Jak jste na tom s přípravou na GDPR?

GDPR ≠ IT + software.

Nové nařízení o ochraně osobních údajů má 778 řádků a z toho jen 26 se přímo týká IT bezpečnosti.

České firmy a instituce i přes narůstající mediální zájem o problematiku GDPR stále tápou, v jakém rozsahu se jich *Obecné nařízení o ochraně osobních údajů* dotkne. Často nevědí, zda vůbec a co případně začít dělat, aby svou organizaci dovedly do stavu souladu s GDPR principy.

Je mylné si myslet, že se malých společností či fyzických osob GDPR vůbec netýká, protože nezpracovávají žádné osobní údaje. Bohužel však zapomínají na jednu maličkost. A to na své **zaměstnance**, kteří jsou zdrojem celé řady údajů, jež je zapotřebí adekvátně chránit a zpracovávat podle zákona.

K tomu bohatě stačí, aby plnily povinnosti podle současného zákona o ochraně osobních údajů. Pak pro ně **GDPR nebude žádnou revolucí**, ale pouhou revizí povinností podle současného zákona, který je s GDPR velmi kompatibilní.

V případě porušení, nezavedení či nepřipravenosti na nové nařízení hrozí povinným subjektům vysoké pokuty, které mohou být v mnoha případech až likvidační.

GDPR po vzoru předpisů na ochranu hospodářské soutěže zavádí několikanásobně vyšší pokuty, než jsme byli doposud zvyklí. Jejich maximální výše je 20.000.000 eur nebo 4 % z celkového ročního obratu společnosti (vyšší z obou možností) a bude záviset na řadě faktorů, jako je např. povaha, závažnost a délka porušování, počet poškozených občanů a míra škody, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, kategorie osobních údajů dotčené porušením a řada dalších.

Je důležité zdůraznit, že maximální výše pokuty může být udělena jak menší společnosti s pěti zaměstnanci, tak velké nadnárodní korporaci, pokud neučiní kroky nezbytné k uvedení do souladu s principy a povinnostmi vyplývajícími z GDPR.

Kromě udělení těchto správních pokut mohou být správci či zpracovatelé osobních údajů navíc vystaveni žalobám podaným fyzickými osobami s nárokem na náhradu škody v případě hmotné či nehmotné újmy. V neposlední řadě jsou společnosti vystaveny ztrátě důvěry a reputačním rizikům způsobeným nesprávným zacházením s osobními údaji.

Z obyčejných dat osobní údaje

Nejde ale zdaleka jen o zaměstnance. S činností firem nebo státních institucí je nerozlučně spjata také **komunikace se zákazníky** nebo obchodními partnery, kteří jsou nositeli dat. A ta se mohou v kontextu dalšího zpracování stát osobními údaji.

Je úplně jedno, jestli jste malou organizací o několika zaměstnancích, nebo velkým nadnárodním korporátem. Dopad povinností vyplývajících z GDPR je neúprosný.

Na základě dosavadních zkušeností jsem pro vás proto níže připravila **praktický dotazník,** který vás navede, jak přistoupit ke *GDPR compliance* projektu zodpovědněji a bez krátkozrakých řešení. Ta mohou v konečném důsledku celý projekt zbytečně prodražit a hlavně vás připravit o další čas v již tak nekompromisně se zkracujícím období. GDPR vstoupí v účinnost už 25. května 2018.

GDPR ≠ IT + software

Znovu si neodpustím rýpnutí do jednorožců ověnčených čerstvě vytištěným barevným certifikátem, kteří teprve nedávno nastartovali svou kariéru v oblasti ochrany dat v domnění, že jim zajistí skvělou finanční budoucnost.

Víte například, že samotný text GDPR nařízení obsahuje 778 řádků a pouze 26 z nich se přímo týká IT bezpečnosti?

Pokud tedy zavedete ve společnosti ISO 27001, tak jste právě splnili 3,34 % z celkových povinností, které obecné nařízení společnostem ukládá. Když vás začnou různí experti přesvědčovat o zavedení této normy nebo nákupu jiného zázračného produktu či softwaru, opět bůhvíjak certifikovaného, mějte se na pozoru.

GDPR totiž není primárně o technologiích, ačkoli na ně má jeho implementace významný dopad. Zbytek povinností souvisí s tzv. **data governance** neboli se způsobem, jak je vaše organizace řízena a kontrolována. A to nejenom prostřednictvím pregnantně napsaných interních směrnic a celé škály pravidel uložených v šuplíku nebo v lepším případě na sdíleném úložišti. Jde o to, jak je podle nich celá organizace nastavená a jak se v reálném životě chová vůči svým zaměstnancům, zákazníkům nebo obchodním partnerům.

Praktické přínosy GDPR

Tento proces musí být zahájen shora, tj. vrcholovým managementem, a musí se stát nezbytnou a samozřejmou aktivitou každého zaměstnance společnosti. Pokud budete GDPR vnímat jen jako další, pod pohrůžkou vysokých pokut Bruselem vynucovaný jednorázový projekt, jehož výsledkem bude sepsání několika dalších směrnic a pravidel, tak snad ani nemá cenu, abyste se novými pravidly vůbec zabývali. GDPR se musí stát vaší **každodenní samozřejmostí** a jeho uplatňování součástí vaší firemní kultury.

Několik příkladů z praxe:

Pokud vám zavolá neznámá firma s nabídkou nového produktu, na který jste se jednou ptali přes jejich web, tak by mělo být samozřejmostí, že se vás na samém začátku rozhovoru zeptají, zda souhlasíte s pokračováním hovoru vedeného se záměrem vám zboží prodat. Když odmítnete, hovor by měl být slušně ukončen a společnost na vás nebude naléhat žádnými dalšími otázkami.

Zdá se vám to nemožné?

Ani návštěva **nemocnice** nebo jakéhokoli jiného zdravotnického zařízení nemusí být doprovázena traumatem z toho, kdo všechno si přečte vaši diagnózu. Nebo si na chodbě, případně v rámci vizity za účasti ostatních pacientů, kteří s vámi sdílejí pokoj, vyslechne o vašich zdravotních problémech takové detaily, jež nesvěřujete ani svému nejbližšímu okolí.

K tomu, aby vše bylo jinak, stačí celkem málo. **Změnit kulturu chování a přístupu k soukromí** tak, že prostřednictvím moderních technologií budete po celou dobu pobytu v nemocnici registrováni pod čárovým kódem nebo jiným identifikátorem. Ten znemožní odhalení identity včetně citlivých osobních údajů široké veřejnosti.

Jednoduchý test GDPR připravenosti

Následující **otázky** představují zkrácený výtah z mnohem delšího dotazníku, který využívám při poradenství pro GDPR analýzy či audity. Jako takový je určený hlavně pro střední a velké organizace s rozsáhlou agendou. Nicméně, i pokud jste živnostník, malá firma či úřad a pracujete s osobními údaji, můžete si tyto otázky jednoduše přizpůsobit a odpovědět na ně.

Pokud na většinu otázek odpovíte uspokojivě, tak vám gratuluji, protože jste **pravděpodobně splnili většinu povinností** vyplývajících už ze současného zákona o ochraně osobních údajů. Adaptace na GDPR pravidla tak pro vás bude hračka.
V opačném případě možná díky dotazníku pochopíte, kde máte mezery a že před sebou máte ještě spoustu práce.

Jste připraveni? Tak pojďme na test:

A. Organizační struktura

1. **Předáváte osobní údaje do zahraničí nebo v rámci skupiny firem tvořících organizační strukturu? Pokud ano, jaké údaje a do jakých zemí?**
Například zpracování osobních údajů zaměstnanců spojených s výplatou mezd zahraniční společností, sdílení klientské databáze s ostatními společnostmi tvořícími holdingovou strukturu.

2. **Máte ve společnosti ustanovenu osobu zodpovědnou za agendu ochrany osobních údajů? Kde se tato osoba nachází v rámci organizační struktury a jaké jsou kvalifikační předpoklady pro výkon této funkce? Jaká je pracovní náplň této osoby?**
Například pověřená osoba v HR oddělení nebo bezpečnostní manažer.

3. **Máte vytvořenu sestavu interních směrnic za účelem ochrany osobních údajů? Kde jsou uloženy? Jak jsou zpřístupněny zaměstnancům a třetím stranám?**
Například samostatná směrnice pro ochranu osobních údajů, která je součástí interní sestavy veškerých směrnic.

4. **Jak často probíhají školení ve vaší společnosti v oblasti nakládání s osobními údaji? Jakou formou jsou vedená, kdo je provádí a pro koho jsou určená?**

5. **Zavedli jste proces identifikace a zvládání incidentů bezpečnosti informací? Pokrývá tento proces případy porušení ochrany osobních údajů, nebo jsou tyto případy řešeny samostatně? Jaká dokumentace k výše uvedenému existuje?**
Například samostatný proces řízení bezpečnostních incidentů zavedený v rámci systému řízení bezpečnosti informací, který zahrnuje případy porušení ochrany osobních údajů formalizovaných v dokumentaci ISMS apod.

B. Osobní údaje a jejich zpracování

6. **Jaká osobní data svých zaměstnanců sbíráte a zpracováváte?**
Například:

- ***Obecné údaje:*** *jméno a příjmení, věk a datum narození, pohlaví, osobní stav, občanství, IP adresa, fotografie nebo jiný obrazový materiál, finanční údaje (čísla kreditních karet, bankovních účtů apod.).*
- ***Organizační údaje:*** *pracovní a osobní e-mailová adresa, pracovní nebo osobní mobilní telefon, pracovní a osobní adresa, číslo pasu a občanského průkazu, rodné číslo či jiné ověřovací a identifikační údaje.*
- ***Citlivé údaje:*** *rasa či etnický původ, náboženské, politické či filozofické vyznání, členství v odborech, sexuální orientace, zdravotní stav, trestní delikty či pravomocné odsouzení, genetické údaje (krevní rozbory, DNA profil, rentgenové snímky, důvěrné lékařské zprávy atd.), biometrické údaje (podpis, daktyloskopické údaje, snímky obličeje či jiných částí těla, hlasové záznamy apod.).*

7. **Jaká další osobní data sbíráte a zpracováváte? Přesně vyjmenujte charakter zákazníků nebo jiných subjektů, jejichž data sbíráte a zpracováváte. Jaký je účel (zákonný důvod) zpracování těchto osobních údajů?**
Například sbíráte data pro marketingové účely, kvůli zasílání obchodních sdělení atd. Charakter dat je podobný jako u předchozí otázky (obecné, organizační a citlivé údaje).

8. **Kdo ve společnosti provádí analýzu rizik osobních údajů?**
Analýza umožní nastavit opatření proti realizaci rizika zneužití osobních údajů.

9. **Kdo osobní údaje ve společnosti sbírá a zpracovává?**
Jaké organizační útvary? Kolik pracovníků? Předáváte osobní údaje do zahraničí nebo v rámci skupiny firem tvořících organizační strukturu? Pokud ano, do jakých zemí?

10. **Po jak dlouhou dobu osobní údaje zpracováváte? Jak často osobní údaje aktualizujete?**
Pro každý zpracovávaný osobní údaj uveďte přesnou lhůtu, po kterou je zpracováván.

11. **Provádíte automatizované nebo manuální zpracování osobních údajů, případně obojí?**
Jakými nejčastějšími/hlavními způsoby jsou přenášena data obsahující osobní údaje směrem od nebo ke klientům (či jiným třetím stranám)?

12. **Jste správcem?**
Správce je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám či společně s jinými určuje účely a prostředky zpracování osobních údajů. Správce je tedy subjekt, který se rozhodl provádět zpracování a tímto zpracováním sleduje určitý cíl. Je tak osobou odpovědnou za nastavení podmínek zpracování.

13. **Jste zpracovatelem?**
Zpracovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce (jako službu). Zpracovatel na rozdíl od správce nezpracovává osobní údaje, aby naplňoval určitý účel, ale pouze technicky zajišťuje určité činnosti při zpracování osobních údajů pro správce. Typickým zpracovatelem je například poskytovatel cloudových služeb, kde má správce uložena data, nebo poskytovatel webhostingu, případně e-mailových služeb nebo služby mzdové agendy.

14. **Jste správcem i zpracovatelem zároveň?**
Vykonáváte obě role?

15. **Požadujete souhlas subjektu dat s poskytnutím jeho osobních údajů pro každé zpracování? Omezujete zpracování osobních údajů pouze pro účely, pro které jste obdrželi souhlas od subjektu údajů?**
Informujete subjekt o důvodech shromažďování a následného zpracování dat včetně poskytnutí jeho osobních údajů třetím stranám?

16. **Máte ve své společnosti nainstalovaný kamerový systém? Po jak dlouhou dobu uchováváte záznamy z těchto systémů?**
Používáte GPS nebo jiný nástroj kromě kamerového systému pro monitorování zaměstnanců nebo vašeho majetku?

17. **Zpracováváte osobní údaje dětí?**
Zpracování osobních údajů dětí mladších 13 let vyžaduje souhlas zákonného zástupce.

18. **Rozesíláte marketingová nebo jiná obchodní sdělení? Provádíte tuto aktivitu sami nebo prostřednictvím třetích osob? Využíváte služeb tzv. call center? Provozujete e-shop?**
V mnoha případech musíte získat předchozí souhlas se zasíláním marketingových sdělení, k nimž se osoby dobrovolně přihlásí (tzv. opt-in). Máte takové souhlasy řádně evidované? Máte vlastní call centrum, nebo využíváte tuto službu od třetí strany?

19. **Máte přehled, kde jsou osobní údaje uloženy včetně externích úložišť?**
Uveďte všechny vám známé úložiště osobních údajů, například listinné dokumenty, CRM, e-maily, různé nestrukturované databáze, mzdové nebo jiné informační systémy.

20. **Máte přehled, kdo a v jakém rozsahu má přístup k osobním údajům včetně externích partnerů?**
Například daňoví poradci, auditoři, advokáti, konzultanti atd. Máte seznam všech externích partnerů, kterým jsou osobní údaje poskytnuty? Máte s nimi podepsány smlouvy o zpracování osobních údajů?

21. **Máte nastavený formální proces a informovanost v podobě interní směrnice pro případ odvolání souhlasu subjektu dat se zpracováním jeho osobních údajů?**
Evidujete souhlasy? V jakém systému? Aktualizujete tuto databázi? Jakým způsobem zajišťujete odvolání souhlasu?

22. **Umíte na požádání subjektu, jehož data zpracováváte, zajistit přístup k jeho osobním údajům? Máte nastavený formální proces a informovanost v podobě interní směrnice pro přístup subjektů k údajům, které o nich zpracováváte?**
Poskytujete informace o tom, kdo, co, kde, jak dlouho a proč zpracovává osobní údaje? Existuje ve vaší společnosti centrální databáze aktuálních osobních údajů?

23. **Umíte na požádání zajistit opravu osobních údajů nebo přenos osobních údajů třetí straně?**
Jak často ověřujete správnost a aktuální informace o svěřených osobních údajích? Je váš informační systém připraven na podobnou žádost subjektu, aby mohly být jeho osobní údaje přeneseny jinému správci?

Právo na opravu znamená, že v případě, kdy máme podezření na nesprávnost našich údajů a to subjektivní nebo objektivní povahy, můžeme požádat danou společnost o nápravu. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení. Správce by měl zajistit podmínky pro to, aby žádosti na opravu mohly být podávány online, zejména v případě zpracování osobních údajů elektronickými prostředky.

24. **Umíte zajistit výmaz osobních údajů z důvodu, že již nejsou potřebné nebo na základě odvolání souhlasu fyzické osoby? Informujete zpracovatele, že mají zpracovávané osobní údaje vymazat?**
Mažete nebo nezpracováváte osobní údaje subjektů, které již nepotřebujete, resp. pominul účel jejich zpracování? Například bezpečné mazání s protokolárním záznamem u souborů údajů, u kterých vypršela retenční doba stanovená v souladu s účelem zpracování. Funguje takové smazání centrálně, tj. údaj se vymaže ve všech databázích včetně záložních (platí pro elektronické i papírové databáze)?

Právo na výmaz je naprosto novým právem podle GDPR, které ukládá správci osobních údajů povinnost bez zbytečného odkladu vymazat naše osobní údaje, pokud je dán jeden z těchto důvodů:

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
- Občan odvolá souhlas, pokud je zpracování založeno na souhlasu, a neexistuje žádný další právní důvod pro zpracování.
- Občan vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
- Osobní údaje byly zpracovány protiprávně.
- Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí.
- Právní povinnost stanovená právem Unie nebo členským státem.

C. Informační bezpečnost

25. **Kdo má zodpovědnost za řízení informační bezpečnosti organizace?**
Jaký k tomu má mandát, jaké povinnosti a odpovědnosti? Podílejí se na řízení informační bezpečnosti vlastníci či garanti primárních aktiv organizace? Jak? Existuje procesní mapa s vazbou na IT organizace anebo vlastníky? Existuje role IT architekta a popis IT architektury v rámci organizace?

26. **Kdy byla naposledy provedena analýza rizik? Máte zavedený systém řízení bezpečnosti informací? Pokud ano, podle jaké normy?**
Zahrnovala analýza rizik všechna primární aktiva organizace? Zahrnovala i podpůrná aktiva? Budou nám výstupy analýzy rizik poskytnuty? Existují výstupy z jiných interních projektů, které by usnadnily analytickou fázi (např. Data Quality, SAP implementace, IT Architektura, ISO 27000)?

27. **Jaké bezpečnostní politiky či směrnice ve vaší organizaci platí?**
Pro koho jsou závazné? Máte vytvořenu sestavu interních směrnic za účelem ochrany osobních údajů, kde jsou uloženy, jak jsou zpřístupněny zaměstnancům a třetím stranám?

28. **Jak je řízena bezpečnost informací ve vztahu k dodavatelům?**
Jsou běžně podepisována NDA neboli smlouvy o ochraně důvěrnosti sdělovaných informací? Je závazek zajistit bezpečnost informací běžnou součástí smluvních vztahů s dodavateli? Je prosazováno právo auditu u dodavatelů?

29. **Jak jsou vaši pracovníci seznamováni s požadavky na ochranu informací?**
Je bezpečnostní školení povinnou součástí nástupní procedury? Probíhá proškolování zaměstnanců pravidelně?

30. **Existuje evidence bezpečnostních incidentů?**
Byly v minulosti zjištěny a prošetřovány nějaké bezpečnostní incidenty? Neoprávněný přístup, ztráta dat apod.? Jak máte nastaven interní proces pro případ porušení ochrany dat? Existuje za tímto účelem interní směrnice?

31. **Má uživatel jeden uživatelský účet napříč celou organizací?**
Jak řešíte duplicitní uživatelská jména? Jak řešíte změny uživatelských jmen, například po změně příjmení?

32. **Jak silné ověření uživatelské identity používáte?**
Vynucujete kvalitu hesel technickými prostředky? Používáte vícefaktorovou autentizaci, nebo například kartu zaměstnance?

33. **Jaké komunikační nástroje využíváte interně a externě?**
Máte centrální mailový systém? Nebo má každá firma vlastní? Jaké další komunikační nástroje plošně využíváte? Jak často komunikujete se státní správou a jakým způsobem (datová schránka, písemně, e-mail)? Jak často jsou předmětem této komunikace elektronicky podepsané dokumenty?

34. **Probíhá ve vaší organizaci pravidelně bezpečnostní audit?**
Jaký? Jak často? Interní, nebo externí audit? Je oblast ochrany osobních údajů zahrnuta do interního, nebo externího auditu?

35. **Provádíte klasifikaci dat? Jak jsou osobní údaje zahrnuty do některého klasifikačního stupně?**
Označujete dokumenty systematicky jako citlivé nebo důvěrné? Například zahrnutí osobních údajů do klasifikačního stupně Citlivé se stanovením způsobů nakládání s informacemi uvedeného klasifikačního stupně.

36. **Aplikovali jste nějaká opatření dle zákona 181/2014 Sb., o kybernetické bezpečnosti? Pokud ano, jaká? A v jakém rozsahu?**
Například přijetí technických a organizačních opatření v rozsahu určeném pro provoz významného systému apod.

37. **Jakým způsobem jsou osobní údaje poskytnuté vaší společnosti zabezpečeny proti zneužití, ztrátě, zničení, nepovolenému odhalení nebo přístupu?**
Používáte pseudonymizační nebo jiné šifrovací techniky?

České znění NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Zdroj: zpracováno dle www.gdpr.cz