Nařízení (EU) 2016/679 – Obecné Nařízení o ochraně osobních údajů a o zrušení směrnice 95/46/ES

Elektrotechnická asociace ČR

RNDr. Karel Neuwirt

30. listopad 2017

74 % Evropanů považuje zveřejňování osobních informací jako narůstající součást moderního způsobu života

hlavními důvody zveřejňování informací jsou přístup k on-line službám v sociálních sítích a sdílených stránkách (61 %) a on-line nákupy (79 %)

43 % uživatelů internetu je přesvědčeno, že po nich je požadováno větší množství údajů než je potřeba

90% Evropanů požaduje, aby v EU byla jednotná ochrana osobních údajů

Zdroj: Special Eurobarometer 359, 2011

22 let stará směrnice 95/46 (1995)
36 let stará Úmluva 108 (1981)

nejsou schopny dostatečně čelit novým výzvám

V dnešním složitém digitálním prostředí stávající pravidla neposkytují

- **potřebnou úroveň harmonizace,**
- **nezbytnou účinnost pro zajištění práva na ochranu osobních údajů**

Ochrana údajů se mění podle zásady od
„od teorie k praxi“

Svět kolem nás se změnil

Novými výzvami současné společnosti v oblasti ochrany osobních údajů jsou:

- **rychlý pokrok a rozvoj technologií**
- **rostoucí globalizace**

„Stručně řečeno, zdravý rozum není pramenem práva. Avšak výklad by se jím měl určitě řídit. Bylo by nanejvýš nešťastné, kdyby se ***ochrana*** osobních údajů měla přeměnit na ***obstrukci*** prostřednictvím osobních údajů.“

GENERÁLNÍ ADVOKÁT CJEU MICHAL BOBEK ve svém Stanovisku ve Věci C-13-16, předneseném dne 26. ledna 2017

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) - též „GDPR“

Platnost: 25. 5. 2016 Účinnost: 25. 5. 2018

Úřední věstník Evropské unie L119, 4. května 2016

Revoluce nebo evoluce v ochraně osobních údajů?

GDPR vytváří tlak na změnu chování, zvyšuje povědomí o ochraně údajů

Řada institucí jmenovala Pověřence pro ochranu údajů – nikoliv z právní povinnosti, ale jako integrující prvek mezi byznysem, technologiemi a právním prostředím

Cíle a zásady dosavadní Směrnice 95/46/ES nadále platí

Nařízení 2016/679 je postaveno na základech dosavadní legislativy

- posiluje práva subjektů údajů
- uplatňuje přístup založený na posuzování rizik
- posiluje pravomoci dozoru
- stanovuje přísnější sankce

Nebezpečí při uplatňování zásad a pravidel GDPR v praxi

velmi široký výklad

aplikační absolutismus

Odpovědnost správce

- povinnost správce přijmout
  - vhodná a účinná opatření k ochraně osobních údajů,

- povinnost doložit, že opatření jsou
  - aplikována
  - v souladu s nařízením (zákonem)

- opatření musí zohlednit
  - povahu, rozsah, kontext a účely zpracování a
  - riziko pro práva a svobody fyzických osob

GDPR ukládá povinnosti správcům, zpracovatelům, příjemcům osobních údajů – tj. subjektům, které jakkoliv nakládají (zpracovávají) osobní údaje fyzických osob

GDPR neukládá povinnosti vývojovým pracovištím, výrobcům, distributorům technických a sw produktů a prostředků pro zpracování údajů

Taková pracoviště však budou vystavena tlaku uživatelů, aby jejich produkty zohledňovaly požadavky GDPR a usnadnily práci koncovým uživatelům

- Privacy by Design - Privacy by Default
- Realizovat práva subjektů údajů (výmaz, přenositelnost, aktualizaci, …,)
- Zabezpečení a ochrana osobních informací
- Ohlašovací povinnost narušení bezpečnosti

Privacy by design (záměrná ochrana)
znamená **zabudovat soukromí** do specifikace, návrhu, činnosti a řízení daného systému, a do obchodního procesu.
Koncept PbD je založen na sedmi jednoduchých základních pravidlech:

1) Být raději pro-aktivní než re-aktivní;
2) Použít ochranu soukromí jako default nastavení;
3) Ochranu soukromí vložit již do návrhu;
4) Vyvarovat se záměně – soukromí *vers*. **bezpečnost;**
5) Poskytovat management dat po celý jejich životní cyklus;
6) Zajistit viditelnost a transparentnost údajů;
7) Být zaměřen na uživatele *(data subject's centric);*

Významným pozitivním přínosem GDPR z pohledu byznysu a je tzv. „přístup na základě rizik“ (risk-based approach)

= zatímco stanovená pravidla jsou stejná pro všechny, jejich aplikace v praxi je rozmanitá a závisí na úrovni rizika, které dané zpracování vytváří vůči soukromí jedinců

Pravděpodobnost a míra rizika vyplývá z

povahy, **rozsahu**, **kontextu a účelu**
zpracování

klíčový faktor při posuzování souladu zpracování s Nařízením

Přístup na základě rizik může být na jedné straně pokládáno jako nedostatek a vytvářet problémy nejistoty, avšak v praxi tento přístup dělá GDPR nejen efektivnější, ale také poctivější (férovější)

Revoluce nebo evoluce

v ochraně osobních údajů?

Povinnosti plynoucí z Nařízení

- analyzovat dopady na současné zpracování údajů

- stanovit postupy pro jejich realizaci

- docílit souladu v roce 2018

Nové zásady při ochraně údajů:

- odpovědnost správce
- zpracování osobních údajů dětí
- zákaz profilování
- právo na přenositelnost údajů (a další práva s.ú.)
- záměrná a standardní ochrana o.ú. (PbD privacy by design, privacy by default)
- společní správci
- ohlašování a oznamování případů narušení bezpečnosti
- posuzování dopadu na ochranu údajů (Data Protection Impact Assessment - DPIA)
- jmenování pověřence pro ochranu údajů
- kodexy chování
- posílení orgánu dozoru
- pravidla pro sankce
- Evropská rada pro ochranu údajů

Povinnosti správce v oblasti bezpečnostní politiky a opatření:

- **vedení** předepsané dokumentace,
- **splnění** požadavků bezpečnosti,
- **vypracování** posouzení dopadu na soukromí,
- **provedení** konzultací s orgánem dozoru,
- **jmenování** pověřence ochrany údajů,
- **ověření** účinnosti všech opatření nezávislým auditorem

zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob

Zásady zpracování

Osobní údaje musí být:

- zpracovávány korektně a zákonným a transparentním způsobem (zásada „zákonnosti, korektnosti a transparentnosti“)

- shromážděny pro určité, výslovně vyjádřené a legitimní účely; údaje nesmí být dále zpracovávány pro účely neslučitelné s původním účelem (zásada „omezení účelem“)

- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování (zásada „minimalizace údajů“)

Zásady zpracování

- přesné a v případě potřeby aktualizované; nepřesné údaje opravit nebo vymazat (zásada „přesnosti“)

- uloženy ve formě umožňující identifikaci po dobu nezbytnou pro naplnění účelu; uchovávat po delší dobu – účel archivace ve veřejném zájmu, vědecký a historický výzkum, statistický (zásada „omezení uložení“)

- zpracovány způsobem, který zajistí náležité zabezpečení údajů, jejich ochranu pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním, před náhodnou ztrátou, zničením nebo poškozením (zásada „integrity a důvěrnosti“)

Správce odpovídá za dodržení zásad a musí být schopen to doložit (zásada „odpovědnosti“)

Zákonnost zpracování

Zpracování osobních údajů je zákonné pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- subjekt údajů udělil souhlas se zpracováním svých údajů pro jeden či více konkrétních účelů;

- zpracování je nezbytné pro plnění smlouvy , jejíž smluvní stranou je s.ú., nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost s.ú.

- zpracování je nezbytné pro splnění právní povinnosti, které podléhá správce;

- zpracování je nezbytné pro ochranu životně důležitých zájmů s.ú.;

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

- zpracování je nezbytné pro uskutečnění oprávněných zájmů správce za podmínky , že tyto zájmy nepřevažují nad zájmem nebo základními právy a svobodami subjektů údajů, vyžadujícími ochranu o.ú., zejména pokud je subjektem údajů dítě.
To se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Správce

…. sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

Zpracovatel

…. správce využije pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování údajů splňovalo požadavky GDPR

…. nezapojí do zpracování žádného dalšího zpracovatele bez povolení správce

… se řídí (písemnou) smlouvou , která jej zavazuje vůči správci. Smlouva stanoví předmět, dobu trvání, povahu a účel zpracování, typ údajů, kategorie s.ú., povinnosti a práva

Záměrná a standardní ochrana údajů
Ochrana údajů již od návrhu (Privacy by design)

1. S ohledem na technické možnosti a na náklady provedení, přijme správce

v době určování prostředků zpracování
při samotném zpracovávání

vhodná technická a organizační opatření a postupy tak, aby dané zpracování splňovalo požadavky nařízení a zaručovalo ochranu práv subjektu údajů

Záměrná a standardní ochrana o.ú.

2. Správce přijme opatření, aby zajistil, že **standardně** se budou zpracovávat **pouze** ty o.ú., které jsou pro každý konkrétní účel zpracování **nezbytné**

Povinnost **minimalizace** se týká:
- **množství** shromážděných údajů
- **rozsahu** zpracování
- **doby** jejich uložení / uchovávání
- **dostupnosti** údajů

Tato opatření zajistí, že o.ú. se nebudou standardně zpřístupňovat neomezenému počtu fyzických osob

Standardní nastavení ochrany údajů
při vývoji a koncipování produktů, služeb a aplikací

- zohledňovat právo na ochranu údajů

- posoudit možnosti současného stavu techniky

Bezpečnost zpracování

Správce a zpracovatel přijmou po vyhodnocení rizik opatření, aby ochránili osobní údaje před náhodným či nepovoleným zničením nebo před náhodnou ztrátou a aby předešli jakýmkoli nepovoleným formám zpracování, zejména nedovolenému sdělování či šíření osobních údajů, přístupu k nim nebo jejich pozměnění

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 příslušnému, ledaže 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

DPIA

Posuzování dopadu na ochranu údajů

Data Protection Impact Assessment (DPIA)

Jestliže je zpracování údajů kvůli své povaze, rozsahu nebo účelu spojeno s pravděpodobnými specifickými riziky z hlediska práv a svobod subjektů údajů, správce nebo zpracovatel posoudí dopad plánovaného zpracování na ochranu osobních údajů (DPIA)

DPIA je efektivní nástroj pro informování managementu o všech rizicích při zpracování údajů

DPIA může také pomoci při přijímání opatření a rozhodnutí k předcházení „pohromy“ při ochraně soukromí

Kdy se musí DPIA provádět?

- při návrhu legislativních opatření
- před zahájením zpracování (v souladu s DP by design)
- při jakýchkoliv změnách zpracování osobních údajů

  před zavedením nových IT systémů pro zpracování údajů

  před významnými změnami v systémech pro zpracování údajů, např. při:

  - stanovení nového účelu zpracování údajů
  - novém způsobu či prostředcích zpracování údajů
  - jakýchkoliv změnách dosavadního modelu zpracování údajů

Jakákoliv data, která jsou shromažďována v informačních systémech, musí být adekvátně chráněna pomocí bezpečnostních opatření

Pro zajištění důvěrnosti a ochrany osobních informací, správce a zpracovatel musí přijmout vhodná technická a organizační opatření pro ochranu před náhodnou či ilegální kompromitací osobních údajů, nebo jejich ztrátě, změnám, neautorizovanému přístupu, zveřejnění apod.

Vztah mezi DPIA a bezpečnostními opatřeními

Pro zajištění souladu s Nařízením při operacích s údaji, které mohou znamenat rizika (nebo vysoká rizika) pro práva a svobody s.ú. provede správce posouzení DPIA a výsledek posouzení zohlední při rozhodování o vhodných bezpečnostních opatřeních

U vysokých rizik opatření konzultuje s dozorovým úřadem

Pověřenec pro ochranu o.ú. (DPO)
jedna z nejvíce diskutovaných a problémových změn

- povinné nebo dobrovolné?
- jaké kritérium zvolit pro povinnost mít Pověřence?

Původní Návrh Nařízení (2012): *čl. 35 b) - zpracování provádí podnik zaměstnávající 250 či více osob*

- na jaké subjekty se vztahuje?

Jmenování DPO není věc nová –
čl. 18 odst. 2 směrnice 95/46/ES umožňoval jmenovat DPO;

převzato z německého modelu:
mají jej všechny unijní instituce a také některé členské státy EU

Studie International Association Privacy Professionals (IAPP) o potřebě DPO ve světě

(podle podílu míry globálního obchodu s EU bude ve světě potřeba 75 000 DPO)

USA 9,000	(míra obchodu – 17,1 %)
Čína 7,568	Švýcarsko 3,682
Rusko 3,068	Turecko 2,045
Norsko 1,790	Japonsko 1,688

Práva subjektů údajů

Právo na přístup k údajům

Právo na opravu

Právo na přenositelnost údajů

Právo vznést námitku

Automatizované individuální rozhodování

Právo být zapomenut a právo na výmaz

Právo na omezení zpracování

Vedoucí dozorový úřad (one-stop-shop)

- je úřad státu v němž má správce/zpracovatel hlavní nebo jedinou provozovnu

- dozorové úřady spolupracují navzájem; též s Komisí

- spolupracuje s ostatními dozorovými úřady v konsensu

- předkládá příslušným dozorovým úřadům návrh rozhodnutí ve věci, požádá je o stanoviska

Sankce

Členské státy stanoví pravidla pro sankce, jež se budou ukládat za porušení tohoto nařízení, a podniknou všechna opatření, která jsou zapotřebí k zajištění jejich provádění.

Stanovené sankce musí být účinné, přiměřené a odrazující.

Orgán dozoru uloží pokutu až do výše 20 000 000 EUR, nebo v případě podniků, až do výše **4%** jejich celkového ročního obratu celosvětově za předchozí rozpočtový rok.

Sankce

za porušení povinností správce nebo zpracovatele:

- osobní údaje dětí,
- DPIA a standardní ochrany,
- zabezpečení zpracování,
- ohlašování případů porušení zabezpečení,
- povinná konzultace s dozorem,
- jmenováním a činností pověřence, aj.

orgán dozoru uloží pokutu až do výše 10 000 000 EUR, nebo v případě podniků, až do výše **2%** jejich celkového ročního obratu celosvětově za předchozí rozpočtový rok

Diskuse, dotazy