Brusel prináša revolúciu v oblasti ochrany osobných údajov

JUDr. Zuzana HEČKO, LL.M.

eFOCUS

ALLEN & OVERY

Obsah:

- Prečo by ste sa mali zaujímať o ochranu osobných údajov (OÚ)?
- Rozdiely medzi zákonom č. 122/2013 o ochrane osobných údajov, prijatou novelou zákona (účinnosť 15.4.2014) a návrhom nariadenia EK o ochrane OÚ
- Nová regulácia EK prináša prvky, ktoré doteraz neboli súčasťou právnej úpravy

© Allen & Overy 2014

1) Oplatí sa byť v súlade so zákonom?

HSBC Bank (2009)

Súhrnná pokuta vo výške **£ 3 200 000** za stratu údajov.

Bank of Scotland (2012)

Pokuta vo výške **£ 4 200 000** za neaktualizáciu údajov týkajúcich sa pôžičiek počas 7 rokov

© Allen & Overy 2014

1) Pokuty a medializácia incidentu

SONY Playstation (2011)

Spoločnosti ukradli dáta 77 miliónov hráčov a pri druhom útoku ukradli dáta ďalších 25 miliónov hráčov za čo bola udelená pokuta **£ 250 000**.

Zurich Insurance (2010)

Pokuta vo výške **£ 2 275 000** za stratu údajov v rámci outsourcingu do dcérskej spoločnosti.

© Allen & Overy 2014

1) Pokles ceny akcií (aj keď pokuta nie je uložená)

Global Payments (2012)

Po úniku dát 10 mil. zákazníkov VISA a MasterCard **cena akcií spoločnosti klesla o 9%**. Spoločnosť bola následkom incidentu odstránená zo zoznamu preferovaných poskytovateľov služieb väčšiny spoločností vo finančnom sektore.

© Allen & Overy 2014

1) Reputačné škody, extrateritorialita

Weltimmo s.r.o. (2012)

Pokuta **€ 37 500** za neoprávnené poskytnutie osobných údajov tretím stranám a neodstránenie osobných údajov na žiadosť dotknutých osôb

Národný Bezpečnostný Úrad SR (2006)

Uhádnuté prístupové heslo *“nbusr123“.*

Státní ústav pro kontrolu léčiv (2011)

Pokuta **CZK 2 300 000** za nelegálne vytvorenie databázy obsahujúce citlivé osobné údaje pacientov.

Komerční pojištovna, a.s. (2006)

Pokuta **CZK 3 000 000** za stratu disku ktorý obsahoval dáta o 700 000 klientoch.

© Allen & Overy 2014

2) Zmeny

Zákon č. 122/2013

- Zákon o ochrane osobných údajov (OU)
- Účinný od 1.7.2013

Novela zákona

- Mení a dopĺňa zákon č.122/2013
- Účinná od 15.4.2014

Návrh nariadenia EK

- Návrh nariadenia prijatý EK vo februári 2012 (COM(2012)11)
- 12.3.2014 prijatý Európskym parlamentom v 1. čítaní (pozmenené bolo postúpené Rade)

© Allen & Overy 2014

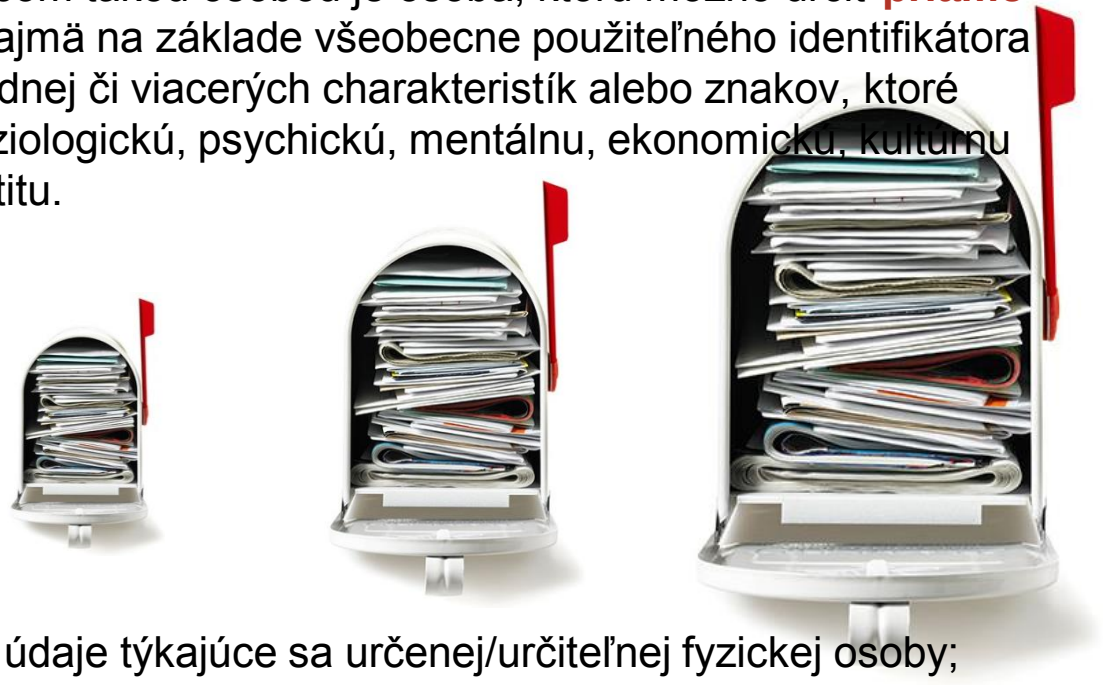
2) Definícia osobného údaju

Zákon č. 122/2013

§4(1) Osobnými údajmi **sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby**, pričom takou osobou je osoba, ktorú možno určiť **priamo alebo nepriamo**, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Novela zákona

Bez zmien



Návrh nariadenia EK

Článok 4(1) OÚ sú údaje týkajúce sa určenej/určiteľnej fyzickej osoby; určiteľná osoba je osoba, ktorú možno určiť priamo alebo nepriamo...

Odôvodnenie 24 This Regulation should be applicable to processing involving identifiers provided by devices, applications, tools and protocols, such as **Internet Protocol addresses, cookie identifiers and Radio Frequency Identification tags, unless those identifiers do not relate to an identified or identifiable natural person.**

© Allen & Overy 2014

2) Biometria

Zákon č. 122/2013

Novela zákona

Návrh nariadenia EK

§4(3)(f) biometrický údaj je OÚ fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej **je jednoznačne a nezameniteľne určiteľná**. Biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny.

– Metodické usmernenie Úradu na ochranu OÚ (aj biometrický podpis alebo chôdza)
– Zvýšené bezpečnostné opatrenia
– Osobitná registrácia

Bez zmien (zákon nerozlišuje medzi silnou a slabou biomertriou)

Článok 4(11) 'biometric data' means any personal data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data.

© Allen & Overy 2014

2) Registrácie informačných systémov

Zákon č. 122/2013

- **§34-42** zákona
- Registrácia - **€20**
- Osobitná registrácia - **€50**

Novela zákona

- Online oznámenie **€0** (registrácia je zrušená)
- Osobitná registrácia **€50** (nie pre OÚ spracúvané na základe §10 ods. 3 písm. g (legitímne záujmy prevádzkovateľa) napr. zabezpečenie bezpečnosti prostredníctvom kamier, monitorovanie zamestnancov, „whistleblowing schemes“ atď.
- Lehoty na rozhodnutie podľa správneho poriadku

Návrh nariadenia EK

- **Článok 39** zavádza možnosť dobrovoľnej certifikácie, ktorá bude fungovať ako „značka kvality“
- European Data Protection Seal (max. 5 rokov)
- Verejný register udelených certifikácií

© Allen & Overy 2014

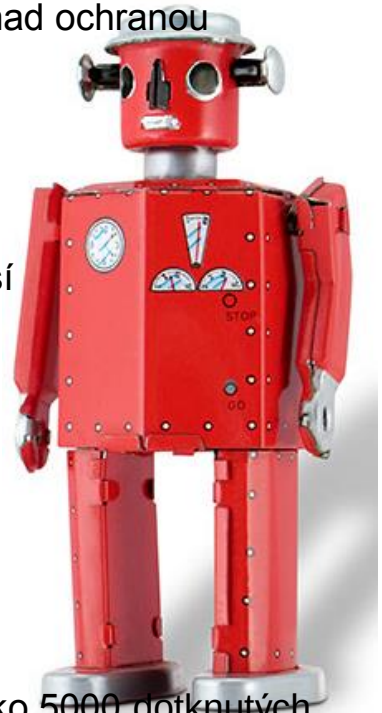
2) Zodpovedná osoba

Zákon č. 122/2013

- **§23(2)** Ak prevádzkovateľ **spracúva OÚ prostredníctvom 20 a viac oprávnených osôb, je povinný** . . . písomne poveriť zodpovednú osobu (ZO) alebo viaceré ZO
- **§24(1)** Fyzická osoba môže byť poverená výkonom dohľadu nad ochranou osobných údajov ako ZO po úspešnom **absolvovaní skúšky**.
- Štatutárny orgán nemôže pôsobiť ako ZO
- Pokuta pre ZO do výšky EUR 3000

Novela zákona

- Nominácia ZO je **fakultatívna** (ak je ale nominovaná ZO, musí absolvovať skúšku)
- ZO môže byť aj štatutárny orgán
- **„Bonzácke ustanovenia“ aj pokuty pre ZO zrušené**



Návrh nariadenia EK

- **Článok 35(1)**
- Nominácia ZO bude povinná ak sú spracovávané OÚ o viac ako 5000 dotknutých osobách počas 12 mesiacov, ak spracúvanie zahŕňa systematické monitorovanie osôb, alebo ak sú spracúvané citlivé OÚ, lokalizačné údaje, údaje o deťoch alebo o zamestnancoch v obsiahlych informačných systémoch.
- EÚ nepozná koncept skúšky

© Allen & Overy 2014

2) Požiadavky na bezpečnosť

Zákon č. 122/2013

- **§19-20: za bezpečnosť osobných údajov zodpovedá prevádzkovateľ.** Minimálny rozsah Bezpečnostných opatrení **je stanovený vyhláškou Úradu č. 164/2013 o rozsahu a dokumentácii bezpečnostných opatrení**.
- Bezpečnostné opatrenia prevádzkovateľ zdokumentuje v:
  (a)Bezpečnostnej smernici,
  alebo
  (b) Bezpečnostnom projekte.

Novela zákona

- Zrušuje sa povinnosť vypracovať bezpečnostnú smernicu.

Návrh nariadenia EK

- **Článok 30** – bezpečnostné opatrenia musia reflektovať „state of the art“ a náklady zavedenia (costs of implementation)

- Detaily budú upresnené European Data Protection Board-om

© Allen & Overy 2014

2) Pokuty sú likvidačné

Zákon č. 122/2013

– **§68** pokuty ukladané **obligatórne** až do výšky **€ 300 000**

Novela zákona

– Pokuty ukladané **fakultatívne** (okrem najzávažnejších porušení) do výšky **€ 200 000**

Návrh nariadenia EK

– **Článok 79(2a):** Sankcie:

1) Písomné upozornenie
2) Pravidelné audity (kontroly)
3) Pokuty až do výšky **€ 100 mil.** alebo až do **5%** ročného globálneho **obratu** spoločnosti.

© Allen & Overy 2014

2) Súhlas so spracovaním

Zákon č. 122/2013

- **§4 ods. 3 písm. d)**: súhlasom dotknutej osoby akýkoľvek **slobodne daný výslovný a zrozumiteľný** prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.
- Preukázateľný súhlas (**§11**)

Novela zákona

Bez zmien

Návrh nariadenia EK

Článok 4(8), odôvodnenia 25 a 57

- Súhlas musí byť daný **explicitne** (tick-box, vyhlásenie a pod.)
- Súhlasom nebude **mlčanie, pasivita alebo samotné používanie služby**
- Ak sa má súhlas poskytnúť na základe elektronickej žiadosti (napr. pop-up window) informácia musí byť jasná, výstižná a nezaťažujúca pre užívateľa
- Ak má dotknutá osoba **právo nesúhlasiť**, toto právo jej musí byť špecificky umožnené a musí byť **jasne oddelené** od iných informácií

© Allen & Overy 2014

2) Notifikácia incidentov regulátorovi

Zákon č. 351/2011

– § 56 ods. 5 **zákona o elektronických komunikáciách**: podnik je pri porušení ochrany osobných údajov povinný bezodkladne oznámiť Úradu pre reguláciu elektronických komunikácií a poštových služieb **porušenie ochrany OÚ**, bezodkladne **informovať účastníkov a užívateľov** o porušení a **viesť zoznam prípadov porušení** ochrany OÚ, ktorý obsahuje podstatné skutočnosti spojené s týmito porušeniami, ich následky a prijaté opatrenia na nápravu.

Novela zákona

– **Zákon o informačnej bezpečnosti** (draft doposiaľ nezverejnený)

Smernica NIS & Nariadenie

– **Smernica o informačnej bezpečnosti** (Smernica NIS): **Nahlasovacia povinnosť** len pre **závažné incidenty** (majúce vplyv na kontinuitu služby, bezpečnosť, spôsobujúca závažné porušenia). Aplikuje sa na **energetiku, transport, bankovníctvo a finančné služby, internet exchange points, zdravotníctvo, zásobovanie** a pod. Vyňaté sú cloud computing, e-commerce platformy, internetové vyhľadávače, verejný sektor.

– **Nariadenie EK na ochranu OÚ**: „bezodkladné“ nahlásenie incidentu (znamená do 72 hodín, odôvodnenie 67 Nariadenia)

© Allen & Overy 2014

© Allen & Overy 2014

3) Právo byť zabudnutý a právo na výmaz

– Pôvodná verzia EK (článok 17): „Právo byť zabudnutý a právo na výmaz“. Verzia pozmenená EP: „Právo na výmaz“

– Okrem nutnosti **vymazať dáta**, povinnosť vymazať všetky linky a kópie ak už nie sú potrebné pre účel, dotknutá osoba vzala súhlas späť, na základe rozhodnutia súdu, ak sa jednalo o nezákonné spracúvanie a pod.

– Smeruje voči prevádzkovateľom ako **aj voči tretím osobám**

– **Znemožnenie prístupu k dátam** (nie výmaz): v prípade keď je presnosť dát otázna, keď už nie sú dáta potrebné pre pôvodný účel ale musia byť uchované ako dôkaz, na základe rozhodnutia súdu alebo keď technológia neumožňuje výmaz (a bola inštalovaná predtým ako Nariadenie vstúpilo do účinnosti ☺)

– Kontroverzné rozhodnutie Súdneho dvora EÚ v prípade Google Španielsko

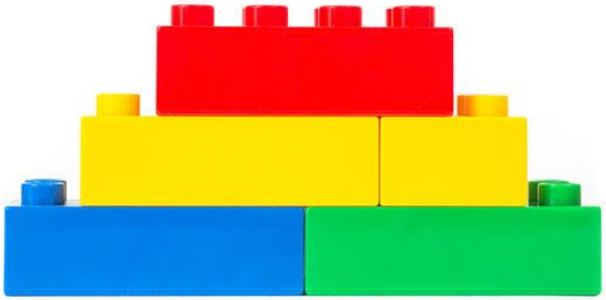
© Allen & Overy 2014

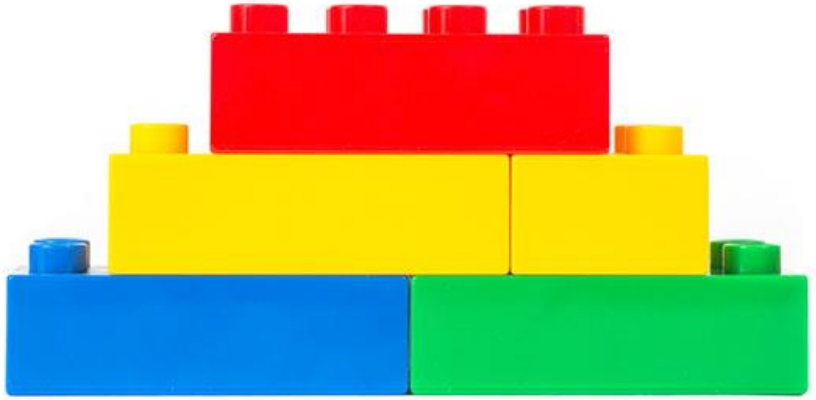
3) Špecifická ochrana údajov detí

– Článok 8, odôvodnenie 29: špecifická úprava pri spracúvaní OÚ detí do 13 rokov

- Ak je spracovanie založené na súhlase, tak súhlas musí byť udelený rodičom alebo poručníkom

- Informácie musia byť poskytnuté v jazyku, ktorý je primeraný pre deti





© Allen & Overy 2014

3) Povinnosť vypracovať „hodnotenie dopadov“

– Články 32a, 33, 33a a odôvodnenia 60, 71a, 74, 74a: **povinnosť vykonávať „analýzu rizík“ pre určité operácie s OÚ** v periodických intervaloch, **aspoň raz ročne** (alebo pri podstatnej zmene spracúvania)

– Spracovateľské operácie, ktoré v sebe potenciálne nesú riziko sú napr. spracúvanie OÚ o viac než 5000 dotknutých osobách počas 12-mesačného obdobia, spracúvanie citlivých údajov, lokalizačných údajov, údaje detí, profilovanie a mnoho ďalších

– Bude potrebné nominovať ZO a **vypracovať „hodnotenie dopadov“** (*impact assessment*). Vypracovanie „hodnotenia dopadov“ je možné združovať podľa príbuzných účelov, obsah detailne je určený Nariadením.

– **„*Compliance review*“** (revízia súladu so zákonom) bude musieť byť vykonávané každé 2 roky

© Allen & Overy 2014

3) Ďalšie

– Špecifické ustanovenia ohľadne spracúvania **OÚ týkajúcich sa zdravia**: články 4(12) a 81, odôvodnenie 122a

– Špecifické ustanovenia o **profilovaní** a nutnosti nesúhlasiť s profilovaním: článok 20

– EP prijal 12.3. 2014 rezolúciu, ktorou žiada **zrušenie „Bezpečného prístavu“** (Safe Harbor) pre prenosy OÚ do USA

– **Územná pôsobnosť**: **extrateritorialita** (článok 3, odôvodnenie 20)

Nariadenie sa bude aplikovať bez ohľadu na to, či spracúvanie je V EÚ alebo mimo EÚ (aplikácia aj v prípade ponuky tovaru do EÚ, a to bez ohľadu či je vyžadovaná platba) a v prípade monitorovania dotknutých osôb v EÚ

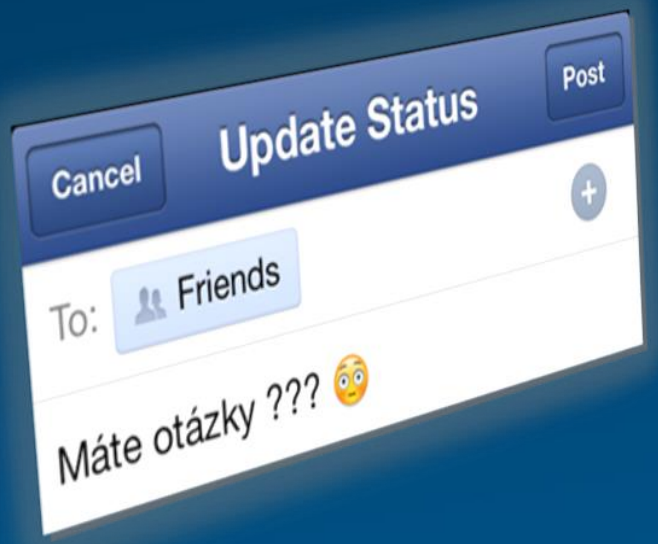
– **...a mnoho ďalších...**

© Allen & Overy 2014

„Dôležité je neprestať sa pýtať.
Zvedavosť má svoj vlastný dôvod existencie.“

Albert Einstein

Zuzana Hečko
Advokátka, Allen & Overy Bratislava, s.r.o.
Tel: +421 (2) 5920 2438
Fax: +421 (2) 5920 2424
zuzana.hecko@allenovery.com



Tento dokument je všeobecný informačný dokument a nepredstavuje konkrétne poradenstvo. V tomto dokumente pojem Allen & Overy znamená Allen & Overy LLP a/alebo jej spriaznené osoby. Slovo partner sa používa na označenie člena Allen & Overy LLP, zamestnanca alebo konzultanta s obdobným postavením a kvalifikáciou, prípadne osoby s obdobným štatútom v jednej zo spriaznených osôb Allen & Overy LLP.

eFOCUS

© 2010 Digit, s.r.o.