



Edu brief pro Americkou obchodní komoru

Nařízení EU o ochraně osobních údajů ve 20 otázkách

16 února a 17 května 2016

Stanislav Bednář

1. Proč je kolem obecného nařízení EU o ochraně osobních údajů takový povyk?



- Jeden předpis, přímo aplikovatelný v 28 členských státech
- Nahrazuje směrnici o ochraně údajů z roku 1995 a národní předpisy transponující tuto směrnici
- Účinné od roku 2018, do této doby platí národní předpisy
- Základní důsledky: bude mít EU vedoucí úlohu v ochraně osobních údajů?

2. Bylo již přijato? Jsou toto konečná pravidla?



- **Poslední týden 2015**
 - 17. prosince 2015: EP LIBE podpořil texty přijaté v trojstranných rozhovorech
 - 18. prosince 2015: COREPER schválil konečný kompromisní text.
- **Jaro 2016**
 - právně-jazykové kontroly textů
 - přijetí evropskou Radou a parlamentem
 - zveřejnění v Úředním věstníku 4. května 2016
 - nařízení platí od 25. května 2016
- **2016-2017**
 - delegované/prováděcí předpisy
- **Jaro 2018**
 - nabytí účinnosti předpisů od 25. května 2018

3. Na koho se vztahuje?



- Zpracování osobních údajů v souvislosti s **aktivitami správce nebo zpracovatele usazenými v EU** bez ohledu na to, zda ke zpracování dochází v EU.
- Zpracování osobních údajů **subjektů údajů v EU** správci a zpracovateli **neusazenými v EU**, kdy zpracování souvisí s **nabídkou zboží či služeb** subjektům údajů v EU **bez ohledu** na to, zda je po subjektu údajů požadována **platba**, nebo v souvislosti s **monitorováním chování** takových subjektů údajů, pokud se odehrává v rámci EU.

4. Zůstanou platné stávající principy nebo se začíná znovu?



- Údaje musí být zpracovány **v souladu se zákonem, spravedlivě a transparentně**.
- Údaje musí být zpracovány pro **určitý, výslovný a legitimní účel** a nemohou být dále zpracovány jiným způsobem.
- Zpracovávané údaje musí být **přiměřené, relevantní a omezené** vzhledem k tomu, co je potřebné pro stanovený účel.
- Údaje musí být zpracovány způsobem, který zajišťuje **vhodné zabezpečení** použitím vhodných technických a organizačních opatření

A nový princip: Správce nese odpovědnost a musí **být schopen prokázat soulad své činnosti** s uvedenými principy.

5. Jak vysoké pokuty lze očekávat?



- Odstupňovaný přístup – **maximálně do 4% světového obratu.**
- S přihlédnutím např. k:
 - **povaze, závažnosti a trvání** přestupku;
 - **úmyslnému charakteru** přestupku;
 - **stupni odpovědnosti** (narušení ochrany údajů záměrné nebo opomenutím) nebo jakémukoliv relevantnímu **předchozímu přestupku**;
 - **spolupráci s dozorovým orgánem** (a způsob jakým se dozorový orgán o přestupku dozvěděl);
 - **kategorie osobních údajů**, kterých se to týká;
 - **další přitěžující nebo polehčující okolnosti** (např. finanční prospěch, apod.)

6. Bude dotčeno mezinárodní předávání údajů?



- Stejná filozofie jako předtím, tj. jen za velmi přísných podmínek:
 - rozhodnutí Komise o **přiměřenosti**.
 - **vhodné záruky**, jako např. standardní doložky o ochraně údajů přijaté Komisí nebo dozorovým orgánem nebo smluvní ujednání dozorovým orgánem;
 - **výjimky**: výslovný souhlas/nutné pro plnění smlouvy/...
 - a co povinnosti týkající se **zpřístupnění** informací?
 - *„Jakýkoliv rozsudek soudu a jakékoliv rozhodnutí správního orgánu třetího státu požadující po správci nebo zpracovateli přenos nebo zpřístupnění osobních údajů může být uznané a vykonatelné jen pokud tak vyplývá z mezinárodní smlouvy, jako je dohoda o vzájemné právní pomoci.“*

7. Bude potřeba jmenovat pověřence ochrany údajů?



- Ano i ne! – pověřenec musí být jmenován, pokud základní aktivity správce / zpracovatele:
 - vyžadují pravidelné a systematické **monitorování subjektů údajů velkého rozsahu**;
 - spočívají ve zpracování „**zvláštních kategorií údajů**“ (čl. 9) nebo údajů souvisejících s **odsouzením za trestné činy a přestupky** v širokém měřítku.
- Společnosti ve skupině mohou jmenovat **jediného pověřence ochrany údajů**.
- Pověřenec ochrany údajů může být **zaměstnancem nebo konzultantem** (smlouva o poskytování služeb), který se bude zodpovídat nejvyššímu managementu.

8. Jak jednotná úprava ovlivní náš compliance program?



- Jednotná úprava relevantní pro jednáním s dozorovými orgány v souvislosti s **přeshraničním zpracováním**.
- Definice přeshraničního zpracování by mohla být upřesněna, přestože záměr je jasný.
- S ohledem na přeshraniční zpracování bude správce nebo zpracovatel spolupracovat jen s **hlavním orgánem dozoru (COMI)**.

9. Co dělat v případě narušení bezpečnosti dat?



- Oznámit neprodleně dozorovému orgánu a **je-li to možné do 72 hodin**, pokud narušení osobních údajů pravděpodobně neohrozí práva a svobody jednotlivců.
- Pokud není narušení oznámeno do 72 hodin, je třeba odůvodnit.
- **Subjekty údajů musí být informovány neprodleně**, pokud hrozí, že únik ohrozí jejich práva a svobody, aby jim bylo umožněno provést potřebná opatření.
- Oznámení subjektu údajů není v určitých případech vyžadováno

10. Můžeme dále zpracovávat údaje na základě souhlasu?



- Ano, **ale**:
 - souhlas by měl být dán **svobodně**, být **konkrétní**, **informovaný** a **jasný**;
 - **prohlášením** nebo **jasným potvrzujícím jednáním**;
 - správce nese **důkazní břemeno**.
- V praxi např. zaškrtnutím políčka,
- Plnění smlouvy nesmí být podmiňováno souhlasem, pokud zpracování údajů není nezbytné.

11. Můžeme dále zpracovávat údaje na základě oprávněného zájmu?



- Ano – **s některými změnami:**
 - povinnost informovat subjekty údajů.
 - subjekt údajů má právo požadovat omezení ve zpracování údajů v průběhu ověřování, zda základní práva nepřevyšují oprávněné zájmy.
- **Příklady:** předcházení podvodům; zajišťování informační bezpečnosti.
- Bude přímý marketing považován za oprávněný zájem?

12. Budou sbírání údajů od dětí nezákonné?



- Ne – použijí se obecné principy zákonnosti zpracování (čl. 6).
- **Zpracování osobních údajů dítěte mladšího 16 let vyžaduje souhlas rodiče** (nebo jiného zákonného zástupce).
- Členské státy mohou snížit věkovou hranici (ale ne na méně než 13 let).
- Správce musí vynaložit **rozumné úsilí na ověření**, zda byl souhlas dán zákonným zástupcem dítěte: berou se v úvahu dostupné technologie.

13. Získají jednotlivci nová práva?



- Ano – několik nových respektive rozšířených práv.
- **Přenositelnost** údajů.
- **Omezení** zpracování.
- Rozšířené právo na výmaz – **právo být zapomenut**.
- Práva související s **profilováním**: *užívat údaje k vyhodnocení určitých osobních aspektů souvisejících s fyzickou osobou, zejména analyzovat nebo předvídat aspekty ohledně pracovního výkonu osoby, ekonomické situace, zdravotního stavu, lokalizace, osobních preferencí, zájmů, spolehlivosti nebo chování.*

14. Získáme nový typ citlivých údajů?



- **Obecné pravidlo** - zákaz zpracovávat osobní údaje odhalující:
 - rasový nebo etnický původ, politické názory, náboženské nebo filozofické vyznání, členství v odborové organizaci, **genetické údaje**, **biometrické údaje** za účelem jednoznačné identifikace osoby nebo údaje ohledně zdraví nebo pohlavního života či sexuální orientace.
- Ale platí **10 výjimek** (výslovný souhlas, apod.)
- **Pozor!**
 - členské státy mohou zavést další podmínky a omezení zpracování genetických údajů, biometrických údajů nebo zdravotních údajů.

15. Uplatní se Nařízení, pokud data anonymizujeme?



- Informace, která nesouvisí s identifikovanou nebo identifikovatelnou fyzickou osobou nebo údaje dané anonymně takovým způsobem, že subjekt údajů není nebo nebude identifikovatelný, **nebude předmětem Nařízení**.
- Údaje, které prošly **pseudonymizaci**, ovšem které mohou být přiřaditelné fyzické osobě s použitím dodatečných informací, jsou osobními údaji, které jsou předmětem Nařízení.
- K určení, zda je osoba identifikovatelná, by měly být **rozumně využity** všechny prostředky vzhledem ke všem **objektivním** faktorům jako jsou náklady a požadovaný čas, dostupná technologie v době zpracování a technologický vývoj.

16. Kdy bude potřeba provést posouzení dopadů na soukromí?



- Při použití nových technologií s možným rizikem pro práva a svobody jednotlivců, zejména:
 - **systematické a rozsáhlé vyhodnocování osobních aspektů založené na automatickém zpracování** (včetně profilování) a na základě kterých jsou činěna rozhodnutí výrazně ovlivňující jednotlivce.
 - **rozsáhlé zpracování zvláštních (nikoli citlivých) druhů údajů nebo údajů v trestních věcech.**
 - **systematické monitorování veřejně přístupného prostoru** v širokém měřítku.
- Dozorový orgán zveřejní seznam operací, které budou (a nebudou) předmětem posouzení dopadů.
- Přezkum posouzení dopadů při změně rizik.

17. Vždy jsme jednali jako zpracovatel – jaká bude naše odpovědnost?



- **Přímé nároky:** subjekt údajů může podat stížnost přímo proti zpracovateli (správní i soudní).
- **Kvalifikovaná odpovědnost:** zpracovatel bude odpovědný za škodu způsobenou zpracováním **jen** v případě, že nesplnil povinnosti z tohoto Nařízení přímo určené zpracovateli nebo jednal mimo či v rozporu se zákonnými instrukcemi správce.
- **Důkazní břemeno:** správce nebo zpracovatel bude zproštěn odpovědnosti, pokud dokáže, že není odpovědný za škodnou událost.
- **Odpovědnost za pověřené osoby:** pokud pověřený zpracovatel nesplní své povinnosti při ochraně údajů, zpracovatel zůstává plně odpovědným správcem za pověřeného zpracovatele.

18. Je pravda, že bude rozpuštěna G29?



- Nezávislý orgán EU s právní osobností – **Evropský sbor pro ochranu osobních údajů** – bude ustaven.
- **Nahradí** Pracovní skupinu dle čl. 29.
- Zmocněn vydávat závazná rozhodnutí.
- Rozhodnutí mohou být předmětem žaloby pro neplatnost k Soudnímu dvoru EU.

19. Vydají zákonodárci doporučení?

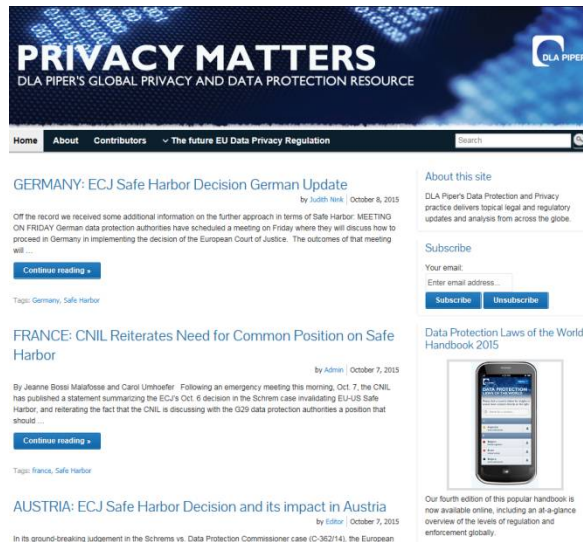


- Komisi bude svěřena pravomoc Nařízení implementovat.
 - **prováděcími předpisy:**
 - schválené kodexy chování;
 - technické standardy pro certifikační mechanismy a ochranu údajů;
 - rozhodnutí o přiměřenosti třetích států;
 - **delegovanými předpisy:**
 - informace zobrazované piktogramy;
 - požadavky pro certifikaci ochrany údajů.

20. Jak daleko harmonizace ve skutečnosti zajde?



- Právo členského státu řeší konflikt mezi **svobodou projevu či právem na informace** na jedné straně a ochranou osobních údajů.
- Právo členského státu nebo kolektivní smlouvy mohou zavést pravidla ohledně **zpracování osobních údajů zaměstnanců**,
- Členský stát může přijmout specifické předpisy, pokud je to třeba k urovnání rozporu mezi právem na ochranu osobních údajů a **povinnosti profesní mlčenlivosti**.



Přihlašte se na náš **Privacy Matters blog**
pro pravidelné novinky

<http://blogs.dlapiper.com/privacymatters/>

Přístup k
**Data Protection Laws of the World
Handbook** na
www.dlapiperdataprotection.com
Nové vydání bude v roce 2016

