Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Podpora II
průvodce světem práce | informace zaměstnancům

GDPR. Obecné nařízení o ochraně osobních údajů.

Expertní skupina pro poradenství

Ing. Viktor Chačaturov
Ing. Eugenie Bouškova
Jarmila Dvořáková

Obsah

1 Úvod

GDPR, tuto zkratku v poslední době slýcháme stále častěji. Co to ale znamená a je potřeba kvůli GDPR něco měnit či zavádět nové procesy? Na tyto a další otázky bychom rádi v této studii poskytli odpovědi.

Úvodem je nutné osvětlit, že GDPR je nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, oficiálně označované i jako obecné nařízení o ochraně osobních údajů. V angličtině jde potom o „General Data Protection Regulation“, z čehož pochází ona populární zkratka GDPR.

GDPR bylo přijato v dubnu 2016, ale platit začíná až od 25. května 2018 a mělo by přinést dosud největší revoluci v ochraně osobních údajů s cílem hájit práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji. GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů.

Ve studii se zaměříme na problematiku GDPR i v souvislosti s přístupem českých firem, jejich aktuální informovaností a co nezanedbat při přípravách.

GDPR je třeba nepodceňovat, ale je nutné se dokázat zorientovat mezi záplavou informací od nejrůznějších poradenských firem, které budou chtít pod hrozbou sankcí na celé integraci vydělat.

V neposlední řadě bychom rádi shrnuli zásadní změny, které GDPR přinese.

Evropská unie má tímto nařízením za cíl nastolit jednotnou úroveň ochrany fyzických osob v celé unii a tím i zamezit rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu a hospodářským subjektům poskytnout jistotu a transparentnost.

Toto nařízení reflektuje vývoj technologií i práva, díky čemuž přináší nová práva subjektům údajů (fyzické osoby) a nové povinnosti správcům a zpracovatelům, nicméně základní pojmy a principy se nemění.

2 Obecné nařízení

Jak již bylo řečeno v úvodu, obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru, které bude od 25. května 2018 přímo stanovovat pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak Obecné nařízení od 25. května 2018 nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů.

Charakteristická pro Obecné nařízení je jeho univerzální použitelnost ve všech státech Evropské unie (a Islandu, Norska a Lichtenštejnska) a tudíž i sjednocující účinek, jelikož jednotná pravidla pro zpracování osobních údajů budou platit v každém státě EU a třech vyjmenovaných. Právě zajištění větší jednotnosti pravidel ochrany osobních údajů bylo i jedním z cílů přijetí Obecného nařízení.

Celý název je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).

2.1 Proč vzniklo?

Současný právní rámec, založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současné době, zejména pokud jde o prostředky, které jsou ke zpracování využívány a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami lety (např. v oblasti profilování, automatizace zpracování osobních údajů atd.). Zároveň v jednotlivých zemích Evropské unie nebyla Směrnicí 95/46/ES dosažena požadovaná míra sjednocení právní úpravy, což správcům působícím ve více zemích činilo problémy.

Cílem Obecného nařízení je přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektu údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu Obecného nařízení a dozoru jednotlivými dozorovými úřady.

2.1.1 Datum použitelnosti

V článku 99 Obecného nařízení se mluví o tzv. použitelnosti. Použitelnost znamená jinými slovy účinnost Obecného nařízení, tedy datum, od kdy se Obecné nařízení začne používat neboli aplikovat. Nyní běží pro správce a zpracovatele dvouletá lhůta, aby uvedli ke dni použitelnosti Obecného nařízení (25. května 2018) svá zpracování osobních údajů do souladu s Obecným nařízením.

2.1.2 Zákon o ochraně osobních údajů, co s ním bude?

Jelikož Obecné nařízení stanovuje práva a povinnosti při zpracování osobních údajů, v tomto rozsahu zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých

zákonů nahrazuje. Práva a povinnosti v současném zákoně o ochraně osobních údajů budou nahrazena právy a povinnostmi vyplývajícími z Obecného nařízení. Zákon o ochraně osobních údajů po jeho novele bude již upravovat jen některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou Obecným nařízením upraveny nebo které Obecné nařízení umožňuje upravit na vnitrostátní úrovni. U některých aspektů dokonce Obecné nařízení předpokládá vnitrostátní úpravu. Mezi ně patří například aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby,

2.2 Nové přístupy a povinnosti

Obecné nařízení je založeno na dvou nových přístupech, kterými jsou princip odpovědnosti správce a přístup založený na riziku.

Princip odpovědnosti znamená odpovědnost správce za dodržení zásad zpracování a zároveň správce musí být schopen tento soulad doložit. K dokládání souladu budou mimo jiné sloužit kodexy, osvědčení či certifikace, případně záznamy o činnostech zpracování.

Kodexy mají správcům, zejména na sektorové úrovni, sloužit jako vodítko správné praxe při zpracování osobních údajů právě s ohledem na specifičnost daného sektoru (např. bankovnictví, telekomunikace, internetové obchody, zdravotnictví). Kodexy budou moci vydávat sdružení či jiné subjekty zastupující různé kategorie správců nebo zpracovatelů přičemž návrh kodexu musí být předložen Úřadu pro ochranu osobních údajů. Osvědčení má sloužit k prokázání souladu zpracování s Obecným nařízením. Osvědčení bude moci vydávat k tomu akreditovaný subjekt. V současné době probíhají práce na stanovení formy a postupů pro akreditaci a pro vydávání osvědčení ze strany akreditovaných subjektů. Záznamy o činnostech zpracování obsahují informace o prováděném zpracování, což správci umožní lehčí orientaci ohledně zpracování, která provádí.

Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. V užším slova smyslu lze hovořit o přístupu založeném na riziku jako o aplikaci některých povinností pouze v případě, kdy zpracování osobních údajů či porušení zabezpečení představuje riziko či vysoké riziko pro práva a svobody fyzické osoby.

Co se týče povinností, tak je třeba zdůraznit, že základní zásady, principy a klíčové instrumenty zůstávají de facto neměnné (např. nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.). Obecné nařízení na těchto základech přináší nástavbu spočívající v dodatečných nových povinnostech, které pro české správce budou nové.

Jde zejména o tyto nové povinnosti:

- povinnost vést záznamy o činnostech zpracování

- posouzení vlivu na ochranu osobních údajů
- předchozí konzultace
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů
- ustavení pověřence pro ochranu osobních údajů

2.3 Hlavní pojmy

Definice pojmů jsou uvedeny v článku 4 odst. 1 Obecného nařízení, nicméně několik zásadních pojmů bychom rádi více rozvedli.

Zpracování osobních údajů

Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracování ve smyslu Obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování.

Pojem zpracování má stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Osobní údaj

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Pojem osobní údaj nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů de facto změněn.

Subjekt údajů

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou

být pouze ve vztahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

Definice s totožným obsahem jako v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Správce

Správcem je subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Správcem může být jakýkoli subjekt. Správcem může být i fyzická osoba, pokud zpracovává osobní údaje způsobem, že tento způsob již vylučuje uplatnění výjimky osobní či domácí činnosti.

Pojem správce nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů změněn.

Zpracovatel

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Je nutné poznamenat, že zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají (např. je správcem při zpracování osobních údajů vlastních zaměstnanců).

Stejně jako u správce, ani u zpracovatele není určující jeho právní forma.

Pojem zpracovatel nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů změněn.

Obecného nařízení a dozoru jednotlivými dozorovými úřady.

2.3.1 Citlivé osobní údaje

Některé osobní údaje jsou takového charakteru, že mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Z tohoto důvodu je taxativně (úplným výčtem) vymezena skupina údajů, které jsou považovány vůči subjektu údajů za citlivé a jimž je poskytnuta ještě zvýšená ochrana při

jejich zpracování. Zvýšená ochrana se projevuje zejména ve stanovených zvláštních právních důvodech, na základě kterých je lze zpracovávat, vázanost některých institutů na jejich zpracování, jako hlavní činnosti (např. posouzení vlivu, ustavení pověřence), důraz na jejich zvýšené zabezpečení.

Citlivými osobními údaji mohou být takové, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.

Jejich výčet je téměř totožný s výčtem citlivých údajů v zákoně č. 101/2000 Sb., o ochraně osobních údajů.

2.4 Zásady a právní důvody zpracování

Zásady lze ve stručnosti shrnout na zásady:

- zákonnost, korektnost, transparentnost - správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,
- omezení účelu - osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
- minimalizace údajů- osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
- přesnost - osobní údaje musí být přesné,
- omezení uložení- osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
- integrita a důvěrnost - technické a organizační zabezpečení osobních údajů.

Dodržování těchto zásad, je pro správce zásadní, nejen z toho důvodu, že to jsou de facto zároveň povinnosti, ale i proto, že v článku 5 odst. 2 Obecného nařízení je stanovena odpovědnost správce za jejich dodržování a zároveň povinnost správce být schopen dodržování těchto zásad (povinností) doložit. Jde o vyjádření tzv. principu odpovědnosti správce. K prokazování souladu s těmito zásadami budou sloužit záznamy o činnostech zpracování a též kodexy a osvědčení.

Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat. Právní důvody tak jsou nezbytným předpokladem k legálnímu zpracování.

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

- subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

2.5 Práva subjektů údajů

Práva subjektu údajů jsou důležitým prvkem ochrany osobních údajů jako celku, jelikož subjekt údajů je často ve slabším postavení než správce a tudíž vybalancovávají vztah mezi ním a správcem.

Subjekt údajů má právo na to být informován o zpracování jeho osobních údajů. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. Úplný výčet informací, které správce poskytuje při shromažďování osobních údajů, lze nalézt v článcích 13 a 14 Obecného nařízení.

Mezi další práva subjektu údajů patří právo na přístup k osobním údajům, právo opravu, resp. doplnění, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku a právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování.

Přístupem k osobním údajům se rozumí právo subjektu údajů získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Právo na výmaz (být zapomenut) představuje v Obecném nařízení jinými slovy vyjádřenou povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna z podmínek, uvedených v Obecném nařízení

Právo na přenositelnost je zcela nové právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Právě uchovávání strukturovaných dat je jedno z velkých IT otázek pro firmy všech velikostí. V dnešní době nikdo téměř žádná

z malých a středních firem data ve strukturované podobě neukládá a je zapotřebí tuto otázku začít aktivně řešit.

S právem subjektu vzniká i otázka ohledně možnosti zneužití tohoto práva. O zneužití práva subjektem údajů lze hovořit zejména tehdy, pokud se žádosti opakují a jsou zjevně nedůvodné či nepřiměřené. V takovém případě může správce uložit přiměřený poplatek nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost dokládá správce.

2.6 Bezpečnost osobních údajů

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením.

Jedním z prvků zabezpečení osobních údajů je např. jejich **pseudonymizace** nebo **šifrování**.

Pseudonymizace osobních údajů je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Klasickým příkladem pseudonymizace jsou údaje kódované pomocí klíče. Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně. Nicméně pseudonymizované osobní údaje nejsou anonymizovanými údaji, proto se na ně vztahuje GDPR.

Tyto prvky však nejsou povinné. Jejich dobrovolné nasazení však správci může přinést i zproštění např. povinnosti ohlásit případ porušení zabezpečení osobních údajů subjektu údajů.

Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu (Úřadu pro ochranu osobních údajů), ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Právě používání pseudonymizace či šifrování může případné riziko zcela eliminovat. Vždy je však nutné míru rizika posoudit, a to i v případě, že byla použita pseudonymizace či šifrování.

Při určování rizika porušení zabezpečení bude nutné vycházet zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovnictví).

2.7 Pověřenec pro ochranu osobních údajů (DPO)

Obecné nařízení pracuje s pojmem tzv. pověřence. Data Protection Officer neboli DPO (česky Pověřenec pro ochranu osobních údajů) je nově vytvořenou pracovní pozicí podle GDPR. Hlavním úkolem DPO bude monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat.

Pověřence je třeba jmenovat, pokud:

- zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,
- hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
- hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech.

Musí mít svého pověřence každá obec?

Vzhledem k tomu, že obec lze považovat za orgán veřejné moci, resp. veřejný subjekt ve smyslu článku 37 odst. 1 písm. a) Obecného nařízení, formálně na ní dopadá povinnost jmenovat pověřence. Obecné nařízení nicméně umožňuje pro více správců, kteří jsou orgánem veřejné moci či veřejným subjektem, jmenovat jednoho pověřence.

Hlavní „vlastnosti“ pověřence

- Pověřenec musí být osoba disponující profesními kvalitami a odbornou znalostí práva a praxe v oblasti ochrany osobních údajů a musí dostatečně ovládat Obecné nařízení.
- Aktuálně není vyžadována žádná speciální certifikace pro osobu pověřence
- Funkci pověřence může vykonávat i právnická osoba,

Mezi hlavní úkoly pověřence patří především poskytování informací a poradenství správci či zpracovateli, včetně zaměstnancům, kteří se na zpracování podílejí. Pověřenec dále monitoruje soulad zpracování s Obecným nařízením a dalšími předpisy. Pověřenec poskytuje na vyžádání poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů. Nedílnou součástí výkonu funkce pověřence je dále spolupráce s Úřadem pro ochranu osobních údajů a působení jako kontaktní místo.

2.8 Sankce a pokuty

Ukládání správních pokut je nastaveno tak, aby bylo účinné, přiměřené, ale zároveň odrazující. Je potřeba říci jednu podstatnou věc, a to tu, že pokuta nemusí být nutně udělena za každé porušení Obecného nařízení, ale správce může být například nejprve upozorněn, že

zamýšlené operace zpracování pravděpodobně porušují Obecné nařízení, nebo může být správci, jehož operace zpracování porušily Obecné nařízení, uděleno napomenutí nebo mu může být nařízeno, aby žádosti subjektu údajů vyhověl.

Pokud by však vznikla skutečnost, že dojde k udělení pokuty, bude její výše následující. Pokuty jsou rozděleny do dvou skupin dle porušení, jakého se správce dopustil.

Pokutu lze udělit:

- buď do výše 10 000 000 EUR (nebo až do 2% celkového ročního celosvětového obratu, jde-li o podnik) nebo
- do výše 20 000 000 EUR (nebo až do 4% celkového ročního celosvětového obratu, jde-li o podnik)

Rozdělení do dvou skupin odráží důležitost porušených povinností, kdy ve skupině s vyšší sazbou jsou povinnosti, u jejichž porušení je očekávána vyšší intenzita zásahu do práva na ochranu osobních údajů, které Obecné nařízení zajišťuje. Do nižší sazby spadá např. porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, zatímco do vyšší sazby jsou například zahrnuta porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů.

Obecné nařízení však určuje také polehčující okolnosti při ukládání pokut. Ty jsou uvedeny v čl. 83 odst. 2 písm. a) až k). Brána v úvahu bude zejména povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu a účelu zpracování, kategorií údajů a počtu dotčených subjektů údajů, zda se jednalo o úmyslné či nedbalostní porušení, kroky podniknuté správcem a spolupráce s Úřadem pro ochranu osobních údajů atd.

V případě, že vznikla subjektu údajů hmotná či nehmotná újma v důsledku porušení Obecného nařízení ze strany správce či zpracovatele, má právo na úhradu újmy. Nejčastěji to bude znamenat obrátit se přímo s žádostí o náhradu na správce či zpracovatele, a pokud ten nebude dobrovolně plnit, bude se subjekt údajů muset obrátit na soud.

2.9 Nejčastější omyly o GDPR

Označování obecného nařízení za revoluci v právech subjektu údajů a v povinnostech správců

Označování obecného nařízení jako právního aktu EU spouštějícího revoluci mělo svůj smysl v době jeho přípravy a oficiálního projednávání, jež započalo v roce 2012 a skončilo v roce 2016. Silné výrazy upoutávaly pozornost a do určité míry zpřehledňovaly objemný text. Po skončení vyjednávání je na místě zůstat v mezích přijaté úpravy a používat přiměřené hodnotící výrazy, a to i tam, kde původní cíle byly ambicióznější.

Skutečnost je taková, že jedním ze základních znaků ochrany osobních údajů podle obecného nařízení je kontinuita - nařízení navazuje ve sledovaných cílech a obsahových

zásadách zpracování a ochrany osobních údajů na směrnici 95/46/ES a sleduje překonání stávající roztříštěnosti v provádění ochrany osobních údajů v Unii soudržným a jednotným uplatňováním pravidel ochrany osobních údajů. Oproti současné obecné formulaci povinností při zabezpečení zpracování v § 13 zákona o ochraně osobních údajů jsou v obecném nařízení akcentovány „technické prostředky" a jmenovitě určené technologie - pseudonymizace a šifrování, obnova dostupnosti, pravidelné testování a hodnocení účinnosti zavedených opatření. Podstatné je i to, že ve všech povinnostech správců a zpracovatelů se promítají konstrukční zásady záměrné a standardní ochrany a přístupu založeného na riziku, které se uplatňují rovněž současně - např. v povinnosti posuzovat vliv jednotlivých zpracování na ochranu osobních údajů.

Rozšiřuje se definice osobního údaje

Nejčastěji se toto tvrzení objevuje v podobě, že osobními údaji dosud jsou pouze údaje identifikační, popř. přímo identifikující subjekt údajů. Někdy se změna dokládá na rozsudku Soudního dvora Evropské unie, v němž Soudní dvůr konstatoval, že dynamická IP adresa představuje osobní údaj ve smyslu směrnice 95/46/ES. Právě tento rozsudek však je dokladem toho, že osobní údaje nejsou omezeny na údaje přímo identifikující nějaký subjekt údajů ani dnes. Obecné nařízení definuje osobní údaj jako veškeré informace o identifikované nebo identifikovatelné fyzické osobě; zákon o ochraně osobních údajů jako jakoukoliv informaci týkající se určeného nebo určitelného subjektu údajů.

Právní definice osobních údajů nemůže být výčtová, protože počet druhů osobních údajů je přirozeně neuzavřený a osobní údaje vznikají neomezeně nejen jako hodnoty vztažené k novým a novým konkrétním subjektům údajů, ale také s novými technologiemi zpracování osobních údajů, jako jsou např. právě internetové technologie. IP adresa je osobním údajem vždy, když se vztahuje k určené nebo určitelné osobě, ne od doby vynesení rozsudku Soudního dvora EU, ale od prvního použití IP adresy v provozu. GDPR již také nemá podmínku systematičnosti zpracování osobních údajů.

Je lepší mít paušální souhlas subjektu údajů, než se zabývat jednotlivými zákonnými důvody

Takové doporučení vychází z nepochopení a nedocenění souhlasu subjektu údajů. Souhlas fyzické osoby, jejíž osobní údaje hodlá správce zpracovávat, je klíčovým institutem evropského modelu ochrany osobních údajů od samých počátků, nelze jej však uplatňovat tam, kde platí jiné právní tituly zpracování (s nimiž nelze souhlas zaměňovat), např. sjednávání a plnění smluv, plnění povinností či ochrana práv a právem chráněných zájmů. V obecném nařízení je udělení souhlasu subjektu údajů se zpracováním pro jeden či více konkrétních účelů jednou ze šesti právních podmínek zákonnosti zpracování (jeho právním základem) a nařízení výslovně upravuje podmínky jeho získání. Ve srovnání se současným stavem v České republice přináší obecné nařízení formální změnu v tom, že souhlas je rovnocenný pěti dalším právním důvodům/titulům, zatímco dnes je alespoň dle textu zákona důvodem/titulem základním a všechny ostatní jsou formálně zakotveny jako výjimky, na něž se zpravidla hledí tak, že mají být vykládány co nejúžeji. Optické srovnání významu uznávaných právních důvodů neznamená snížení váhy souhlasu dotčeného subjektu údajů; jedním ze základních projevů toho je, že souhlas se zpracováním se skutečně uplatní jen tam, kde mohou být

naplněny jeho základní znaky, totiž svobodnost a informovanost. Souhlas může subjekt údajů kdykoli odvolat.

Případné paušální získávání souhlasu subjektu údajů pro veškerá zpracování, která správce bude provádět k různým účelům, by tak bylo v rozporu hned s několika ustanoveními obecného nařízení - počínaje povinností shromažďovat osobní údaje pro určité, výslovně vyjádřené a legitimní účely, přes zásadu transparentnosti vůči subjektu údajů a konče svobodností souhlasu ve vztahu k smluvním vztahům správce a subjektu údajů.

Povinné šifrování

Obecné nařízení neukládá povinnost použít pro zabezpečení zpracování některé specifické opatření.

Naopak, při stanovení povinnosti správce a zpracovatele zabezpečit osobní údaje, se obecné nařízení výslovně dovolává ohledu na stav techniky, náklady na přijetí a provedení jednotlivých technických a organizačních opatření k zabezpečení osobních údajů, povaze, rozsahu, kontextu a účelům samotného zpracování a také k pravděpodobným rizikům pro práva a svobody, jež s sebou zpracování nese. Vlastní povinnost pak zahrnuje zavedení vhodných technických a organizačních opatření a začlenění do zpracování nezbytných záruk, a to jak v době určení prostředků pro zpracování, tak v době vlastního zpracování. Šifrování je uvedeno jako jedno z vhodných opatření („případně včetně /…/ šifrování osobních údajů“). Při posuzování úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům.

Každý správce musí mít pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je jedním z nových nástrojů ochrany osobních údajů, které obecné nařízení zavádí. Správce je povinen jmenovat pověřence, ovšem pouze za splnění jedné ze tří podmínek, které jsme si uvedli již v předchozí kapitole. V jiných případech správce ani zpracovatel povinnost jmenovat pověřence pro ochranu osobních údajů nemají; jinými slovy, správci provádějící jiná zpracování pověřence pro ochranu osobních údajů jmenovat nemusí.

3 Změny, které GDPR přinese

Pojďme si nyní shrnout, co vlastně to „slavné“ GDPR přinese? Jednak jsou to mnohem silnější pravidla ochrany osobních údajů pro občany EU a také větší kontrolu těchto údajů pro občany samotné. Na druhou stranu i pro podniky přináší GDPR pozitivní změnu, která spočívá především ve sjednocení pravidel pro všechny společnosti, které v Unii působí.

GDPR je především o důvěře. Bohužel nedůvěra v současnou ochranu osobních údajů brzdila digitální ekonomiku a tím pádem mohla brzdit i rozvoj samotných firem.

Největším strašákem se pro mnohé stane oznamovací povinnost v případě narušení bezpečnosti údajů. Už by se tedy nemělo stávat, že se o kauzách masivních úniků osobních dat dozvídáme až s odstupem několika let, jako se stalo např. v kauze společnosti Yahoo. Nově bude muset zpracovatel ohlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl. V některých případech bude muset také informovat osoby a subjekty, kterých se únik týkal.

3.1 Zavádění GDPR do českých firem

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.

Stále ještě se objevují názory řady organizací, že se jich 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.

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.

Jedním z hlavních mýtů GDPR je ten, že se vše točí kolem IT bezpečnosti. Samotný text GDPR nařízení obsahuje 778 řádků a pouze 26 z nich se přímo IT bezpečnosti týká. 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.

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.

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.

Několik tipů pro malé a střední podniky, které je dobré dodržovat, a nemusíte se ničeho bát.

- Komunikujte jednoduše. Až po občanech budete údaje vyžadovat, sdělte jim, kdo jste. Uveďte, proč údaje zpracováváte, jak dlouho je budete uchovávat a kdo je získá.
- Obstarejte si od nich jednoznačný souhlas se zpracováním údajů. Shromažďujete údaje od dětí ze sociálních sítí? Ověřte si věkovou hranici, kdy potřebujete souhlas rodičů.
- Umožněte lidem, aby měli ke svým údajům přístup a mohli je poskytnout jiné společnosti.
- Hrozí-li lidem v souvislosti s narušením bezpečnosti údajů vážné riziko, informujte je o tom.
- Dejte lidem „právo být zapomenut“. Požádají-li o to, jejich osobní údaje vymažte – avšak pouze v případě, že to nenaruší svobodu projevu či možnosti zkoumání.
- Pokud při zpracovávání žádostí vedoucích k uzavření právně závazné smlouvy, např. v případě půjček, využíváte profilování, musíte:
    - o tom své zákazníky informovat;
    - v případě, že bude žádost zamítnuta, zajistit, aby celý postup kontroloval člověk, nikoli přístroj;
    - dát žadateli právo rozhodnutí napadnout.
- Dejte lidem právo nepřistoupit na přímý marketing, který využívá jejich údaje.
- Na informace o zdraví, rase, sexuální orientaci a náboženském a politickém přesvědčení uplatňujte nadstandardní ochranu.
- Přenášíte-li údaje do zemí neprověřených orgány EU, přijměte příslušná právní opatření.

3.1.1 Aktuální připravenost českých firem

Růst zájmu řešení pro správu a přístupu k dokumentům na základě lokálního průzkumu:

Acronis, celosvětový lídr v řešeních ochrany dat nové generace, představil výsledky svého lokálního průzkumu v oblasti sdílení a přístupu k podnikovým souborům, který provedl letos mezi českými prodejními partnery. Z průzkumu vyplývá, že sdílení a přístup k podnikovým datům patří k největším výzvám českých SMB společností v oblasti ochrany dat. Nějaké řešení pro sdílení a synchronizaci souborů zvažuje letos nasadit téměř polovina podniků.

Klíčová zjištění z lokálního průzkumu:

- České SMB firmy a organizace v oblasti sdílení a přístupu k podnikovým dokumentům nejčastěji řeší roztříštěnost informací (61 %), nízkou úroveň zabezpečení (56 %) a ukládání pracovních souborů do externích úložišť typu Dropbox (33 %);
- Jejich uživatelé nejčastěji z mobilních zařízení přistupují k obchodním dokumentům (67 %), k marketingovým informacím (39 %) a k servisním případům (38 %);
- Již 44 % podniků zvažuje v letošním roce nasazení specializovaného řešení pro sdílení a synchronizaci souborů (oproti 18 % v roce 2016).

Hlavním motivem nasazení řešení pro sdílení a přístup k podnikovým dokumentům byla vždy rozvíjející se pracovním mobilita. Nyní se ale stále více zákazníků zajímá o řešení přístupu k souborům i souvislosti s blížícím se termínem platnosti směrnice GDPR, protože umožňují nastavit takovou přístupovou politiku, která zabraňuje případům neoprávněného úniku citlivých osobních dat.

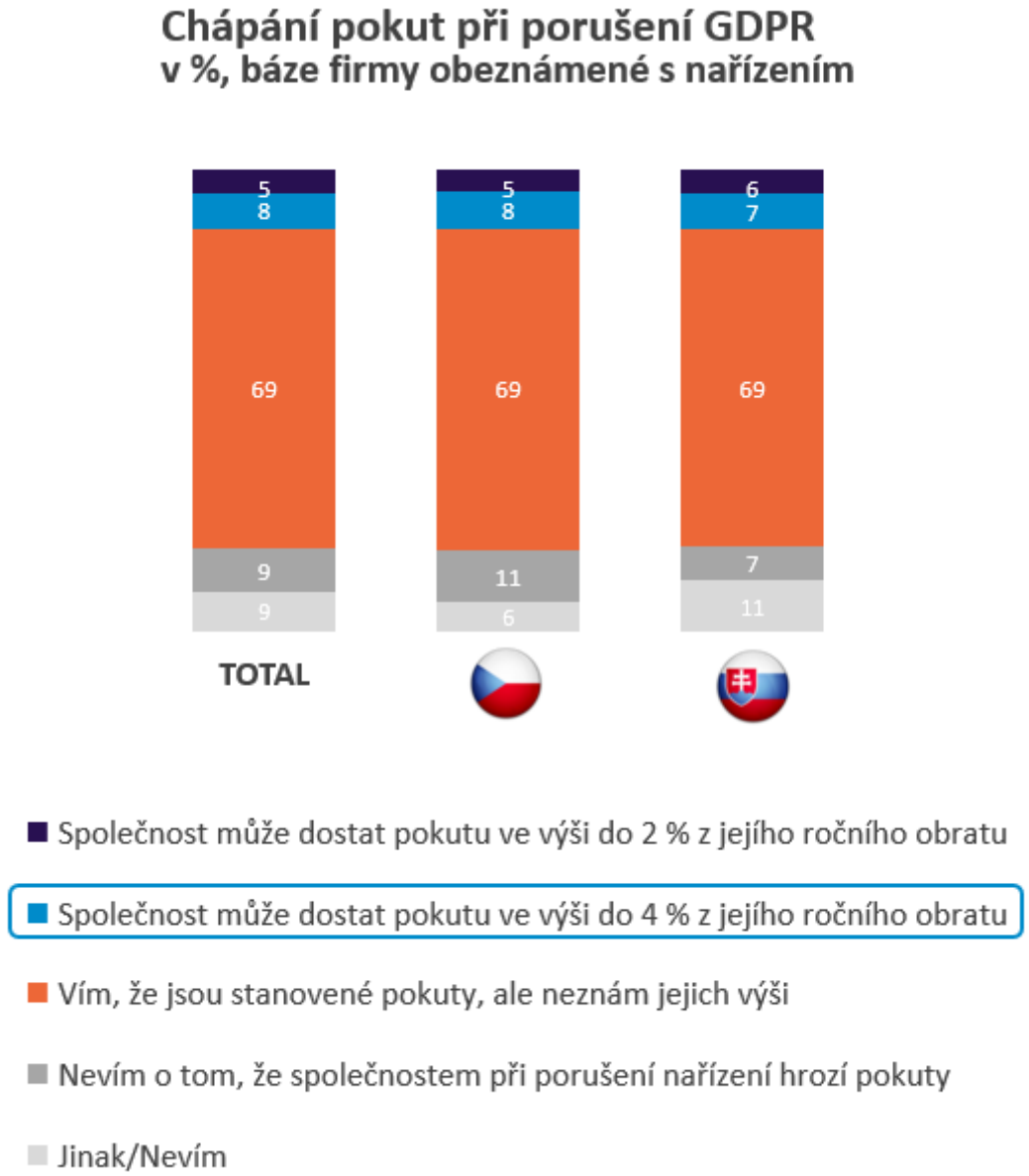
Možné pokuty GDPR zná jen jedna z deseti firem

Většina firem je s novou regulací GDPR obeznámena, finanční dopady si však neuvědomují.

Na GDPR by se měly připravit všechny subjekty, které jakýmkoliv způsobem zpracovávají osobní údaje fyzických osob. Týká se to tedy nejen zadavatelů, kteří shromažďují kontakty na zákazníky, ale i vydavatelů, kteří pracují se svou předplatitelskou bází. Aktuální výzkum společností Trend Micro a WMware, který vznikl ve spolupráci s výzkumnou agenturou Ipsos, však ukazuje, že české firmy jsou sice s GDPR většinou již obeznámeny, zatím si ale příliš neuvědomují možné dopady, které je za narušení bezpečnosti osobních údajů mohou potkat.

Podcení-li firmy totiž svou přípravu, může je za narušení bezpečnosti osobních údajů postihnout pokuta až ve výši 20 milionů eur nebo 4 % z celkového obratu za uplynulý finanční rok. Výše pokuty se přitom bude odvíjet nejen od míry škody, ale také od kroků, které firmy pro ochranu osobních údajů učinily. Téměř 8 z 10 firem o GDPR ví, přičemž jeho znalost je o něco vyšší na Slovensku (89 %) než v České republice (69 %). Potenciální výši pokut si však

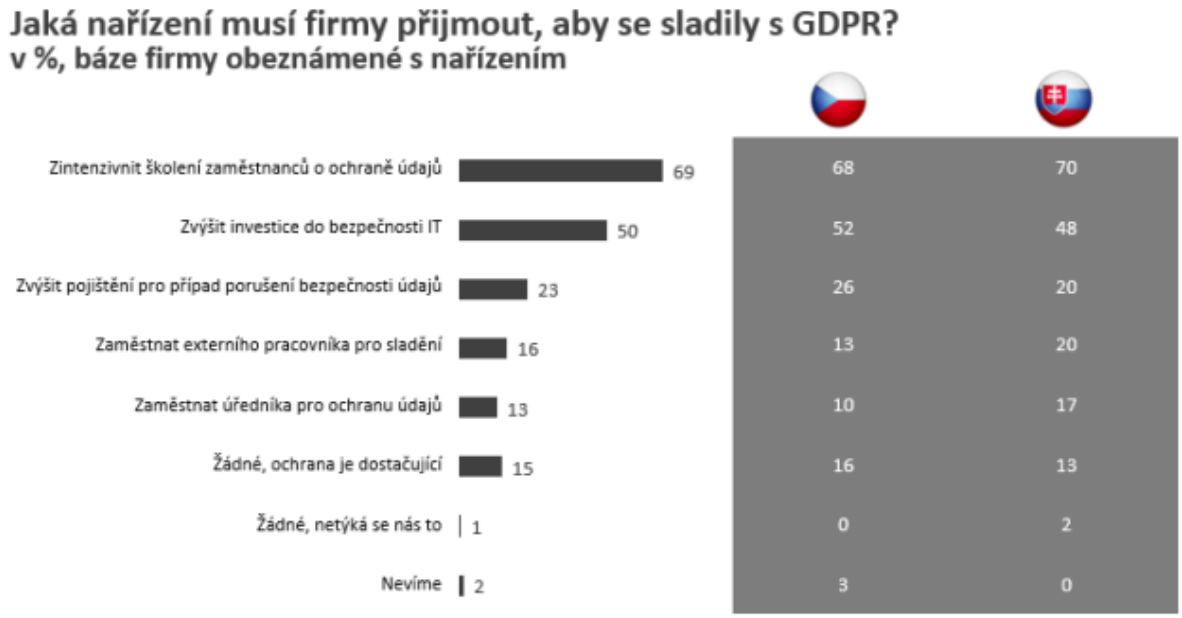
uvědomuje jen jedna z 10 obeznámených firem. O možnosti pokuty ve výši 4 % z obratu ví pouze 8 % ze 151 dotázaných českých a slovenských firem. Respondenty přitom byly osoby, které mají na starosti osobní údaje a jejich bezpečnost ve firmách s více než 100 zaměstnanci.



Nové nařízení se soustředí na otázku otevřenosti problematiky ochrany údajů – každý případ narušení bezpečnosti, únik dat či neoprávněná manipulace s nimi musí být obeznámen klientům firmy a informaci o takové skutečnosti musí obdržet příslušný regulátor. To má ukončit dosavadní praxi, kdy se narušení bezpečnosti před veřejností utajovalo, což vedlo k všeobecnému ignorování tohoto problému jako údajně málo důležitého a nevyžadujícího jakékoliv investice. I z tohoto důvodu je jednou z novinek nařízení povinnost zavést odpovídající bezpečností technologie.

Většina českých firem (82 %) se domnívá, že má nejvyšší možnou míru ochrany proti narušení bezpečnosti údajů už nyní. Více než pětina z nich (22 %) si je tím jista, 60 % je o tom téměř přesvědčena. Zároveň však jako největší hrozbu pro bezpečnost dat uvádějí firmy na prvním místě náhodnou ztrátu údajů zaměstnanci (29 %), možnost kyberzločinu (28 %) a úmyslné odcizení údajů zaměstnanci (23 %).

Z tohoto důvodů je kromě bezpečnostní technologie potřeba investovat i do školení zaměstnanců. Firma musí investovat do technologií, ale ta bohužel nezamezí tomu, aby si zaměstnanec poslal údaje z pracovního počítače na soukromý e-mail s tím, že s nimi bude pracovat doma. Zintenzivnit školení zaměstnanců o ochraně dat plánuje kvůli GDPR 69 % firem. Polovina firem (50 %) hodlá také navýšit své investice do bezpečnosti IT nebo zvyšovat pojištění pro případ narušení bezpečnosti (23 %).



Právo být zapomenut

Nařízení GDPR také přiznává fyzickým osobám právo „být zapomenut“, tedy okamžitého vymazání osobních údajů. Veřejnosti je z minulosti znám například případ Maria Gonzáleza, jehož stížnosti na Google v roce 2014 vyhověl Soudní dvůr EU. Vyhledávač po soudním rozhodnutí musel vymazat irelevantní a zastaralá“ soukromá data týkajícího se Gonzálezova dluhu. Podle průzkumu však celých 41 % firem není schopno toto právo být zapomenut uplatnit.

3.1.2 Řešení pro malé podniky přechodem na cloud

Co se týká technologického řešení, tím nejsnazším a relativně laciným bude pro malé firmy přechod na cloud. Poskytovatelé cloudových služeb si totiž bezpečnost pečlivě hlídají. V

praxi budou data v naprosté většině případů více v bezpečí v cloudu než ve firmě, kde je bezpečnost dat na lokálních serverech řešena všelijak. Výhodou cloudových služeb je navíc to, že servery, úložiště, služby a aplikace, které tyto služby nabízejí, jsou uživatelům dostupné vzdáleně přes síť nebo internet. Firmám se nejspíš vyplatí jít do cloudu a nechat bezpečnost na lidech, kteří jí rozumí.

Na druhou stranu není možné spoléhat na to, že přesunem osobních dat do cloudu některého z jeho providerů máte vše s GDPR vyřešeno, a to i za předpokladu, že dodavatel prohlásí, že je v souladu s nařízením. Používáním těchto služeb se správce nezbavuje vlastní zodpovědnosti za dodržování pravidel nařízení, protože GDPR počítá se sdílenou zodpovědností za zpracování dat. Správci budou mít povinnost nastavit si se zpracovateli takové smlouvy, ze kterých bude zjevné, kdo je odpovědný za případný únik dat nebo jiné narušení ochrany. V neposlední řadě by také ve smlouvě měli ošetřit situaci, kdo ponese odpovědnost za případné škody. Jak už je všeobecně známo, sankce mohou při porušení pravidel GDPR dosáhnout až 4 procent celkového ročního obratu nebo 20 milionů eur a organizace navíc mohou být vystaveny žalobám od subjektů dat s nárokem na odškodnění v případě hmotné či nehmotné újmy.

„Je na správci, aby analyzoval dopady řešení využití cloud computingu, zajistil adekvátní opatření na své straně a aby si uzavřením smluvních vztahů s případným poskytovatelem služeb cloud computingu ošetřil veškeré podmínky zpracování. Z hlediska zákonných pravidel a záruk požadovaných pro předávání osobních údajů lze doporučit využívat pouze webové služby a cloudová úložiště, které se nacházejí na území EU a jsou plně pod jurisdikcí evropského práva," komentuje za Úřad pro ochranu osobních údajů jeho mluvčí David Pavlát.

Server Podnikatel.cz se obrátil na některé z cloudových providerů, jejichž služeb často využívají malé a střední podniky, aby zjistil, jak se na GDPR připravují, zda se jejich klienti mohou spolehnout na dodržování nových zákonných požadavků a počítat s jejich podporou.

Prohlášení o shodě s nařízením GDPR už před nějakým časem potvrdily obě společnosti Google a Microsoft, takže lze oprávněně předpokládat, že značnou část povinností a odpovědnosti za bezpečné zacházení s osobními údaji převezmou za svoje klienty.

Ostatní poskytovatelé uvádějí, že jsou ve fázi důkladného mapování a dokumentování procesů zpracovávání osobních údajů a připravují se na nezbytné organizační a technologické změny. Nicméně je nutné zdůraznit ten fakt, že se nová pravidla GDPR rozhodně nevztahují pouze na dodavatele cloudových řešení, ale na každý subjekt, který je v roli zpracovatele, ať už jde o poskytovatele jakéhokoliv informačního systému, v němž jsou zpracovávána osobní data, nebo o zpracovatele v roli poskytovatelů služeb různého charakteru.

3.1.3 Eshopy

Provozovatele eshopů jistě bude nejvíce zajímat, zda budou potřebovat souhlas zákazníků ke zpracování jejich údajů a jak to bude z již získanými souhlasy?

K provozu internetového obchodu (pro účely plnění smlouvy) není nutné obstarávat souhlas se zpracováním osobních údajů. Každý provozovatel e-shopu musí vzít Obecné nařízení (stejně tak jako dnes zákon č. 101/2000 Sb., o ochraně osobních údajů) v úvahu ve vztahu ke všem činnostem s osobními údaji, které provádí. Obstarávání souhlasu čeká ty správce, kteří musí ke zpracování osobních údajů mít souhlas a zároveň tento souhlas neodpovídá především podmínkám článku 7 Obecného nařízení (např. byl presumován v obchodních podmínkách, aniž by subjekt údajů měl reálnou možnost uzavřít plnění i bez takto presumovaného souhlasu).

Pro úplnost je třeba upozornit, že pravidla pro používání cookies a zpracování osobních údajů za účelem elektronické reklamy, dosud upravená zvláštními předpisy (zákon č. 127/2005 Sb. a č. 480/2004 Sb.), budou ovlivněna přijetím dalšího předpisu EU, tzv. nařízení o e-privacy, jehož schválení lze očekávat v 2. pol. roku 2018.

Po obsahové stránce dosavadní definici zpracování osobních údajů Obecné nařízení nemění, povinnosti zpracování osobních údajů se tak vztahují na nakládání s papírovými dokumenty a evidencemi, stejně jako na počítačové databáze a přenosy, tedy typické operace e-shopů s osobními údaji.

Co se týče eshopů a povinnosti jmenování pověřence, tak běžný provoz e-shopů nemá důvod jej jmenovat.

Poslední co jistě stojí za zmínku tak je situace, kdy si nějaký provozovatel koupí databázi kontaktů, aby mohl rozšířit síť potenciálních klientů a zasílat mu například marketingová sdělení. Pokud si tedy koupíte od třetí strany databázi kontaktů obsahující mimo ostatní údaje e-mailovou adresu fyzické osoby, na kterou jí chcete zaslat marketingové sdělení či obchodní nabídku, tak se nezbavujete povinnosti zajistit si k této aktivitě souhlas dotčené osoby. A to buď ujištěním od prodávajícího, že takový souhlas od osob vedených v předmětné databázi získal nebo si ho budete muset znovu vyžádat sami přímo od samotných osob. Stáváte se totiž novým správcem jejích osobních údajů a dle článku 14 GDPR máte povinnost informovat fyzickou osobu vedenou v databázi o zdroji, od kterého jste její osobní údaje koupili a za jakým účelem s nimi chcete nakládat.

3.1.4 Hotely a cestovní ruch

Evidujete osobní údaje ubytovaných hostů? Nebo Vaše restaurace vyžaduje email pro přihlášení do wifi? Pak se o GDPR zajímejte.

V první řadě bude třeba rozlišit, zda osobní údaje, ať už hostů nebo zaměstnanců, musíte evidovat na základě nějakého právního předpisu, anebo zda jde o údaje, které dostáváte na základě souhlasu se zpracováním. Souhlasy se zpracováním a poskytované informace budou muset být v souladu s novým nařízením. Udělené souhlasy budete coby správce muset umět doložit kontrolnímu orgánu i v budoucnu. Zvláštní podmínky se navíc budou

vztahovat na ochranu dětí, neboť u nich bude navíc nutný souhlas rodičů. Nová pravidla upravují povinnosti hlásit neprodleně dozorovému úřadu případy porušení zabezpečení ochrany osobních údajů. Kromě dalšího bude potřeba nastavit procesy pro odvolávání souhlasů s dalším zpracováním a zabezpečit poskytování informací dotčeným osobám o zpracovávaných jejich osobních údajů.

- Změn tedy bude celá řada, ale čím začít?
- Zajímejte se o GDPR a ideálně určete osobu ve vedení, která bude mít GDPR na starosti.
- Pokud máte pobočky v EU, zjistěte, zda již někdo GDPR neřeší, neboť se vyplatí postupovat jednotně. Zjistěte, jaké osobní údaje vlastně zpracováváte.
- Zjistěte, s kým osobní údaje sdílíte a kam je fyzicky ukládáte, zejména zda jsou úložiště v EU.
- Vyhledejte odborníky na nastavení procesů, úpravu počítačového systému a kontrolu textů souhlasů se zpracováním a dalších textů.

Ještě bychom rádi zmínili jak podle Obecného nařízení postupovat při zapisování osobních údajů hostů ubytovacího zařízení do ubytovací knihy a ubytovací knihy cizinců pro účely cizinecké policie. Pokud budete provádět zpracování, které Vám jako ubytovacímu zařízení ukládá zákon nebo jiná právní norma, bude se jednat o zpracování prováděné na základě právního důvodu uvedeného v čl. 6 odst. 1 písm. c) Obecného nařízení (GDPR), tj. zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje. V této věci doporučujeme si prostudovat čl. 13 a 14 Obecného nařízení.

3.1.5 Neziskovky

Co nového bude GDPR znamenat pro takovou nestátní neziskovou organizaci, která poskytuje sociální služby podle zákona o sociálních službách?

Asi hlavní změnou je to, že GDPR zavedlo některé nové instituty, například institut tzv. pověřence. V oddílu 4 Obecného nařízení je stanoveno, v kterých případech správce a zpracovatel jmenují pověřence, jeho postavení a úkoly.

Dalšími novými instituty jsou například:

- posouzení vlivu na ochranu osobních údajů podle čl. 35 Obecného nařízení,
- předchozí konzultace podle čl. 36 Obecného nařízení,
- povinnost vést záznamy o činnostech zpracování podle čl. 30 Obecného nařízení.

Tyto povinnosti se však nevztahují na každého správce a Vy sami si musíte posoudit, které z těchto činností budete aplikovat.

Další podrobnosti zatím nejsou známé, nicméně neziskovky můžou vždy požádat o radu Ministerstvo práce a sociálních věcí, které má povinnost od 25. května 2018 pověřence mít podle čl. 37 odst. 1 písm. a) GDPR, když se jedná o zpracovávání osobních údajů orgánem veřejné moci.

4 Závěr

GDPR začne platit 25. května 2018 a přinese několik nových pravidel, které by měly nastartovat důvěru spotřebitelů a potažmo i podniků. Občané získají větší kontrolu nad svými osobními údaji a zároveň podniky dostanou možnost se dále digitálně rozvíjet a růst.

GDPR není pouze o IT bezpečnosti, naopak je to především o tom, aby firmy s osobními údaji nás občanů zacházeli s co největší opatrností a nakládali s nimi jako s maximálně důvěrnými informacemi

GDPR přináší nové pojmy, jako jsou správce (firma co ukládá informace o nás), subjekt údajů (občané) či pověřenec (ten kdo monitoruje, aby vše bylo v pořádku).

GDPR nově ukládá nemalé pokuty, dojde-li k porušení jeho ustanovení.

GDPR dává občanům právo být zapomenut. Nicméně to neznamená, že by občan u každé instituce mohl žádat o úplný výmaz informací či záznamů o něm, především co se týče těch negativních, jako může být například záznam v registru dlužníků atd.

V neposlední řadě je třeba, aby firmy a instituce co nejvíce chránili práva lidí, kteří jim své údaje poskytují.

5 (Zdroje)

http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

https://www.uoou.cz/

www.gdpr.cz

https://braveshow.tv/

https://www.ipsos.com/en