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)

GDPR – General Data Protection Regulation

Obsah:

Co je GDPR?

Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) je nová revoluční legislativa EU, která výrazně zvýší ochranu osobních dat občanů.

OBECNÉ INFORMACE

Obecné nařízení o ochraně osobních údajů, anglicky General Data Protection Regulation (odtud zkratka „GDPR"), celým názvem 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 je novou celoevropsky přímo závaznou komplexní právní regulací, která výrazně zvýší ochranu osobních dat občanů. GDPR nabývá účinnosti 25. května 2018. České republice nahradí dosud platný zákon č. 101/2000 Sb., o ochraně osobních údajů. Hlavním smyslem tohoto předpisu je vyšší harmonizace úpravy ochrany osobních údajů a posílení práv subjektů údajů, a tedy i kvalitnější kontrola nakládání s osobními daty lidí. Rovněž dochází k přesnějšímu stanovení povinností správců a zvýšení sankcí za jejich porušení.

PRÁVA SUBJEKTŮ ÚDAJŮ

GDPR výrazně posiluje práva fyzických osob neboli subjektů údajů. Mezi tato práva patří zejména právo na přístup, opravu, výmaz, právo na omezení zpracování, přenositelnost údajů a právo vznést námitku. Každý subjekt má právo ke všem údajům, které má o něm k dispozici podnik, který zpracovává osobní údaje, tzn. i k nestrukturovaným údajům, které mohou tvořit přílohy e-mailů, nebo které jsou uloženy na různých interních a externích úložištích.

Osoby mají právo na přístup, tedy možnost ověřit si zákonnost zpracování jejich údajů. Toto právo lze omezit v zájmu národní nebo veřejné bezpečnosti, obrany a soudních řízení. Osoby mohou získat přístup k informacím o svém zdravotním stavu, k údajům ve své zdravotní dokumentaci.

GDPR také obsahuje právo být informován o tom, za jakým účelem se osobní údaje dané osoby zpracovávají nebo na jak dlouhou dobu jsou uchovávány, nemělo by se to ovšem dotknout obchodního tajemství nebo duševního vlastnictví.

V případě, že jsou uvedeny nesprávné údaje, může osoba, jejichž údajů se to týká, požádat společnost, která tyto údaje zpracovává, ať je napraví. Společnost zpracovávající údaje by měla umožnit podávat žádosti o nápravu nesprávných údajů online.

Nově mají osoby právo na to, aby podnik zpracovávající jejich osobní údaje, tyto údaje vymazal. Právo na výmaz (právo být zapomenut), je upraveno v článku 17 GDPR. Aby se údaje mohly vymazat, musí být splněna jedna z těchto podmínek:

1. Osobní údaje již nejsou potřebné pro účel, pro který byly zpracovávány.
2. Dojde k odvolání souhlasu, pokud je zpracovávání založeno na souhlasu a není jiný právní důvod pro zpracování těchto osobních údajů.
3. Byla vznesena námitka proti zpracování.
4. Osobní údaje jsou zpracovávány protiprávně.
5. Rodiče nedaly souhlas se zpracováním osobních údajů svých dětí.

Pokud osoba nemá právo na výmaz, může vznést námitku. Správce, který zpracovává předmětné osobní údaje, potom musí omezit zpracování.

Novinkou je zavedení práva na přenositelnost údajů v článku 20 GDPR. Osoby mohou od správce, který zpracovává jejich údaje, získat své osobní údaje v běžně používaném a strojově čitelném formátu. Tyto údaje pak mohou osoby předat bez překážek jinému správci ke zpracování.

DOPAD GDPR NA SME - Malé a střední podniky (Small and Medium Enterprise)

GDPR, až na malé výjimky, nejde a priori cestou úlev pro malé a střední podniky, nýbrž rozsah povinností definuje podle parametrů prováděného zpracování. I SME mohou provádět riziková a rozsáhlá zpracování, a proto by měly splňovat přísné nároky. Pro rozsah povinností tedy není důležitý počet zaměstnanců ani velikost podniku, ale rizikovost a rozsah zpracování, které podnik provádí.

Všichni správci musí dodržovat zásady zpracování osobních údajů uvedené v článku 5 GDPR. Osobní údaje musí být zpracovány korektně a zákonným transparentním způsobem, pro určitý výslovně uvedený a legitimní účel. Mělo by být shromažďováno co nejméně údajů, které jsou nezbytné pro dosažení účelu. Zpracovatel musí osobní údaje zpracovat tak, aby byly náležitě zabezpečeny, chráněny pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním. Základním požadavkem zpracování je jeho zákonnost, která vyplývá předně ze souhlasu subjektu údajů se zpracováním, podnik má pak podle článku 7 povinnost tento souhlas na vyžádání doložit (subjekt ovšem neztrácí právo tento souhlas vzít kdykoliv zpět). Dále může podnik zpracovávat osobní údaje, pokud je to nezbytné pro splnění právní povinnosti nebo je to např. nezbytné pro ochranu životně důležitých zájmů subjektu údajů.

Nyní platná směrnice 95/46/ES stanovila obecnou povinnost ohlašovat zpracování osobních údajů dozorovým úřadům. Tato obecná ohlašovací povinnost byla nařízením zrušena a nahrazena účinnějšími postupy a mechanismy, které se zaměří na postupy zpracování, jež mohou představovat vysoké riziko pro práva a svobody občanů.

Nařízení zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.

Aby správce mohl doložit soulad s GDPR, měl by přijmout vnitřní koncepce, provést procesní změny a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by měla mj. spočívat v minimalizaci zpracování osobních údajů, v jejich co nejrychlejší pseudonymizaci, v transparentnosti účelů a v umožnění přístupu občanů k jejich údajům. Pseudonymizace znamená takové zpracování, při němž už nelze ke konkrétnímu člověku přiřadit jeho osobní údaje bez použití dodatečných informací, které jsou uchovávány odděleně a chráněny, aby k původním údajům nemohly být opět přiřazeny.

Podnik si musí podle článku 30 vést záznamy o činnostech zpracování, za něž odpovídá. Každý správce a zpracovatel má povinnost spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohla být tato zpracování monitorováno.

Tyto záznamy o činnostech musí obsahovat následující informace:

- jméno a kontaktní údaje správce a zpracovatele včetně jména DPO
- účely zpracování

- popis kategorií subjektů údajů a kategorií osobních údajů
- kategorie příjemců, kterým byly nebo budou údaje zpřístupněny
- informace o mezinárodním předávání osobních údajů
- lhůty pro výmaz jednotlivých kategorií údajů
- popis technických a organizačních opatření

Výjimku z povinnosti vést záznamy mají organizace s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností a neexistuje u nich žádné riziko, které by ohrožovalo práva subjektů údajů, tyto organizace citlivé údaje nezpracovávají nebo se osobní údaje týkají rozsudků v trestních věcech.

Jakékoli porušení zabezpečení osobních údajů musí být podle článku 33 GDPR nahlášeno bez zbytečného odkladu (tj. do 72 hodin) dozorovému úřadu, v České republice tedy Úřadu pro ochranu osobních údajů. Pokud zpracovatel zjistí porušení zabezpečení, ohlásí takovou skutečnost neprodleně správci. Pokud jsou práva subjektů ohrožena vysokým rizikem, musí to správce subjektu oznámit., musí to správce subjektu oznámit.

Pokud jsou při zpracování rozsáhlým způsobem ohrožena práva a svobody fyzických osob, musí správce vypracovat posudek vlivu na ochranu osobních údajů, v angličtině DPIA, neboli Data Protection Impact Assessment. Posouzení vlivu na ochranu osobních údaj upravuje článek 35 GDPR. Společnosti či instituce jej budou muset vypracovat, pokud provádějí systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování. Typickým příkladem je činnost bank, pojišťoven nebo leasingových či jiných finančních institucí. Algoritmickým posouzením informací o klientovi vyhodnocují jeho situaci za účelem nabídky služby.

Dále posouzení vlivu na ochranu osobních údajů budou muset vypracovat společnosti poskytující věrnostní programy, online nebo telekomunikační služby založené na lokalizačních datech nebo cílenou behaviorální reklamu.

Obdobnou povinnost pak budou mít všechny společnosti nebo instituce, které v rozsáhlém objemu zpracovávají citlivé osobní údaje anebo systematicky monitorují veřejně přístupné prostory. Příkladem této kategorie společností jsou bezpečnostní agentury, zdravotní pojišťovny nebo nemocnice.

Správce nebo zpracovatel má povinnost podle článku 37 GDPR jmenovat pověřence pro ochranu osobních údajů. Musí tak učinit ve třech případech.

1. zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů),
2. hlavní činnosti správce nebo zpracovatele spočívají v takových operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů,
3. hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

POSTUPY IMPLEMENTACE.

Implementaci GDPR by podnik neměl podceňovat. Doba potřebná pro přípravu GDPR se může pohybovat v rozmezí od 2 do 24 měsíců, u malých a středních podniků je tato doba kratší – od 2 do 12 měsíců. Implementaci můžeme rozdělit do 3 základních fází:

1. mapování a rozdílová (GAP) analýza;
2. dopadová analýza; a
3. implementace GDPR.

1. Mapování a rozdílová (GAP) analýza

Nejprve podnik musí posoudit, jaké informace zpracovává a jak splňuje v současnosti požadavky dle GDPR. Následně se bude posuzovat, jak podnik splňuje právní a technické požadavky GDPR. Nesoulad se předpokládá tam, kde GDPR zavádí nové povinnosti (např. při povinnosti jmenování pověřence).

2. Dopadová analýza

Poté se musí analyzovat dopady, které změny vyvolané nutností zajištění souladu přinesou. U každého nedostatku je třeba posoudit, co je potřeba provést, aby byl tento nedostatek odstraněn. V rámci dopadové analýzy by měly malé a střední podniky zhodnotit, zda a v jakém rozsahu se jich bude týkat jediná relevantní výjimka (právě pro malé a střední podniky) z povinnosti vést záznamy o činnosti zpracování podle čl. 30 GDPR. Podniky nemusí vést záznamy o činnosti zpracování, pokud zaměstnávají méně než 250 osob, pokud zpracování osobních údajů není jejich hlavní činností a právům subjektů údajů u nich nehrozí žádné riziko, tyto organizace nezpracovávají citlivé údaje nebo se osobní údaje netýkají rozsudků v trestních věcech. Je třeba také celkově posoudit rizika konkrétního zpracování. Je to důležité pro zvolení takových opatření k zajištění souladu, která jsou vzhledem k úrovni rizika potřeba, a k ověření, jestli je nutné provádět posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR. Musí se také zjistit riziko zpracování např. při posouzení oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR, posouzení slučitelnosti účelů dle čl. 6 odst. 4 GDPR, splnění požadavků dle čl. 25 GDPR atd. Dále je nezbytné posoudit bezpečnostní rizika podle čl. 32 GDPR a je namístě navrhnout vhodná technická a organizační opatření k zajištění integrity a bezpečnosti zpracování. Dále se pak nelze vyhnout nutnosti posoudit, jestli má podnik povinnost jmenovat pověřence pro ochranu osobních údajů. U malých a středních podniků k tomu nebude často docházet. Pokud podnik dojde k závěru, že musí pověřence jmenovat, měl by tak učinit ještě před zahájením samotné implementace navržených kroků z dopadové analýzy. Pověřenec tak bude moci dát podniku kvalifikované stanovisko k tomu, jestli jsou navrhovaná opatření dostatečná, či nikoliv.

3. Implementace GDPR.

Po dokončení analýzy dopadů podnik začne postupně provádět všechna opatření, která byla v jejím rámci navrhnuta.

1. Mělo by dojít k úpravě externí dokumentace. Měly by se upravit souhlasy se zpracováním, obchodní podmínky, podmínky ochrany osobních údajů, zpracovatelské smlouvy apod.
2. Je třeba upravit interní dokumentace jako např. vnitřní předpisy a jinou dokumentaci určenou zaměstnancům, vytvořit koncepci ochrany osobních údajů, podle potřeby provést a zdokumentovat různá posouzení.
3. Dále je vhodné upravit procesy zpracování osobních údajů, a to jak uvnitř společnosti, tak navenek.
4. Nelze se vyhnout ani úpravě informačních systémů. Aby byl správce schopen plnit povinnosti podle GDPR, pak musí mít pořádek v datech.
5. Musí být vytvořen plán pro případ porušení zabezpečení osobních údajů. Musí se vytvořit procesy interního reportování, vyšetřování a mírnění důsledků porušení zabezpečení.
6. Správce se musí připravit na výkon práv subjektů údajů. Musí se zavést nutná organizační a technická opatření k tomu, aby byl subjektům údajů umožněn a usnadňován výkon jejich práv.
7. Správce se také neobejde bez vytvoření komplexního accountability mechanismu. Procesy správce by měly automaticky generovat potřebnou dokumentaci, která se uchovává. Správce je totiž povinen vždy být schopen prokázat soulad s GDPR. Proto je důležité, aby byla veškerá zpracování podrobně a přehledně dokumentována.
8. Správce musí implementovat zásady záměrné a standardní ochrany osobních údajů. Musí se zavést technická a organizační opatření k zajištění naplňování základních zásad zpracování.

POSTUP V PŘÍPADĚ PORUŠENÍ ZABEZPEČENÍ.

Správce nebo zpracovatel mají povinnost zabezpečit zpracovávané údaje. Přesto může dojít k porušení zabezpečení osobních údajů. Jakékoli porušení zabezpečení osobních údajů musí být podle článku 33 nahlášeno bez zbytečného odkladu dozorovému úřadu, v České republice tedy Úřadu pro ochranu osobních údajů. Pro hlášení je stanovena lhůta 72 hodin. Protože porušení zabezpečení se může vyskytnout kdekoliv v organizaci, měla by se opatření, která jsou nezbytná pro plnění v případě porušení zabezpečení osobních údajů, zavést předem. Musí se nastavit postupy, které budou napomáhat předcházení incidentům, postupy, které pomohou odhalit a vyhodnotit případný konflikt, a postupy uplatňované při řešení incidentu, minimalizaci negativních následků a ohlašování na příslušná místa.

Správce by měl předem vypracovat vhodné plány, které budou určené k řešení případů porušení zabezpečení osobních údajů. Měl by zřídit kontaktní místo pro všechny osoby ohlašující incident, díky čemuž bude schopen zajistit, aby na porušení bylo reagováno rychle a účinně.

Ohlašovací povinnost nedopadá na všechna porušení. Správce nemusí ohlašovat dozorovému úřadu ani subjektu údajů takové porušení, které nepředstavuje riziko pro práva a svobody dotčených fyzických osob, porušení, které nemá nepříznivý dopad nebo neohrozí soukromí dotčených fyzických osob. Např. se jedná o situace, kdy jsou data dostatečně zabezpečena. Neoprávněná osoba je nemůže přečíst, protože byla provedena pseudonymizace nebo šifrování. Nebo třeba v případě, kdy byla data zaslána známému a spolehlivému příjemci omylem a příjemce se zaručí, že zpřístupněné údaje již nevlastní a vymazal je. Riziko už není pravděpodobné. Správce má povinnost dokumentovat veškeré případy porušení, tedy i takové, které nepředstavují riziko pro práva a svobody dotčeného subjektu údajů, a tedy nepodléhají ohlašovací povinnosti Úřadu.

Správce musí hlásit porušení zabezpečení až v případě, kdy dané porušení představuje riziko pro dotčené fyzické osoby. Při ohlášení se musí popsat povaha případu porušení a jméno a kontaktní údaje pověřence nebo jiného kontaktního místa, které může poskytnout bližší informace. Dále se popíší pravděpodobné důsledky porušení a opatření, která správce přijal nebo navrhuje s cílem vyřešit a minimalizovat důsledky porušení. Pokud zpracovatel zjistí takovéto porušení zabezpečení, ohlásí to neprodleně správci.

Pokud existuje vysoké riziko pro práva dotčených osob, je v GDPR stanovena ohlašovací povinnost nejen vůči dozorčímu úřadu, ale i povinnost oznámit takovou skutečnost dotčeným subjektům. Vymezit druhy operací, které pravděpodobně budou mít za následek vysoké riziko pro práva a svobody fyzických osob, je úkolem jednotlivých dozorových úřadů, které by měly takové seznamy sestavit, zveřejnit a předat nově vzniklému Sboru pro ochranu osobních údajů (čl. 35 odst. 4 GDPR). Určující by měla být míra pravděpodobnosti a závažnosti takového rizika. Např. zcizení klientské databáze v nezašifrované podobě, obsahující identifikační údaje, rodné číslo, číslo účtu, přístupové údaje, uživatelské jméno, zákaznické číslo nebo zdravotní stav, přičemž cílem zcizení databáze bylo zneužití osobních údajů, by bylo nutné považovat za vysoce rizikové. Oznámení porušení by mělo být provedeno bez zbytečného odkladu. V oznámení by měla být alespoň popsána povaha porušení, jméno a kontaktní údaje pověřence nebo jiné kontaktní osoby, která může poskytnout podrobnější informace, popis důsledků porušení a doporučení pro dotčenou fyzickou osobu, jak může případné nežádoucí účinky zmírnit. GDPR stanoví výjimky, kdy oznamovat porušení dotčené osobě není nutné. Výjimkou je případ, když zasažené údaje byly nečitelné nebo nešly přiřadit ke konkrétním osobám, byla přijata

opatření, která zajistila, že vysoké riziko již nehrozí nebo by oznámení vyžadovalo nepřiměřené úsilí. V posledním případě místo toho dojde k veřejnému oznámení, které subjekty informuje stejně účinně.

ŠETŘENÍ O UPLATŇOVÁNÍ GDPR

Dodržování GDPR monitorují podle článku 51 GDPR dozorové úřady jako nezávislé orgány veřejné moci. V České republice je tímto dozorovým úřadem Úřad pro ochranu osobních údajů. Dozorový úřad provádí šetření o uplatňování GDPR. Informace o porušení GDPR může dozorový úřad zjistit od jiného dozorového úřadu nebo od jiného orgánu veřejné moci, fyzické osoby mohou podávat stížnosti. Při šetření musí podle článku 58 GDPR podnik, který zpracovává osobní údaje, poskytnout veškeré informace, přístup do všech prostor, kde působí, i přístup k informacím, které dozorový úřad potřebuje pro svoje vyšetřování. Vyšetřování je provedeno formou auditu ochrany údajů. Dozorový úřad ohlásí podniku porušení GDPR. Může mu udělit napomenutí nebo nařídit, aby uvedl operace zpracování do souladu s GDPR. K tomu mu poskytne lhůtu. Dále může nařídit, aby vyhověl žádosti subjektu nebo aby subjektu oznámil případy porušení zabezpečení osobních údajů. Dozorový úřad může také zakázat zpracování osobních údajů, případně dočasně nebo trvale omezit zpracování. Také nařizuje opravu či výmaz osobních údajů. Za porušení se ukládají pokuty.

POKUTY A SANKCE

Úřad pro ochranu osobních údajů ukládá pokuty za porušení GDPR. Ukládání správních pokut je vymezeno v článku 83 GDPR. Pokuty mají být účinné, přiměřené a odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu. Zhodnotí se např. zda k porušení došlo úmyslně nebo z nedbalosti, jak dlouho porušení trvalo nebo jak bylo závažné. Při méně závažném porušení hrozí pokuta až do výše 10 000 000 euro nebo do výše 2 % z celkového celosvětového ročního obratu za předchozí finanční rok. Při závažnějším porušení hrozí pokuta až do výše 20 000 000 euro nebo až do výše 4 % z celkového celosvětového ročního obratu společnosti za předchozí finanční rok. Hodnota pokuty bude stanovena jako vyšší z obou možností. Za závažnější porušení zpracování osobních údajů se považuje např. porušení základních zásad pro zpracování.

Podnik také může být nucen pozastavit zpracování osobních údajů, případně mu hrozí, že nebude moci zpracovávat osobní údaje vůbec.

Podnik, který zpracovává osobní údaje, také odpovídá podle článku 82 GDPR za hmotnou či nehmotnou újmu, kterou způsobil subjektu údajů. Odpovědnosti se může zprostit, pokud prokáže, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Co přináší GDPR nového.

1. Povinnost provádět posouzení dopadu na ochranu osobních údajů

Jak již bylo výše uvedeno, obecná oznamovací povinnost, kdy bylo v zásadě nutné dozorovému orgánu oznamovat jakékoliv zpracování, na které se nevztahovala některá ze zákonných výjimek, bude zrušena a nahrazena jinými mechanismy, které by se měly zaměřit pouze na ty zpracování, které na základě své povahy, rozsahu a účelu mohou představovat vysoké riziko z hlediska práv a svobod subjektů údajů. A právě u těchto, řekněme rizikových zpracování, bude správce povinen ještě před zahájením samotného zpracování provést tzv. posouzení dopadu na ochranu osobních údajů. Posouzení dopadu by mělo obsahovat systematický popis zamýšleného zpracování, posouzení rizik z hlediska práv a svobod subjektů údajů, provedení testu proporcionality včetně posouzení, zda je zpracování ve vztahu k deklarovaným účelům nezbytné. Přičemž se předpokládá, že vypracování takového posouzení by mohlo být delegováno na inspektora pro ochranu údajů, pokud bude danou společností jmenován.

Nařízení zároveň uvádí příkladný výčet situací, kdy posouzení dopadu bude nutné, např. v případě zpracování citlivých údajů, systematického monitorování veřejně přístupných míst nebo systematického a rozsáhlého vyhodnocování osobních aspektů fyzických osob, včetně profilování, jestliže je zpracování osobních údajů prováděno automatizovaným způsobem a rozhodnutí na něm založená působí právní účinky dotýkající se jednotlivých osob nebo jej ovlivní obdobným závažným způsobem.

Správce bude muset v posouzení dopadu rovněž jasně definovat přijatá bezpečností opatření a záruky, které by měly přispět k tomu, že předem definované vysoké riziko bude přijatými opatřeními eliminováno, a tím zajištěna dostatečná ochrana osobním údajům v souladu s nařízením.

V souvislosti s touto novou povinností správce jsou kladeny požadavky i na samotné dozorové orgány jednotlivých členských zemí EU. Ty by měly sepsat a zveřejnit seznam zpracování, na která se vztahují povinnosti provést posouzení dopadu a následně tento seznam sdělit nově zřízené Evropské radě pro ochranu dat. Nově zřízený evropský orgán, by měl nahradit dosavadní Pracovní skupinu podle čl. 29 směrnice (WP 29). Podobným způsobem mohou dozorové orgány vytvořit a zveřejnit seznam zpracování, na která se tato povinnost vztahovat nebude. Dozorovým orgánům se tak ukládá povinnost pozitivního, ale také možnost negativního vymezení zpracovatelských operací, které budou, resp. nebudou předmětem posuzování dopadu ze strany správců. Bude pravděpodobně záležet na jednotlivých členských státech, jakou formu v rámci vnitrostátní právní úpravy nakonec zvolí s ohledem na fakt, že technologický rozvoj je dnes natolik rychlý, že zpracování podléhající či nepodléhající povinnosti posouzení se mohou a pravděpodobně budou v čase měnit.

Povinnost vymezit zpracovatelské operace, které by mohly představovat zvláštní rizika z hlediska práv a svobod subjektů údajů a ty následně podrobit předběžné kontrole dozorového orgánu, předpokládá i směrnice. Některé členské státy provedly taxativní výčet rizikových zpracování a včlenily je do vnitrostátní právní úpravy ochrany údajů, jiné, jako např. Česká republika, tak neučinily a rizikovost zpracování posuzují ad hoc v rámci konkrétního šetření.

Posuzovat přiměřenost zásahu do práv druhých, jejichž údaje budou předmětem zpracování, ještě před zahájením samotného zpracování, v současnosti vyplývá pro správce z obecných principů ochrany osobních údajů obsažených ve směrnici, zejména z povinnosti správce stanovit legální a legitimní účel zpracování, zpracovávat osobní údaje pouze na základě řádného právního titulu a v přiměřeném rozsahu. Například v rámci posuzování přípustnosti uplatnění právního titulu podle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, je povinností správce provést analýzu rizik a test

proporcionality, které by měly být základním předpokladem pro zahájení procesu zpracování osobních údajů. Jsou to právě zpracování založená na právním titulu podle § 5 odst. 2 písm. e) realizovaná bez souhlasu subjektů údajů, která jsou svou povahou často riziková a vysokou mírou zasahující do práv osob, jejichž údaje jsou zpracovávány.

Obecné nařízení proces provádění analýzy rizik, resp. posuzování dopadu na ochranu údajů institucionalizuje, stanoví obecná pravidla, obsah a rámcově vymezuje zpracovatelské operace, na které se má vztahovat. Navíc ukládá povinnost ve vymezených případech provedenou analýzu předložit dozorovému orgánu k posouzení (viz níže předběžné konzultace). Posuzování vlivu zpracování na ochranu osobních údajů může správcům činit do budoucna problémy spojené s neznalostí procesů jeho vytváření. Evropská rada pro ochranu dat, případně jednotlivé orgány dozoru, by měly do budoucna zvážit vytvoření jednotného standardizovaného formuláře, který by jasně definoval požadavky, které bude muset takové posouzení obsahovat, aby je bylo možné předložit dozorovému orgánu v rámci povinné konzultace k posouzení.

2. Předběžné konzultace

Bezprostředně s povinností správce osobních údajů provést v určitých případech předem posouzení dopadu na ochranu údajů, souvisí povinnost správce takovéto případy zpracování předem oznámit dozorovému orgánu k posouzení neboli k předběžné konzultaci. Správce má povinnost zpracování konzultovat s orgánem dozoru v případě, pokud by z posouzení dopadu vyplynulo, že zpracování je vysoce rizikové a zároveň platí, že správce je toho názoru, že riziko nelze zmírnit přiměřenými prostředky, pokud jde o dostupnost technologií a nákladů na jejich zavedení. Dozorový orgán by měl následně zkoumat soulad zamýšleného zpracování s nařízením, přičemž může dospět k závěru, že zamýšlené zpracování není v souladu s nařízením a doporučit správci upravit zpracování tak, aby případná rizika byla dostatečným způsobem omezena a zpracování nebylo v rozporu s nařízením. Pokud ovšem sám správce, již ve stádiu posuzování dopadu, usoudí, že opatření ke zmírnění rizika vzhledem k dostupným technologiím a nákladům na jejich zavedení neexistují, pak je otázkou, jaké doporučení může očekávat od orgánu dozoru v rámci povinné konzultace, resp., jak v těchto případech bude orgán dozoru postupovat. Pokud by žádná opatření, jak ze strany správce, tak dozorového orgánu nalezena nebyla, pak by zřejmě nezbývalo dozorovému orgánu než konstatovat, že zpracování nelze provádět.

Další nevyjasněnou otázkou zůstává, jaký charakter má nebo má mít stanovisko dozorového orgánu vydaného v rámci konzultací, tedy zda se bude jednat o systém povolení, např. podobný současnému systému předběžných kontrol podle § 17 zákona č. 101/2000 Sb., prováděných v rámci správního řízení, nebo se bude jednat o konzultace v pravém slova smyslu, které budou mít pouze doporučující charakter. Ohledně stanoviska/povolení dozorového orgánu lze vzhledem k tomu, že nařízení ponechává finální podobu tohoto institutu na samotných členských státech, důvodně předpokládat, že mohou v tomto ohledu panovat do budoucna značné rozdíly mezi jednotlivými členskými státy. Vyjdeme-li ovšem z gramatického výkladu, jelikož nařízení výslovně hovoří o konzultaci nikoliv o povolení, pak se spíše lze přiklonit k názoru, že by se mělo jednat pouze o určité doporučení či radu dozorového úřadu, nežli o schvalovací proces, na jehož konci by bylo vydání individuálního správního aktu. Alespoň otázku závaznosti stanoviska dozorového orgánu pro jeho případnou další dozorovou činnost, řeší nařízení tím způsobem, že nevyjádření se dozorového orgánu ve stanovené lhůtě, nebude mít vliv na dozorové pravomoci orgánu dozoru včetně pravomoci zpracování zakázat např. v rámci provedené kontroly.

Z výše uvedeného vyplývá, že část dosavadní oznamovací povinnosti zůstala prostřednictvím povinných konzultací zachována, a to ta část, která se týká povinnosti správce oznámit rizikové zpracování a povinnosti dozorového orgánu takové zpracování podrobit tzv. předběžné kontrole, resp. předchozí konzultaci. Vágnost institutu předběžných konzultací by však přeci jenom měla být alarmující, neboť neprovedení posouzení dopadu nebo zpracování osobních údajů bez předchozí konzultace může být penalizováno až do výše 10 000 000 EUR nebo v případě podniků do výše 2 % jejich ročního celosvětového obratu.

3. Povinnost vést záznamy o zpracováních osobních údajů

Další administrativní povinností správce, případně zpracovatele nebo zástupce správce nebo zpracovatele bude vést záznamy o všech zpracováních, za která nesou odpovědnost. Nařízení vymezuje, jaké konkrétní údaje musí být součástí takové dokumentace (jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů). Nařízení počítá s výjimkami z povinnosti vést dokumentaci zpracování pro podniky s méně než 250 zaměstnanci. Nicméně i malé podniky mohou zpracovávat velký objem dat a provádět vysoce rizikové zpracování. Proto je výjimka omezena pouze na taková zpracování, která nelze kvalifikovat jako riziková, resp. nezasahující závažným způsobem do práv a svobod jednotlivců nebo zpracování, která nebudou zahrnovat citlivé údaje.

Jak z výše uvedeného vyplývá, bude správce povinen vést dokumentaci, jejímž obsahem bude v zásadě podobné penzum informací, které je v současné době správce povinen sdělovat dozorovému orgánu v rámci oznamovací povinnosti, a které dozorový orgán následně zapisuje do veřejného registru zpracování. Na rozdíl od současné právní úpravy nebude již povinností správců dokumentaci obsahující informace o zpracování zasílat dozorovým orgánům za účelem jejich registrace, nicméně správci budou povinni záznamy o zpracování dozorovému orgánu na jeho žádost zpřístupnit.

4. Povinnost ohlašovat případy narušení bezpečnosti

Další, svou povahou ohlašovací povinností, která pro správce může znamenat nezanedbatelnou administrativní zátěž, je ohlašování případů narušení bezpečnosti osobních údajů (tzv. data breaches). Nejedná se o institut zcela nový. Do českého právního řádu byl v souladu s právem EU tento nový nástroj ochrany osobních údajů a soukromí zaveden dne 1. ledna 2012, kdy nabyl účinnosti zákon č. 468/2011 Sb., kterým se současně mění tři zákony týkající se oblasti elektronických komunikací, ochrany osobních údajů a služeb informační společnosti. Podle tohoto zákona se poskytovatelům služeb elektronických komunikací výslovně stanoví povinnost řešit případy porušení ochrany osobních údajů, včetně povinnosti takové narušení oznámit Úřadu pro ochranu osobních údajů.

Zatímco dnes se tato povinnost vztahuje ve většině členských států pouze na poskytovatele elektronických komunikací, podle nového nařízení musí tuto povinnost plnit každý správce, a to během 72 hodin od doby, kdy se o narušení dozví. Nařízení vyjmenovává minimální množství informací, které musí správce poskytnout dozorovému orgánu. Nařízení však připouští výjimku z této povinnosti, a to v případě, kdy narušení bezpečnosti by pravděpodobně nepředstavovalo riziko z hlediska práv a svobod jednotlivce. Znamená to tedy, že by tak nemuselo docházet k ohlašování drobných bezpečnostních incidentů, nebo omylů způsobených např. selháním lidského faktoru, kdy by bylo možné konstatovat, že riziko pro práva a svobody fyzických osob není

vysoké. Správce má rovněž povinnost vést přehled narušení ochrany osobních údajů včetně informací o okolnostech porušení, jeho dopadech a opatření přijatých k nápravě stavu.

Správce ovšem nemá povinnost oznamovat bezpečnostní incidenty pouze dozorovému orgánu ale také samotným dotčeným subjektům, a to v případě, že narušení bezpečnosti by představovalo vysoké riziko pro práva a svobody fyzických osob. V průběhu přípravy nařízení došlo postupným vývojem alespoň k určitému omezení administrativní zátěže související s touto povinností správce v tom smyslu, že oznámení případů narušení bezpečnosti subjektu údajů nebude nutné provádět, pokud správce bude schopen prokázat, že zavedl příslušná technická a organizační ochranná opatření, která byla použita u údajů dotčených narušením bezpečnosti (např. byly údaje šifrovány), nebo prokáže, že přijal následná opatření, která zajistí, že riziko pro práva a svobody subjektů údajů se pravděpodobně již nebude opakovat.

Dosavadní zkušenosti s ohlašováním narušení bezpečnosti údajů nejen z ČR ale i z ostatních států EU však ukazují, že povinné subjekty plní tuto zákonem danou povinnost pouze velmi sporadicky. Většinou se jedná řádově o několik podání za rok. O důvodech takto nízkého počtu oznámení se vedou již několik let v rámci EU diskuse. Jeden z hlavních důvodů nezájmu správců oznamovat případy narušení lze určitě shledat v obavách oznamovatelů z případných sankcí, pokud by se přiznali, že k narušení bezpečnosti osobních údajů v jejich společnosti došlo. Otázkou rovněž zůstává i efektivnost oznamování narušení ve vztahu ke zvýšení úrovně ochrany bezpečnosti.

5. Povinnost jmenovat inspektora ochrany údajů

Neméně významnou novinkou obecného nařízení, která doposud v právním řádu České republiky chyběla, je výše několikrát zmíněná funkce inspektora ochrany osobních údajů. Jedná se o osobu s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany údajů, jež pro správce nebo zpracovatele zajišťuje soulad s nařízením, případně dalšími předpisy v oblasti ochrany osobních údajů. Povinnost jmenovat inspektora ochrany údajů je nařízením explicitně stanovena pro orgány veřejné moci, správce nebo zpracovatele, jejichž hlavní činnost spočívá v operacích, které kvůli své povaze, rozsahu a/nebo účelu vyžadují pravidelné a systematické monitorování subjektů údajů v širokém rozsahu anebo jejichž hlavní činnosti spočívají ve zpracování zvláštních kategorií osobních údajů. V jiných případech je povinností správce, zpracovatele či asociací nebo jiných institucích zastupujících kategorie správců či zpracovatelů jmenovat inspektora ochrany údajů pouze pokud tak stanoví unijní či vnitrostátní zákon, z čeho lze dovodit, že je v kompetenci členských států tuto povinnost rozšířit i na další subjekty. Jinými slovy, na rozdíl od původního záměru Komise, není jmenování inspektorů ochrany údajů povinné, ale je ponecháno na vůli jednotlivých členských států, zda povinnost jmenovat inspektory ochrany údajů rozšíří i na jiné subjekty, resp. okruhy zpracování, než obligatorně stanoví nařízení.

Danou činnost může osoba v této funkci pro správce či zpracovatele vykonávat jako pracovník i na základě smlouvy o poskytování služeb. Inspektor ochrany údajů má být přímo podřízen vrcholným řídícím pracovníků správce nebo zpracovatele. V členských státech, které již povinnost jmenovat inspektora ochrany osobních údajů mají ve svých právních předpisech stanovenou, je u podnikatelských subjektů tato funkce často svěřená do působnosti právních či compliance útvarů, přičemž výjimkou není ani outsourcing této funkce na další specializované entity. Nařízení pro tuto funkci stanoví nejen předpoklady a požadavky, jež musí každý inspektor ochrany údajů splňovat, ale také úkoly, které má v rámci své funkce plnit. Inspektor ochrany údajů, pokud je jmenován, musí být náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů,

k plnění svých úkolů mu musí být poskytnuty nezbytné zdroje a rovněž přístup k osobním údajům a operacím zpracování. Pod pojmem potřebné zdroje si lze představit například personál, rozpočet či konkrétní nástroje pro zajištění řádného provádění výkonu funkce inspektora ochrany údajů jako například software pro reporting.

Mezi hlavní povinnosti inspektora ochrany údajů patří sledování souladu s regulací a poskytování informací a poradenství ohledně povinností vyplývajících z nařízení a má rovněž spolupracovat a sloužit jako kontaktní místo pro jednání s dozorovým orgánem. Na inspektora ochrany údajů se mohou také obracet subjekty údajů, a to ve všech záležitostech souvisejících se zpracováním jejich osobních údajů nebo výkonem práv podle nařízení. Dle nařízení není vyloučen ani výkon dalších činností inspektora ochrany údajů, za předpokladu, že nevedou ke střetu zájmu. Správce nebo zpracovatel má také povinnosti zajistit, aby inspektor ochrany údajů mohl jednat nezávisle. Skupiny podniků pak mají dle nařízení možnost jmenovat pouze jednoho inspektora ochrany údajů, za předpokladu, že je snadno dostupný pro všechny členy skupiny.

Další povinnosti

Kromě výše popsaných, je v nařízení obsažená i řada dalších povinností správců a zpracovatelů, jež jsou přímo odvozeny od práv subjektu údajů. Subjektům údajů nařízení totiž přináší posílení jejich stávajících práv, a to prostřednictvím výrazně větší kontroly nad vlastními osobními údaji. Nařízení fyzickým osobám poskytuje snazší přístup k jejich osobním údajům tím, že správci či zpracovatelé je budou muset důkladněji informovat o způsobu zpracovávání jejich osobních údajů, přičemž tyto informace mají být dostupné v jasné a srozumitelné podobě. Uvedené se odráží také v nových požadavcích, které jsou kladeny na souhlas subjektu údajů se zpracováním svých osobních údajů, jehož prokázání je odpovědností správce. Fyzické osoby budou nově disponovat také právem na přenositelnost osobních údajů mezi poskytovateli služeb a dnes zejména v souvislosti s internetovými vyhledávači často diskutovaným právem být zapomenut, které spočívá v tom, že pokud si to subjekt údajů nepřeje a správci či zpracovateli nesvědčí žádný právní titul, musí být osobní údaje vymazány. V této souvislosti lze také ještě jednou zmínit výše popsané právo subjektu údajů být informován o zneužití vlastních osobních údajů. Obecnou povinností správce i nadále zůstává povinnost zavést vhodná technická a organizační opatření a postupy tak, aby dané zpracování splňovalo požadavky nařízení a zaručovalo ochranu práv subjektů údajů.

Jaké povinnosti ukládá GDPR institucím a firmám.

Nyní platná směrnice 95/46/ES stanovila obecnou povinnost ohlašovat zpracování osobních údajů dozorovým úřadům.

Tato povinnost představuje zátěž pro firmy, avšak nepřispěla ke zlepšení ochrany osobních údajů. Proto bude tato obecná ohlašovací povinnost nařízením zrušena a nahrazena účinnějšími postupy a mechanismy, které se zaměří na postupy zpracování, jež mohou představovat vysoké riziko pro práva a svobody občanů.

Nařízení nově zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR. Uplatnění principu zodpovědnosti bude představovat pro podnikatele nemalé časové a finanční investice. Ty se budou týkat zejména těchto oblastí:

- implementace záměrné a nezbytné ochrany dat
- vypracování posouzení vlivu na ochranu osobních údajů, v angličtině DPIA neboli Data Protection Impact Assessment
- jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)
- zavedení tzv. pseudonymizace osobních údajů
- vedení záznamů o činnostech zpracování
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů

DPIA neboli posouzení vlivu na ochranu osobních údajů bude naprostou novinkou. Společnosti či instituce jej budou muset vypracovat, pokud provádějí systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování. Typickým příkladem je činnost bank, pojišťoven, leasingových či jiných finančních institucí. Algoritmickým posouzením informací o klientovi vyhodnocují jeho situaci za účelem nabídky služby.

Významnou skupinou firem, která bude muset čelit této administrativní povinnosti, jsou společnosti poskytující věrnostní programy, online nebo telekomunikační služby založené na lokalizačních datech nebo cílenou behaviorální reklamu.

Obdobnou povinnost pak budou mít všechny společnosti nebo instituce, které v rozsáhlém objemu zpracovávají citlivé osobní údaje anebo systematicky monitorují veřejně přístupné prostory. Příkladem této kategorie společností jsou bezpečnostní agentury, zdravotní pojišťovny nebo nemocnice.
Aby správce mohl doložit soulad s GDPR, měl by přijmout vnitřní koncepce, provést procesní změny a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by měla mj. spočívat v minimalizaci zpracování osobních údajů, v jejich co nejrychlejší pseudonymizaci, v transparentnosti s ohledem na účely a zpracování osobních údajů a v umožnění přístupu občanů k jejich údajům.
Pseudonymizací se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu člověku bez použití dodatečných informací, které jsou uchovávány odděleně a chráněny proti opětovnému přiřazení k původním údajům.

Dalším principem spadajícím do oblasti zodpovědnosti je povinnost správců nebo zpracovatelů vést záznamy o činnostech zpracování, za které zodpovídají. Každý správce a zpracovatel bude povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány.

Tyto záznamy o činnostech musí obsahovat následující informace:

- jméno a kontaktní údaje správce a zpracovatele včetně jména DPO
- účely zpracování

- popis kategorií subjektů údajů a kategorií osobních údajů
- kategorie příjemců, kterým byly nebo budou údaje zpřístupněny
- informace o mezinárodním předávání osobních údajů
- lhůty pro výmaz jednotlivých kategorií údajů
- popis technických a organizačních opatření

Výjimky z povinnosti vést záznamy o činnostech zpracování lze uplatnit pro organizaci s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje u nich riziko pro práva a svobody osob a tyto organizace nezpracovávají citlivé údaje.

Jaké sankce hrozí firmám, které budou GDPR ignorovat.

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.

Co považuje GDPR za osobní údaje.

Osobní údaje jsou ve stávající směrnici z roku 1995 i v GDPR definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.

Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

Obecné nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, jimiž jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.

Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby nebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace. Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem, které vypovídají o tělesném nebo dušením zdraví člověka.
Biometrickým údajem jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, ale podle poslední judikatury i podpis.
Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, údaje zemřelých osob a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter. Týká se to tedy údajů, které zpracováváme pro osobní potřebu a s nikým je nebudeme sdílet.

Správný souhlas podle GDPR.

GDPR a změny, které toto nařízení přinese, se dnes skloňují ze všech stran, a i přesto, že jedním z klíčových požadavků GDPR je transparentnost a srozumitelnost, tak srozumitelných návodů jak získat souhlas, je jen velmi málo. Pokusíme se proto přispět do této debaty návodem, který by měl v první řadě pomoci s přípravou na získání souhlasu ke zpracování osobních údajů udělovaným za účelem zasílání obchodních sdělení.

Co je vlastně souhlas.

Pro začátek je nutné si říci, že souhlas je jen jedním z mnoha právních titulů, které opravňují ke zpracování osobních údajů. Např. právní titul nezbytnosti zpracování pro splnění právní povinnosti vás opravňuje zpracovávat údaje subjektu v rozsahu nezbytném pro plnění vašich povinností uložených jinými zákony – na uchování údajů na fakturách v účetnictví nepotřebujete další souhlas. Stejně tak na e-mailový marketing jen těžko budete moci uplatnit právní titul veřejného zájmu nebo ochrany životně důležitých zájmů.

Dnes většina marketérů využívala titulu plnění smlouvy – neboli vztahu dodavatele se zákazníkem, který zná i GDPR – a nezískávala přímo souhlas. Tento přístup má však zásadní omezení, a to především v rozsahu možného použití údajů. Z pohledu obchodního vztahu lze za oprávněné použití považovat např. zaslání informace o končící záruce, neboť taková zpráva se vztahuje k obchodnímu vztahu. Marketingová sdělení však nelze dát do souvislosti s plněním smlouvy ani obchodního vztahu – pro užívání zboží či služeb nejsou obchodní sdělení nezbytná. Často se v tomto směru skloňuje i titul oprávněného zájmu správce. Ten však není bezbřehý a na jeho základě lze provádět jen omezenější analytické činnosti, typické pro klasický hromadný (necílený) marketing.

Obchodní sdělení.

Další omezení jsou obsažena v úpravě zákona o některých službách informační společnosti, upravující podmínky, za kterých lze zasílat obchodní sdělení elektronickými prostředky. Tato úprava tedy nereguluje zpracování osobních údajů, ale využití určitého kanálu pro zasílání obchodních sdělení. Velmi stručně lze říci, že podmínkou pro zaslání jakéhokoli obchodního sdělení je získání opt-in či opt-out souhlasu, přičemž na základě opt-out souhlasu lze zasílat obchodní sdělení pouze v případě, že k získání e-mailové adresy došlo v souvislosti s prodejem zboží nebo služby. Navíc předmětem těchto marketingových sdělení musejí být pouze vlastní obdobné výrobky nebo služby. Subjekt však musí mít možnost vyslovit nesouhlas s jejich zasíláním (proto opt-out). Ve všech ostatních případech (sdělení o odlišných produktech a službách, o produktech a službách třetích stran, telefonické oslovování apod.) je nutno získat tzv. opt-in souhlas, který subjekt musí aktivně a vědomě udělit (např. zaškrtnutím políčka).

Když jsme si teď řekli, co nelze, tak si pojďme říci, co lze, tzn. jaký mít právní titul pro zpracování osobních údajů, abyste mohli realizovat vaše e-mailové marketingové kampaně bez obav. S ohledem na řadu omezení, které se pojí s užitím titulu oprávněného zájmu, je jediným vhodným právním titulem pro cílený marketing souhlas příjemce se zpracováním osobních údajů a zasíláním obchodních sdělení (viz výše). Souhlas musí být prokazatelný, dobrovolný, mít jednoznačný účel a rozsah a dále musí být informovaný. Zjednodušeně řečeno subjekt, který uděluje souhlas, tak musí učinit z vlastní vůle a musí vědět, s čím souhlasí, komu tento souhlas uděluje a za jakým účelem. Pojďme si rozebrat jednotlivé části tohoto souhlasu.

Prokazatelný – správce osobních údajů nese důkazní břemeno ohledně udělení souhlasu, tzn. musí využít dostupných prostředků k ověření pravosti souhlasu, aby byl schopen tento souhlas prokázat. V případě e-mailů je takovým technickým nástrojem zaslání ověřovacího e-mailu na uvedenou adresu s odkazem pro potvrzení, zvané double opt-in nebo také confirmed opt-in.

Často se lze setkat s názorem, že GDPR ani zákon o některých službách informační společnosti o double opt-inu nikde nehovoří, ale to je zcela mylný výklad – jedná se o obecné právní předpisy, které musí fungovat nejen pro e-maily, a tak by vyjmenovávání konkrétních technických řešení bylo principiálně špatné.
Nutnost double opt-inu vyplývá z důkazního břemene a faktu, že se jedná o jedinou metodu, jak vytvořit vazbu mezi zadanými údaji a e-mailovou adresou. Všechny ostatní metody jako např. Re-Captcha, checkboxy, opakované zadání atp. pouze chrání před automatizovaným zadáním a mohou zaznamenat pouze údaje o vyplnění údajů, nikoliv o souhlasu vlastníka e-mailové adresy.

Dobrovolný - dobrovolnost nebo také nepodmíněnost je reakcí na častou praxi, kdy docházelo ke spojování a podmiňování souhlasů. Vznikaly tak situace, kdy nebylo možné provést nákup bez potvrzení zcela abstraktního souhlasu se zpracováním osobních údajů. Navíc tyto souhlasy byly často skryté, a tak se mnohdy jednalo o souhlas se všeobecnými obchodními podmínkami, ve kterých pak byl někde hluboko zakotven souhlas se zpracováním osobních údajů a zasíláním obchodních sdělení. Vzhledem k tomu, že GDPR silně cílí na transparentnost, tak je toto pochopitelně zcela nepřípustné.

Jednoznačný účel a rozsah - tento bod se také vztahuje k praxi rozsáhlých všeobecných podmínek a nedostatečné transparentnosti. Nově tak musí být zcela jasné, za jakým účelem osobní údaje poskytujete (proč) a v jakém rozsahu budou zpracovávány (k čemu). Tzn. pokud poskytnete souhlas čistě se zasíláním obchodních sdělení a zpracováním osobních údajů za tímto účelem a poskytnete pouze svou e-mailovou adresu, znamená to, že správce může použít pro zasílání obchodních sdělení pouze tento údaj. Aby vám však mohl posílat např. personalizované zprávy podle toho, jaké produkty navštívíte na jeho stránkách, musí mít váš souhlas i k tomuto.
Jednoznačný projev vůle – podobně jako v současnosti i podle GDPR platí, že souhlas musí být udělen jednoznačným projevem vůle osoby. Z tohoto projevu musí být zjevné, že osoba skutečně chtěla udělit souhlas se zpracováním osobních údajů, nikoli že pouze vyjadřovala souhlas s obchodními podmínkami, uzavřením smlouvy, popř. že pouze nevyjádřila nesouhlas.
Informovaný - toto platí i dnes. GDPR specifikuje, že subjekt, který uděluje souhlas, musí vědět, komu konkrétně tento souhlas uděluje, a být informován o účelu a rozsahu zpracování. Což v praxi znamená, že musí být uvedeno označení konkrétního správce a zpracovatelů, kteří budou mít přístup k osobním údajům, a jak konkrétně budou data použita. Zvláštní důraz je pak kladen na upozornění na jakékoliv zpracování probíhající mimo území EU. V případě souhlasu se zasíláním obchodních sdělení to znamená, že subjekt (příjemce) bude vědět, kdo mu bude co posílat. Tzn. obecné formulace typu "souhlasím s předáním údajů třetím stranám" v žádném případě nejsou přípustné, tyto třetí strany by měly být vyjmenované. Ačkoliv taková povinnost neplyne přímo z GDPR, je její splnění vyžadováno dozorovými orgány v zájmu zajištění informovanosti subjektu. Zvláště v případě využívání cloudových služeb je nutné dát pozor na to, že data mohou opustit EU. Není také přípustné, aby tyto informace byly skryté ve všeobecných podmínkách - naopak GDPR vyžaduje, aby byly dostupné a jasně pochopitelné.

Odebrání souhlasu.

GDPR samozřejmě zachovává i povinnost umožnit odebrání souhlasu se zpracováním osobních údajů, což samozřejmě znamená i odebrání souhlasu se zasíláním obchodních sdělení. Novinkou se však stává právo na přenositelnost dat,tzn. možnost subjektu získat informace o všech údajích, které o něm správce uchovává na základě jeho souhlasu nebo plnění smlouvy, a to ve strukturované podobě. Teoreticky by to mohlo znamenat, že si u vašeho dodavatele vyžádáte tímto způsobem vaši historii a předáte ji novému dodavateli a ten vám na základě toho poskytne např. množstevní slevy. V praxi však nelze čekat, že by tato přenositelnost byla zcela univerzální, neboť tato povinnost nedopadne na veškeré

údaje a navíc každý správce bude disponovat rozdílnými daty v rozdílných formátech a účelem je především umožnit subjektům získat lepší informace o tom, co o nich správce vede za údaje.

Všechna tato pravidla mohou vypadat komplikovaně, ale v zásadě nejde o žádnou novinku - GDPR de facto dohání best practice, které jsou platné již mnoho let. Double opt-in i požadavek na aktivní a informované udělení souhlasu jsou standardem již mnoho let a transparentní chování by mělo být naprostou samozřejmostí. Bohužel mnoho marketérů si za cíl stanovovalo rychlost růstu databáze příjemců, nikoliv jejich kvalitu, a tak si nyní stěžují na GDPR. Realita je však taková, že kdyby se řídili best practice, tak by nyní možná měli výrazně méně adres, zato však kvalitních a se souhlasy, které by odpovídaly GDPR. Pokud však doposud nezískávali souhlasy a využívali adres získaných z obchodního vztahu, tak budou muset všechny tyto adresy přepotvrdit tak, aby k nim získali souhlas v souladu s GDPR.

Otázky a odpovědi ke GDPR.

1. Kdo všechno spadá pod GDPR?
    a. GDPR se vztahuje na všechny fyzické nebo právnické osoby, orgány veřejné moci, agentury nebo jiné subjekty, které shromažďují nebo zpracovávají osobní údaje. Velikost subjektu zde nehraje žádnou roli.
2. Bude se GDPR řídit i živnostník, který nemá zaměstnance?
    a. Pokud živnostník bude shromažďovat nebo zpracovávat osobní údaje, bude se i jeho týkat GDPR. Živnostník může zpracovávat osobní údaje svých klientů nebo dodavatelů.
3. Bude se GDPR řídit e-shop, který má 2 zaměstnance, ale zpracovává údaje stovek zákazníků?
    a. Ano, i e-shop s dvěma zaměstnanci se bude řídit GDPR. Ochrana osobních údajů se týká nejen zaměstnanců, ale i zákazníků, a to bez ohledu na jejich počet.
4. Musím si kvůli tomu kupovat speciální SW nebo HW?
    a. Technická opatřená by měla být přijímána s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob. Lze proto říci, že velká část menších podniků nebude muset pořizovat speciální SW a HW, pokud odpovídají běžným standardům zabezpečení. Užívaný software by měl ideálně pocházet od spolehlivého dodavatele, který garantuje soulad s GDPR.
5. Dopadne GDPR i na kontakty, které jsme získali před zahájením platnosti GDPR? Potřebujeme, aby zákazníci poskytli znovu svůj souhlas, aby tento souhlas splňoval nové podmínky?
    a. Na tyto kontakty se GDPR vztahuje. Starší souhlas bude vyhovující za předpokladu, že způsob jeho udělení bude v souladu s GDPR. Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých údajů a tento souhlas byl udělen svobodně a byl konkrétní, informovaný, jednoznačný a ničím nepodmíněný. Lze předpokládat, že v řadě případů tato podmínka splněna nebude, zejména tehdy, kdy byl souhlas součástí související smluvní dokumentace nebo byl podmínkou pro čerpání služeb.
6. Je právo na výmaz absolutním právem? Pokud zákazník, kterému mám doručit objednávku, požádá o výmaz, tak to musím udělat? Jaké jsou následky výmazu?
    a. Právo na výmaz není absolutním právem. Může se uplatnit pouze za předpokladu, že nejsou osobní údaje již potřebné pro účel, pro který byly shromažďovány nebo zpracovávány. Dále k výmazu nemůže dojít, pokud existuje jiná právní povinnost nebo zákon, který výmazu brání, např. zákon o archivaci obsahuje povinnost organizací archivovat dokumenty obsahující osobní údaje po určitou, zákonem stanovenou dobu.
7. Budou muset personální agentury jmenovat pověřence?
    a. Personální agentury zpracovávají velké množství osobních údajů, a proto budou muset jmenovat DPO, neboli pověřence pro ochranu osobních údajů.
8. Kde najdu, co to je „rozsáhlé zpracování"? Je vydefinováno množství dat?
    a. Tyto termíny nejsou v nařízení jasně definovány, dle výkladových vodítek WP 29 je rozsáhlé zpracování definováno pomocí několika faktorů: počet dotčených subjektů údajů, objem dat, doba trvání zpracování, územní rozsah. Jako příklad rozsáhlého zpracování lze uvést zpracovávání údajů o pacientech v rámci běžné činnosti nemocnice (zpracování údajů o pacientech jednotlivým lékařem se

však za rozsáhlé nepovažuje). Rozsáhlým zpracováním bude i zpracování osobních údajů vyhledávačem pro potřeby cílené reklamy či zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky.

9. Jakou roli bude zastávat Úřad na ochranu osobních údajů? Budu mít povinnost registrovat se u Úřadu?
    a. Povinnost registrace (oznámení zpracování osobních údajů) s účinností GDPR odpadá. GDPR Úřad zachovává a upravuje jej jako nezávislý dozorový úřad.
10. Měl by být odepřen přístup na web návštěvníkovi, který neodsouhlasil sběr osobních údajů?
    a. Subjekt údajů musí udělit jednoznačný a ničím nepodmíněný souhlas. Pokud se ke zpracování osobních údajů takový souhlas potřebuje a subjekt tento souhlas neudělí, nemůže to být důvodem k odmítnutí poskytnout službu, pokud to samotná služba nevyžaduje. Konkrétní příklad u e-shopu: pokud poskytnu jejímu provozovateli osobní údaje nezbytné k zakoupení výrobku, tak neudělení souhlasu k zasílaní marketingových mailů nemůže být důvodem odmítnutí samotného zakoupení produktu.
11. Pokud správu GDPR bude provádět externí firma, kdo bude odpovědný při úniku citlivých dat? Dá se odpovědnost převést na dodavatelskou firmu?
    a. Povinnost ochrany osobních údajů se dle GDPR vztahuje jak na správce, tak i zpracovatele (externí organizaci, která data zpracovává). Obě entity jsou tedy odpovědné za jejich ochranu, jelikož tato data zpracovávají – i v případě, že správce pouze data posbírá a pošle dodavateli.
    b. Pokud evidujeme údaje a ukládáme je v cloudových službách od Google (má povinnost zabezpečit ochranu dat dodavatelská firma Google nebo my?
    c. Poskytovatelé cloudových služeb musí zajistit, aby jejich služby byly v souladu s GDPR. Společnost Google nedávno zveřejnila na svých webových stránkách, že na uvedení do souladu jejich služeb s GDPR intenzivně pracuje. Stále jste však zodpovědní za dodržování pravidel nařízení, GDPR má dopad na celou vaši organizaci, informační systémy, a to vše za vás např. přesun všech osobních údajů do G-suite nevyřeší.
12. Bere se jako osobní údaj i evidence o docházce zaměstnance?
    a. Zaměstnanec je fyzická osoba a pokud lze záznam o docházce jednoznačně spojit s identifikátorem zaměstnance, pak se jedná o osobní údaj.

Pro účely tohoto nařízení se rozumí:

1) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

2) „zpracováním“ jakákoliv 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 jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

3) „omezením zpracování“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

4) „profilováním“ jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

5) „pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

6) „evidencí“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

7) „správcem“ je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

8) „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

9) „příjemcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

10) „třetí stranou“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;

11) „souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

12) „porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

13) „genetickými údaji“ osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

14) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

15) „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

16) „hlavní provozovnou“:

a) v případě správce s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, ledaže jsou rozhodnutí o účelech a prostředcích zpracování osobních údajů přijímána v jiné provozovně správce v Unii a tato jiná provozovna má pravomoc vymáhat provádění těchto rozhodnutí, přičemž v takovém případě je za hlavní provozovnu považována provozovna, která tato rozhodnutí přijala;

b) v případě zpracovatele s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, nebo pokud zpracovatel nemá v Unii žádnou ústřední správu, pak ta provozovna zpracovatele v Unii, kde probíhají hlavní činnosti zpracování v souvislosti s činnostmi provozovny zpracovatele, v rozsahu, v jakém se na zpracovatele vztahují specifické povinnosti podle tohoto nařízení;

17) „zástupcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení;

18) „podnikem“ jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost;

19) „skupinou podniků“ skupina zahrnující řídící podnik a jím řízené podniky;

20) „závaznými podnikovými pravidly“ koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost;

21) „dozorovým úřadem“ nezávislý orgán veřejné moci zřízený členským státem podle článku 51;

22) „dotčeným dozorovým úřadem“ dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť:

a) správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu;

b) subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo

c) u něj byla podána stížnost;

23) „přeshraničním zpracováním“ buď:

a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě; nebo

b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě;

24) „relevantní a odůvodněnou námitkou“ námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení tohoto nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie;

25) „službou informační společnosti“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535 (19);

26) „mezinárodní organizací“ organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě.

ÚOOÚ uveřejnil nejčastější dotazy ke GDPR.

Úřad pro ochranu osobních údajů (ÚOOÚ) uveřejnil na svých webových stránkách nejčastěji kladené dotazy ke GDPR, na které je pravidelně dotazován. „V současné chvíli rubrika Otázky a odpovědi obsahuje témata jako je certifikace, vydávání osvědčení, kodexy chování pro veřejnou správu, porušení zabezpečení osobních údajů, posouzení vlivu na ochranu osobních údajů, pověřenec pro ochranu osobních údajů, práva subjektu údajů, právní důvody zpracování a sociální služby,“ informoval mluvčí Úřadu Tomáš Paták.
S ohledem na důležitost některých odpovědí ze strany ÚOOÚ na nejčastěji kladené dotazy si zaslouží některá témata podrobnější výklad.

Certifikace a vydávání osvědčení.
Úřad konečně vnesl jasno do této veřejností velmi diskutované oblasti, která je doprovázena řadou mýtů a nesprávných doporučení.
Jak Úřad uvádí, v rámci českého překladu nařízení byla v souvislosti s certifikacemi použita odlišná terminologie, která není v souladu se stávající terminologií používanou v oblasti akreditace. Pokud nedojde k úpravě překladu uvedeného nařízení, je nutno řešit vztah obou terminologií. Proto v rámci jednotlivých dotazů zpřesnil pojmy z nařízení a přiřadil k nim ekvivalent dle současné terminologie v oblasti akreditace (v ČR zastřešuje Český institut pro akreditaci, o.p.s.):

- osvědčení = certifikát
- subjekt pro vydávání osvědčení = certifikační orgán
- kritéria pro vydávání osvědčení = certifikační požadavky
- kritéria pro akreditaci subjektů = akreditační požadavky

Co je osvědčení neboli certifikát?
Osvědčení (certifikát) o ochraně osobních údajů je dokument vydaný orgánem oficiálně akreditovaným pro vydávání osvědčení (certifikačním orgánem), kterým subjekt (správce, zpracovatel, výrobce atd.) prokazuje zajištění souladu s požadavky nařízení 2016/679.
Kromě získání osvědčení (certifikátu) jsou jinými možnostmi prokázání souladu s nařízením 2016/679 podpis a dodržování kodexu chování (pokud pro danou oblast existuje) nebo zajištění nezbytné dokumentace a přístupu k činnostem zpracování tak, aby soulad s nařízením bylo možno posoudit například v rámci kontroly dozorového orgánu (Úřad pro ochranu osobních údajů).
Naprosto kategoricky ÚOOÚ uvedl, že osvědčení neboli certifikát o ochraně osobních údajů mohou vydávat pouze subjekty pro vydávání osvědčení (certifikační orgány) pro tuto činnost akreditované. Návrh zákona o zpracování osobních údajů aktuálně počítá s variantou, že akreditaci subjektů pro vydávání osvědčení bude provádět vnitrostátní akreditační orgán České republiky, Český institut pro akreditaci, o.p.s., s nímž již nyní Úřad úzce spolupracuje. Tento orgán tedy bude jedinou autoritou, která subjekty pro vydávání certifikací bude akreditovat.

V současné době Úřad pracuje na přípravě kritérií pro vydávání certifikátů a podmínek pro akreditaci subjektů pro jejich vydávání. V této souvislosti je však očekáváno i vydání vodítek ze strany pracovní skupiny podle článku 29, proto prozatím nelze žádat o akreditaci, a tudíž nelze ani žádat o vydání osvědčení (certifikátu) k určitému produktu, službě nebo zpracování.V okamžiku, kdy to bude možné, bude veřejnost Úřadem informována.
Do budoucna lze tedy počítat s certifikací některých činností v rámci zpracování osobních údajů podporovaných jedním nebo více informačními systémy, produkty (SW a HW) nebo službami. Naopak součástí připravovaného schématu vydávání certifikátu není certifikace osob, především pověřenců pro ochranu osobních údajů, což ÚOOÚ ve svých odpovědích několikrát zdůraznil.

Pověřenec pro ochranu osobních údajů.
Úřad opětovně potvrdil fakt, že GDPR žádnou certifikaci pověřenců nestanovuje jako předpoklad výkonu této funkce.

Pověřenec tak certifikát mít nemusí a správce může jako pověřence vybrat i „necertifikovanou" osobu, která disponuje dostatečným právním povědomím o ochraně osobních údajů a citovaném obecném nařízení. V současné době hojně nabízené kurzy DPO spojené s udělením certifikátu jsou pouhým marketingovým počinem společností, které je nabízejí, ale nemají žádnou oporu v zákoně. Není také náhodou, že když začátkem tohoto roku Facebook vypsal výběrové řízení na pozici interního pověřence pro jejich centrálu v Dublinu, tak jedním z rozhodujících kritérií výběru vhodného kandidáta byla jeho nejméně desetiletá zkušenost v oblastí ochrany osobních údajů a informací. O nějakém certifikátu nepadlo ani slovo.

Mnohem důležitější než krásně vybarvený certifikát bude u výběru vhodného pověřence hrát roli jeho kompetence a znalost nejenom předpisů v oblasti ochrany osobních údajů, ale také prostředí společnosti, pro kterou bude tuto funkci vykonávat. WP 29 totiž nedávno uveřejnila další ze svých výkladových vodítek, tentokrát pro stanovení výše pokut podle GDPR, v nichž mimo jiné podtrhuje povinnost správců nebo zpracovatelů uposlechnout doporučení pověřence, jinak jim v opačném případě může hrozit i vyšší sankce za úmyslné nedodržení jeho pokynů. Z tohoto důvodu výběr kvalitního a odborně zdatného jedince bude mít pro fungování společnosti v oblasti ochrany dat ve světle nových GDPR pravidel klíčovou roli, kterou žádný certifikát nemůže nahradit.

Podle názoru ÚOOÚ nemusí mít společenství vlastníků bytových jednotek ani domov pro seniory vlastního pověřence, nicméně i Úřad doporučuje zřídit tuto funkci na dobrovolné bázi nebo alespoň mít v organizaci určenou osobu, která se bude ochraně osobních údajů věnovat.