GDPR - pojmy

co je GDPR
GDPR (General Data Protection Regulation) je právní předpis, který přijala Evropská unie a tudíž je závazný pro všechny členské země EU, tudíž i pro Českou republiku. Jedná se o nařízení, což má vyšší právní váhu než častěji vydávané směrnice. Toto nařízení zpracovává legislativu o ochraně osobních údajů fyzických osob, které jsou definovány zákonem č. 101/2000 Sb., o ochraně osobních údajů.

termín
Norma vstoupila v platnost v květnu 2016. Zavedena musí být od 25. května 2018.

cíle normy
Nařízení je primárně zaměřeno na ochranu osobních údajů před zneužitím organizací podnikajících v kyberprostoru. Ale v konečném důsledku dopadá na všechny firmy a jednotlivce, kteří zpracovávají osobní údaje svých zaměstnanců, zákazníků, dodavatelů, žáků.

subjekt údajů
Fyzická osoba, které se osobní údaje týkají.

osobní údaj
Jsou to údaje, které sami o sobě, či ve vzájemné kombinaci, identifikují konkrétní osobu. Například u osoby Hrubohlavoun Kolohnátivý již jeho jméno a příjmení jsou, pro svou jedinečnost, dostatečnou identifikací. U jména Miloš Zeman tomu tak není. Ale pokud k tomuto jménu přidáme adresu Lány, je osoba opět plně identifikovaná.
Takže osobním údajem jsou jméno, adresa, identifikace (rodné číslo, DIČ a tak podobně), ale i další identifikace, jako jsou fyzický, psychický, duševní, genetický, ekonomický, kulturní nebo i jiný rys fyzické osoby.

citlivé osobní údaje
Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu než obecné údaje, které mohou subjekty těchto údajů poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jejich diskriminaci. Jedná se o údaje o rasovém či etnickém původu, politických názorech, náboženském, filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci. Je jasné, že ideálním řešením je žádné citlivé údaje nezpracovávat.

foto, audio, video
O tom, jak nejasný je prozatím GDPR svědčí příklad používání fotek. Například umístíte-li na firemní WEB fotografie svých žáků:

- 1) jak pracují v dílnách
- 2) jak pracují v dílnách s popiskem: studenti 1. ročníku obor truhlář
- 3) s popiskem: nejlepší studenti oboru truhlář za rok 2017/2018
- 4) s popiskem: Mácha a Erben, nejlepší studenti oboru truhlář za rok 2017/2018
- 5) s popiskem: Karel Mácha a Jaromír Erben, nejlepší studenti oboru truhlář za rok 2017/2018

Pak někteří tvrdí to, a druzí ono, že :

- ve všech případech potřebujete písemný souhlas a ten dokonce i dočasně omezený (např. na rok)
- jen v případě 5 potřebujete písemný souhlas
- nepotřebujete žádný písemný souhlas v žádné situaci

zpracování osobních údajů
Zpracování osobních údajů je jakákoli operace, kdy je s údaji nějak manipulováno: zaznamenávání, shromažďování, vyhledávání, nahlížení, přenos, ale i vymazání či zpřístupnění údajů. Nezáleží na tom, jestli je to strojově, či tzv. ručně.

správce osobních údajů
Správcem je subjekt jakékoliv právní formy, který za zpracování primárně odpovídá. Určuje účely a prostředky zpracování osobních údajů.

zpracovatel osobních údajů

Zpracovatel osobních údajů je najímán správcem a jeho jménem zpracovává osobní údaje. Vždycky ale provádí jen takové operace, kterými ho správce pověří nebo jaké vyplývají z jeho dosavadní činnosti. Může se tedy jednat například o externí účetní, která pro organizaci zpracovává osobní údaje jejich klientů.

DPO - pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (Data Protection Officer nebo zkráceně DPO) může být zaměstnancem organizace, či může úkoly plnit právnické, či fyzická osoba na základě smlouvy o poskytování služeb. Zákon určuje, kdo takového DPO musí mít:

- úřad (státní správa),
- firma, jejíž hlavní činnost vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů (např. personální agentury),
- firma, jejíž hlavní činnost spočívá v rozsáhlém zpracování údajů týkajících se rozsudků v trestních věcech a trestných činů.

právo subjektu údajů

Každý subjekt má podle nařízení GDPR právo požádat :

- na opravu nepřesných údajů,
- na vymazání svých osobních údajů ze strany správce, pokud: osobní údaje již nejsou potřebné pro účely, pro které byly zpracovány, subjekt údajů odvolal svůj souhlas se zpracováním, či údaje byly zpracovány protiprávně.
- na omezení zpracování v případech podobných jako v předchozím bodě, ale subjekt nepožaduje jejich výmaz

GDPR - interní systém

interní systém

Organizace by si měla sestavit svůj vlastní Interní systém GDPR. Ten bude obsahovat jednak počáteční ustanovení:

- identifikace organizace
- jmenovaný správce osobních údajů, který, dle výše uvedeného popisu sice být ustanoven nemusí, ale ustanoven být může, a vždy je lepší, existuje-li jeden člověk, u něhož se vše související s GDPR sbíhá
- seznam agend, u nichž se provádí zpracování osobních údajů (jedná se o agendy ať již softwarové, či jiné povahy). Pro příklad lze uvést určitě SW pro zpracování mezd a personalistiku, SW Fakturace, SW Pokladna atp. Dokonce i tak nevinně vyhlížející agendy, jako je například evidence majetku je třeba takto ošetřit, protože se v nich eviduje vazba mezi jednotlivými majetky a osobami, kterým je majetek svěřen. A ty osoby, i když jsou uvedeny jen jménem, jsou díky zúžení na skupinu zaměstnanců jednoznačně identifikovatelné.
- jmenný seznam pracovníků, kteří provádějí vlastní zpracování osobních údajů. Jedná se zejména o pracovníky, kteří pracují s výše definovanými evidencemi.
- kategorie subjektů, kterých se zpracování týká (například: zaměstnanci, studenti, fyzické osoby mezi obchodními partnery)
- jak je naplněno právo subjektu údajů, k přístupu ke svým údajům (například tím, že lze v SW vytisknout protokol o všech o něm evidovaných údajích)

No a pak bude interní systém obsahovat (třeba jen jako přílohu) informace o evidovaných údajích v jednotlivých agendách:

- 1) které osobní údaje zpracováváte
- 2) jakým způsobem (písemně, elektronicky, audio, video, foto atp.)
- 3) proč je zpracováváte, z jakého právního titulu
- 4) jak a kdo s nimi nakládá
- 5) jak jsou zabezpečeny proti zneužití
- 6) jak údaje archivujete,
- 7) komu a jak a za jakých okolností je poskytujete
- 8) jak je likvidujete

Takový protokol lze vytisknout v každém našem SW.

Součástí interního systému by mohl být i přehled toho, jak které dokumenty archivujete a z jakých důvodů.Například takto:

dokument	*let*	*co to ustanovuje*
účetní závěrky a výroční zprávy	10	563/1991 Sb., o účetnictví – § 31 a § 32
účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh, přehledy	5	
účetní záznamy, kterými účetní jednotky dokládají vedení účetnictví (daňové doklady aj.)	5	
doklady od osob povinných k dani z přidané hodnoty	10	235/2004 Sb., o dani z přidané hodnoty – § 35 a § 35a
stejnopisy evidenčních listů	3	582/1991 Sb., o organizaci a provádění sociálního zabezpečení – § 35a (4) a § 37 (1)
mzdové listy	30	
mzdové listy poživatelů starobního důchodu	10	
údaje potřebné pro stanovení a odvod pojistného	10	589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti – § 22c

DPIA

Článek 35 nařízení GDPR) zmiňuje tzv. Data Protection Impact Assessment (DPIA). Má to být „nástroj“ (posouzení vlivu na ochranu osobních údajů), který má být nápomocen uvést interní pravidla organizace do souladu s GDPR. Ve skutečnosti jde o elaborát, o takové slohové cvičení, čím rozsáhlejší, tím lepší. Vizuálně hezky uspořádané a zabalené ve zlatých deskách.

DPIA se povinně provádí:

- při systematickém a rozsáhlém vyhodnocování osobních aspektů týkajících se fyzických osob, které je založené na automatizovaném zpracování,
- při rozsáhlém zpracování citlivých osobních údajů,
- při rozsáhlém systematickém monitorování veřejně přístupných prostorů,
- další případy, kdy je provedení DPIA povinné, může určit dozorový orgán.

DPIA musí obsahovat alespoň:

- popis zamýšleného zpracování, účel a oprávněné zájmy,
- posouzení nezbytnosti a přiměřenosti zpracování,
- posouzení rizik pro práva a svobody subjektů údajů,
- plánovaná opatření k odstranění nebo snížení těchto rizik.

GDPR a software

V nových verzích, které s právě teď dokončují a budou uvolněny v polovině měsíce května, bude nová funkce ***Obsluha - O počítači - GDPR***. A v ní budou možné:

- vytisknout protokol o v SW evidovaných osobních údajích (ten by měl být přiložen k internímu systému)
- vymazat osobní údaje, které jsou evidovány, ale nejsou pro vlastní výkon nutné
- protokolární výmaz osobních údajů subjektu, který si nepřeje, aby o něm tyto informace byly evidovány
- vytisknout protokol pro zaznamenání skutečnosti, kdy měla třetí osoba přístup k osobním údajům (například fyzická přítomnost pracovníka dodavatelské firmy SW u počítače, vzdálená správa k SW, odeslání dat SW firmě pro řešení mimořádných situací, atp.)
- protokol o principech archivovaní dat s osobními údaji
- vzor žádanky k souhlasu s evidováním osobních údajů
- protokol o aktuálním stavu evidovaných osobních údajů konkrétního subjektu
- protokol o vývoji evidovaných osobních údajů konkrétního subjektu

závěr

Možná, že majitelům sociálních sítí nařízení GDPR skutečně ztíží jejich základní obchodní praktiky, tedy prodávání dat svých klientů. To by bylo dobré. Mám ale pocit, že půjde zase o nafouknutou bublinu. V začátku se na tom přiživí několik firem poskytujících školení, poradenství, či sestavení interního sytému GDPR.
Velice silně mi to připomíná HACCP, který svého času také poutal velikou pozornost a sliboval nám, že nás zachrání od všeho zlého. A po jeho zavedení už po něm vlastně ani pes neštěkl. A přes jeho zavedení následně umřelo přes 50 lidí na otravu metanolem, což tedy byla čistě kriminální záležitost. A potravinářské firmy do stejnojmenných výrobků, do kterých v zahraničí dávají maso, u nás dávají kůžičky, separáty a podobné hnusy, nejspíše plně v souladu s HACCP. Což je vlastně také kriminální záležitost.
Nicméně byrokracii musí být učiněno zadost. Takže je dobré si vytvořit Interní systém GDPR (viz připojený vzor). K němu přiložit protokoly o evidovaných osobních údajích, které si vytisknete v jednotlivých SW. A pak, pokud s daty bude někdo, kdo není organizací k tomu určen, vytisknout v SW a vyplnit protokol o mimořádném zpracování (odeslání dat, osobní návštěva třetí osoby u PC, vzdálená správa).
A pokud si to nějaký subjekt bude přát, vytisknout mu protokol o vámi evidovaných jeho údajích, případně je na jeho vyžádání vymazat.
Budete-li zpracovávat osobní údaje nad rámec zákonných povinností, měli byste si vyžádat souhlas subjektu(ů).
Všechny tyto dokumenty pak založte do společného interního systému GDPR.