřejné moci (ministerstva, obce, kraje a jejich příspěvkové organizace);
- Provádí-li-ho správci či zpracovatelé, jejichž hlavní činnost vyžaduje rozsáhlé, pravidelné a systematické monitorování subjektů (spadají sem zejména subjekty, které používají emailový retargeting, profilování, dále věrnostní programy, lokalizační údaje, monitorování prostor a další);
- Provádí-li-ho správci či zpracovatelé, jejichž hlavní činnost vyžaduje rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů;

V případě, že povinnost jmenovat Pověřence máte a neučiníte tak, může vám být uložena sankce až do výše 10 milionů EUR nebo 2 % celosvětového ročního obratu společnosti, podle toho, co je větší.

Pověřenec na ochranu osobních údajů musí být především expert v oblasti ochrany dat, znalý práva, interních procesů a IT technologií. Je nutné, aby byl přímo podřízen nejvýše postavené osobě ve společnosti a nedocházelo u něj ke střetu zájmů. Můžete si tuto osobu zajistit jak interním, tak i externím způsobem. Jeho hlavní povinností bude dbát na dodržování Nařízení a být kontaktní osobou jak pro subjekty osobních údajů (ty zejména), ale také pro dozorový úřad. Na prvním místě by pro něj měl být zájem subjektů údajů před

zájmy samotného správce osobních údajů. Pro tuto pozici neexistuje jednotně uznávaná certifikace.

Pokud tedy máte povinnost jmenovat Pověřence, tato fáze je nejzazší možnou dobou, kdy tak můžete učinit. Mnohem efektivnější však je Pověřence jmenovat již v přípravné fázi, aby mohl být plnohodnotnou součástí přípravy společnosti na GDPR. Například v rámci vypracování dokumentu Posouzení vlivu na ochranu osobních údajů, Nařízení stanovuje včasné zapojení DPO do přípravy dokumentu, včetně vypracování posudku.

V rámci této fáze je také nutné, aby došlo k proškolení všech zaměstnanců, kteří v rámci školení budou seznámeni s novými změnami a také jim budou vysvětlena nová pravidla, která musí dodržovat.
Dále společnost také musí nastavit postupy, které minimalizují škody v případě úniku dat či porušení zabezpečení a zároveň zajistí nahlášení události dozorovému orgánu (maximálně do 72 hodin) a popřípadě i samotnému subjektu údajů.

<u>Samotná závěrečná implementace by měla obsahovat tyto kroky:</u>

- Vývoj a nastavení nových technologií;
- Změna a aktualizace systémů a procesů na zpracovávání osobních údajů;
- Kontrola, zda veškerá dokumentace a nastavené postupy pro spolupráci s externími složkami, včetně dodavatelů jsou v souladu s GDPR;
- Aktualizace kodexů, interních předpisů, směrnic a dalších dokumentů;
- Dostatečné proškolení zaměstnanců;
- Spuštění bezpečnostních a kontrolních mechanismů;
- Stanovená účelů a právních titulů pro zpracovávání osobních údajů;
- Stanovení nového procesu získávání a uchovávání souhlasů, tak, aby vše bylo v souladu s GDPR;

V případě, že si nejste jisti, zda harmonogram přípravy na GDPR máte zpracován dobře, či nevíte zda harmonogram obsahuje všechno, nebojte se obrátit na odborné firmy, které se GDPR zabývají a dokáží vám tak relevantně poradit a pomoci.

Mgr. Barbora Švandrlíková

Absolvovala s vyznamenáním magisterský studijní program Mezinárodní a diplomatická studia na Vysoké škole mezinárodních a veřejných vztahů Praha, o. p. s., čímž ukončila své devítileté studium mezinárodních vztahů, diplomacie, národní a mezinárodní bezpečnosti, včetně integračních procesů v regionálních i mezinárodních organizacích.

Necelé dva roky také působila v Kabinetu ministra na Ministerstvu zahraničních věcí ČR, náplní její práce byla manipulace s důvěrnými a tajnými dokumenty.

V současné době Barbora své zkušenosti a praxi zúročuje ve společnosti Goodking Holding a. s., ve které působí jako Data Protection Officer a zajišťuje chod vzdělávacích kurzů.