GDPR
Obecné evropské nařízení o ochraně osobních údajů

Marie Báčová, ČKAIT

Dne 25. května 2018 nabývá účinnosti

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)

Regulation (EU) 2016/679 of the European Parliament and of the Council

of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Úřední věstník EU, část L 119, 4. 5. 2016, s. 1 – 88 *Celexové číslo: 32016R0679*

Evropské právní předpisy:

- směrnice jsou závazné pro vlády členských států EU, nikoliv pro jejich občany, musí být transponovány (převzaty a zapracovány) do právního řádu každé členské země,
- nařízení jsou univerzálně závazná pro instituce a občany, aniž by musela proběhnout jejich transpozice do národních právních předpisů.

Důvod revize ochrany osobních údajů v Evropské unii

- rozdílná úroveň a forma ochrany v jednotlivých zemích,
- rychlá modernizace prostředků používaných ke zpracování osobních dat.

Národní právní úprava v ČR před 25. květnem 2018

zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon transponoval do našeho právního řádu zmíněnou, nyní rušenou evropskou směrnici 95/46/ES.

Otázka: Je zákon č. 1012/2000 Sb., platný i po 25. květnu 2018?

Adaptační zákon

Evropské nařízení (GDPR) umožňuje, aby se v jím definovaných případech členské státy odchýlily od úpravy v obecném nařízení, nebo dokonce stanovuje, že některé jeho aspekty mají být upraveny ve vnitrostátním právu členského státu.

Nejedná se o svébytný zákon, ale jen o národní doplňkový zákon k obecnému evropskému nařízení podporující proces adaptace českého právního řádu na GDPR.

Právě s ohledem na nutnost přípravy a přijetí adaptačních zákonů v členských státech bylo datum účinnosti GDPR stanoveno s dvouletým odkladem od data jeho přijetí Evropským parlamentem.

Vláda ČR projednala návrh adaptačního zákona **21. 3. 2018**

a předložila návrh sněmovně **28. 3. 2018 s návrhem na projednání návrhu zákona v tzv. zkráceném řízení**

Tak by adaptační zákon nabyl účinnosti současně s evropským obecným nařízením.

Sněmovna se zabývala návrhem zákona **18. 4. 2018 a odmítla jej projednávat ve zkráceném řízení.**

2. čtení - obecná rozprava, zařazeno na jednání od **23. 5. 2018**

Sněmovní tisk 138/0: vládní návrh zákona o zpracování osobních údajů **https://www.psp.cz/sqw/tisky.sqw**

Národní právní předpisy s dopadem na ochranu fyzických osob

Zákon č. 89/2012 Sb., občanský zákoník (Jméno člověka a jeho ochrana, osobnost člověka - § 77 a následující)

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (šíření obchodních sdělení)

Zákon č. 89/1995 Sb., o státní statistické službě

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,

Zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon)

Zákon č. 111/2009 Sb., o základních registrech

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů

Zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů.

Zákon č. 186/2013 Sb., o státním občanství ČR a o změně některých zákonů

Zákon č. 106/99 Sb., o svobodném přístupu k informacím

Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)

Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.

Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů

Zákon č. 111/94 Sb., o silniční dopravě

Zákon č. 111/98 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách)

Sdělení č. 115/2001 Sb. M. S., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat

Základní termíny používané v GDPR, jejich definice

Osobní údaje

veškeré informace o identifikované nebo identifikovatelné fyzické osobě, 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

Správce

fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

Zpracovatel

fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

poskytuje informace a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování; spolupracuje s dozorovým úřadem. Je jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly obecného nařízení.Dozorový úřad

nezávislý orgán veřejné moci zřízený členským státem; v ČR Úřad pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů

Sbor by měl nahradit pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízenou směrnicí 95/46/ES. Měl by být složen z vedoucího dozorového úřadu každého členského státu a evropského inspektora ochrany údajů nebo jejich příslušných zástupců.

Základní termíny používané v GDPR, jejich definice

Zpracování

operace nebo soubor operací s osobními údaji nebo soubory osobních údajů prováděný pomocí či bez pomoci automatizovaných postupů, tj. 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

Profilování

automatizované zpracování osobních údajů s cílem provést hodnocení některých osobních aspektů u fyzické osoby, týkajících se zejména jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu (nutný souhlas subjektu údajů)

Pseudonymizace

zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétní fyzické osobě bez použití dodatečných informací

Evidence

strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií

Souhlas subjektu údajů

svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů

Genetické údaje

osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby a poskytující informace o její fyziologii či zdraví (= citlivé osobní údaje)

Biometrické údaje

osobní údaje týkající se fyzických či fyziologických znaků fyzické osoby nebo znaků jejího chování, které umožňují nebo potvrzují její identifikaci, například zobrazení obličeje nebo daktyloskopické údaje (= citlivé osobní údaje)

Zákonnost zpracování

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) 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;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany,

- zákonnost, korektnost a transparentnost
- účelové omezení
- minimalizace údajů
- přesnost omezení uložení
- integrita a důvěrnost

Zvláštní kategorie osobních údajů

Zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, je možné provádět jen v případech vyjmenovaných v článku 9 obecného nařízení.Pokud se osobní údaje získávají od subjektu údajů, **poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace:**

a) totožnost a kontaktní údaje správce a jeho případného zástupce;

b) kontaktní údaje pověřence pro ochranu osobních údajů, pokud je jmenován;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) oprávněné zájmy správce nebo třetí strany;

e) případné příjemce nebo kategorie příjemců osobních údajů;

f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně;

g) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

h) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

ch) pokud je zpracování založeno na udělení souhlasu, existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

i) existence práva podat stížnost u dozorového úřadu;

e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a možné důsledky neposkytnutí těchto údajů;

f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování,

Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly původně shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu. Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká;

s výjimkou případů, kdy

nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů,povoleno právem Unie nebo členského státu,je to založeno na výslovném souhlasu subjektu údajů.Povinnost vést záznamy o činnostech zpracování **se netýká malých a středních podniků nebo organizací zaměstnávajících méně než 250 osob**, pokud zpracování, které provádějí, nepředstavuje riziko pro práva a svobody subjektů údajů, zpracování je příležitostné (tzv. podpůrné zpracování), nezahrnuje zpracování citlivých údajů. áznamy obsahují tyto informace:

a) jméno a kontaktní údaje správce, případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;

b) účely zpracování;

c) popis kategorií subjektů údajů a kategorií osobních údajů;

d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;

e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci;

f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;

g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření

Zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují:

a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;

b) kategorie zpracování prováděného pro každého ze správců;

c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace;

d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Záznamy se vyhotovují písemně, případně v elektronické formě.

Posouzení vlivu na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován.

Posouzení vlivu na ochranu osobních údajů je nutné provést zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů. Seznam předá Evropskému sboru pro ochranu osobních údajů.

Dozorový úřad může rovněž sestavit a zveřejnit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Rovněž tento seznam předá dozorový úřad Evropskému sboru pro ochranu osobních údajů.

Posouzení musí obsahovat:

a) systematický popis zamýšlených operací zpracování a účelů zpracování, případně oprávněných zájmů správce;

b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

c) posouzení rizik pro práva a svobody subjektů údajů;

d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů.

Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů vždy, pokud

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;

b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;

c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

Jeden pověřenec může být jmenován pro více podniků, pokud je snadno dosažitelný z každého podniku. Stejně tak může být jmenován pro několik orgánů veřejné moci nebo veřejných subjektů s přihlédnutím k jejich organizační struktuře a velikosti. Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a na základě své schopnosti plnit úkoly podle obecného evropského nařízení.

Pověřenec může být pracovníkem správce či zpracovatele, nebo může plnit úkoly na základě jiného smluvního vztahu. Správce nebo zpracovatel zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu. Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Správce a zpracovatel podporují pověřence pro ochranu osobních údajů při plnění jeho úkolů tím, že mu poskytují zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí. Správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele. Pověřenec může plnit i jiné úkoly a povinnosti. Správce nebo zpracovatel zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:

a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle obecného evropského nařízení a dalších předpisů Evropské unie a členského státu v oblasti ochrany údajů;

b) monitorování souladu s tímto nařízením, dalšími předpisy Evropské unie a členského státu v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů včetně rozdělení odpovědnosti,

c) zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

d) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování;

e) spolupráce s dozorovým úřademSubjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle obecného evropského nařízení.

Povinnosti vyplývající z obecného nařízení o ochranně osobních údajů	**Správce osobních údajů**			
	Malá firma provádějící podpůrné zpracování	**Malá firma provádějící podstatné zpracování**	**Velká firma provádějící podpůrné zpracování**	**Velká firma provádějící podstatné zpracování**
	Cukrářství, truhlářství	Menší e-shop, samostatný lékař, advokát	Stavební firma, výrobce motocyklů	Telekomunikační operátor, nemocnice, banka
Pověřenec	Nemusí	Samostatný lékař nebo advokát nemusí (malý rozsah), e-shop podle rozsahu dat	Nemusí	Musí
Posouzení vlivu	Nemusí, pokud nejde o inovativní zpracování	Někdy (vzhledem k rozsahu, inovativnosti)	Někdy (vzhledem k rozsahu)	Musí
Záznamy o činnostech zpracování	Nemusí (pokud nezpracovává citlivé údaje)	Někdy (rozsah, citlivé údaje)	Musí	Musí

Povinnosti stanovené správcům a zpracovatelům se nerozlišují pouze podle toho, zda jde o malou, střední nebo velkou firmu. Rozhodující pro rozsah povinností správce a zpracovatele je rizikovost zpracování, jeho rozsah, povaha, kontext a účely zpracování. Z toho plyne, že i velká stavební firma může mít menší povinnosti než malý podnik v oblasti IT provádějící rozsáhlá zpracování nebo než střední personální agentura zpracovávající řadu citlivých údajů.

Správce a zpracovatel a případný zástupce správce nebo zpracovatele spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů.

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu. Nemusí tak učinit, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s obecným evropským nařízením.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

správce zavedl technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je na příklad šifrování.

Příslušný dozorový úřad schvaluje **závazná podniková pravidla** pro mezinárodní předávání údajů mimo Evropskou unii organizacím ve stejné skupině podniků nebo uskupení podniků vykonávajícím společnou hospodářskou činnost za předpokladu, že: jsou právně závazná a platná pro všechny a prosazovaná všemi dotčenými členy skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, včetně jejich zaměstnanců.

Členské státy, dozorové úřady, Evropský sbor pro ochranu osobních údajů a Komise podporují vypracování kodexů chování, které mají přispět k řádnému uplatňování tohoto nařízení s ohledem na konkrétní povahu různých odvětví provádějících zpracování a na konkrétní potřeby mikropodniků a malých a středních podnikůSdružení nebo jiné subjekty, které mají v úmyslu vypracovat kodex chování nebo upravit či rozšířit existující kodex, předloží návrh kodexu či návrhy na úpravu či rozšíření kodexu dozorového úřadu. Dozorový úřad posoudí návrh, vydá k němu případné stanovisko a schválí jej. Dozorový úřad kodex zaregistruje a zveřejní.

Kodexy by měly obsahovat pokyny pro zavádění vhodných opatření a pro prokázání souladu s obecným evropským nařízením a národními právními předpisy, zejména pokud jde o zjištění rizika souvisejícího se zpracováním osobních údajů, jeho posouzení z hlediska pravděpodobnosti a závažnosti, a stanovení osvědčených postupů ke snížení rizika.

Při vypracovávání kodexu chování nebo při jeho změně či rozšíření by sdružení a jiné subjekty zastupující různé kategorie správců nebo zpracovatelů měly konzultovat příslušné zúčastněné strany, pokud možno i subjekty údajů, a měly by zohledňovat návrhy a stanoviska vyjádřené v reakci na tyto konzultace.

Marie Báčová, ČKAIT

Zavedení mechanismů pro vydávání osvědčení o ochraně osobních údajů

Vydávání osvědčení o ochraně osobní údajů, zavedení pečetí a známek by mělo dokládat souladu s obecným evropským nařízením v případě operací zpracování prováděných správci a zpracovateli.

Vydávání osvědčení je dobrovolné. Osvědčení vydávají subjekty pro vydávání osvědčení nebo příslušný dozorový úřad na základě kritérií jím schválených.

Správce nebo zpracovatel, který předloží své zpracování mechanismu pro vydávání osvědčení, poskytne subjektu pro vydávání osvědčení nebo příslušnému dozorovému úřadu veškeré informace a přístup ke svým činnostem zpracování, které jsou pro provedení postupu vydávání osvědčení nezbytné.

Osvědčení se vydává správci nebo zpracovateli na dobu nejvýše tří let a lze je obnovit za stejných podmínek, pokud jsou i nadále plněny příslušné požadavky.

Subjekty pro vydávání osvědčení by musely být akreditovány

a) národním dozorovým úřadem, nebo

b) vnitrostátním akreditačním orgánem určeným v souladu s evropskými právními předpisy (Český institut pro akreditaci)

Akreditační systém České republiky – soubor procesů, postupů a pravidel umožňující získat od příslušného autoritativního orgánu akreditaci – je upraven především nařízením Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008. Národním akreditačním orgánem České republiky je Český institut pro akreditaci, o.p.s. (ČIA), a to na základě pověření Ministerstvem průmyslu a obchodu a notifikace u Evropské komise v souladu výše uvedenými právními předpisy. V akreditačním procesu má ČIA jako národní akreditační orgán postavení orgánu veřejné moci.

Informace z workshopu k GDPR

V dubnu se zástupkyně ČIA zúčastnila workshopu On data protection certification mechanisms, seals, and marks, který proběhl v Bruselu.

Cílem cesty bylo získání nejnovějších informací o vývoji v oblasti akreditace certifikačních orgánů certifikujících produkty podle nařízení GDPR a poskytnutí pohledu akreditačního orgánu na požadavky pro akreditaci/certifikaci zabezpečení osobních údajů v souladu s tímto nařízením.

Workshop se zabýval tématy technických standardů a alternativních opatření, schémat GDPR a dalších požadavků na akreditace, certifikací přenosu dat a také certifikačními kritérii a procesy certifikace. V rámci diskuze byly prezentovány názory pracovníků akreditačních orgánů, zástupců úřadů na ochranu osobních údajů a také certifikačních orgánů v tom smyslu, že Komise by měla vypracovat kritéria pro akreditaci a certifikaci tak, aby byly požadavky jednotné, a tedy harmonizované na území celé EU.

Marie Báčová, ČKAIT

Informační podpora a informační zdroje

ČKAIT

- článek v časopise Zprávy a informace ČKAIT
- článek v časopise Stavebnictví
- odborné semináře ve všech oblastech Komory

Členové Komory se mohou na Kancelář Praha obracet se svými dotazy, které se týkají aplikace GDPR.

ckait@ckait.cz

Po přijetí tzv. adaptačního zákona bude zpracován „Kodex chování pro členy ČKAIT“ a publikován v rámci informačního systému PROFESIS.

Úřad pro ochranu osobních údajů - ÚOOÚ

www.uoou.cz

Jednotlivá ministerstva vydávají vysvětlující a návodné publikace ke GDPR

Ministerstvo průmyslu a obchodu vydalo pomůcku pro malé a střední firmy k nařízení GDPR

https://i.iinfo.cz/files/podnikatel/631/prirucku-pro-pripravu-malych-a-strednich-firem-na-gdpr.pdf

Ministerstvo školství, mládeže a tělovýchovy

Ministerstvo zdravotnictví

Děkuji za pozornost

Marie Báčová, ČKAIT
mbacova@ckait.cz