

Současnost s budoucnost ochrany osobních údajů



Logo partnera

Návrh na novou evropskou legislativu na ochranu údajů

Karel Neuwirt

konzultant pro ochranu osobních údajů

Komisař Rady Evropy 2007-2012

Logo partnera



Ochrana osobních údajů v Evropě

EU: Směrnice 95/46/ES o ochraně jednotlivců s ohledem na zpracování osobních údajů a o volném pohybu těchto údajů (Brusel, 24. 10. 1995)

Rada Evropy: Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat
(ETS 108, Štrasburk 28. 1. 1981)

Směrnice 95/46/ES

- **Milník v historii ochrany osobních údajů v EU**
- **Dva hlavní cíle směrnice v evropském integračním procesu:**
 - ochrana základních práv a svobod jednotlivců
 - dosažení vnitřního obchodu (volný pohyb osobních údajů, odstranění překážek při pohybu údajů)
- **Harmonizace legislativy členských států v oblasti ochrany osobních údajů**

20 let stará směrnice 95/46 (1995)
34 let stará Úmluva 108 (1981)
nejsou schopny dostatečně čelit novým výzvám

Stále zůstávají v platnosti cíle Úmluvy a směrnice

- zajistit fungování jednotného trhu a účinnou ochranu základních práv a svobod fyzických osob.

V dnešním novém, složitém digitálním prostředí však stávající pravidla neposkytují ani potřebnou úroveň harmonizace, ani nezbytnou účinnost pro zajištění práva na ochranu osobních údajů.

EU potrebuje mnohem podrobnější a
propracovanější politiku o ochraně základních práv
a osobních údajů

Rada Evropy usiluje, aby se modernizovaná Úmluva
108 stala celosvětovým standardem

Zásada „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

Edvard Snowden



*Národní bezpečnostní
agentura*

zveřejnil informace o rozsáhlých programech sledujících hlasové i datové komunikace Američanů i cizinců, včetně hlav a vlád spřátelených států.

Toto odhalení činnosti NSA vyvolalo rozsáhlou debatu o rovnováze mezi soukromím a bezpečnostními ohledy, na které se odvolávají špionážní služby.

Změna pohledu politiků EU

5 oblastí změny pohledu na ochranu soukromí

1. Politikové byli přinuceni **otevřeně hovořit** o sledovacích systémech
2. Změna **veřejného mínění** a pohledu na sledování osob
3. Zvýšilo se **povědomí** o hodnotě osobních informací
4. Problematice ochrany soukromí se více věnují **média**
5. **Evropa začala konat** – Evropský soudní dvůr prohlásil směrnici 2006/24/ES *(o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí)* za neplatnou a v rozporu s evropským právem

Nový přístup v EU

- Vliv **nových technologií** na soukromí
- Zvýšení důležitosti ochrany údajů ve vnitřním trhu EU = zlepšení **úrovně harmonizace** legislativy pro ochranu údajů
- Díky **globalizaci** je nutno zkvalitnit legislativu pro přenos dat přes hranice států = zjednodušit a odstranit byrokracii
- **Přísnější institucionální dozor** nad dodržováním zákonů a pravidel pro ochranu údajů = posílení úlohy dozorových orgánů
- Zlepšení soudržnosti právního rámce pro ochranu soukromí = potřeba dosažení **zastřešujícího právního instrumentu**, aplikovatelného na zpracování údajů ve všech sektorech a všech oblastech v EU

Návrh Nařízení EP a Rady

**o ochraně fyzických osob v souvislosti se
zpracováním osobních údajů a o volném pohybu
těchto údajů (obecné nařízení o ochraně údajů)**

COM(2012) 11 final, Brusel 25.1.2012

Návrh Nařízení obsahuje 91 článků a 139 vysvětlujících komentářů

Při projednávání v EP bylo předloženo na 4 tisíce pozměňovacích návrhů a připomínek

Komise – Parlament - Rada

EK - 25. 1. 2012 publikován návrh Nařízení

EP - 13. 3. 2014 schválena upravená verze

Rada - Návrh nyní projednává Rada EU

Návrh přináší zpřesnění dosavadního předpisu (Směrnice) a řadu nových principů a ustanovení.

Přijetí Nařízení se očekává v období 2015 /2016

– je vhodná doba se na novou legislativu připravovat!!

Nové princípy ochrany údajů

- definice (osobní údaj, biometrický a genetický údaj, ...)
- odpovědnost správce
- ohlašování případů narušení bezpečnosti
- zpracování osobních údajů dětí
- ochrana o.ú. již od návrhu (privacy by design)
- posuzování dopadu na ochranu údajů (Data Protection Impact Assessment)
- jmenování inspektora ochrany údajů
- jeden dozorový úřad (One-Stop-Shop)
- kodexy chování
- práva subjektů údajů
- posílení orgánu dozoru
- pravidla pro sankce a jejich výše
- Evropská rada pro ochranu údajů

Definice

„subjekt údajů“ - identifikovaná fyzická osoba nebo FO, kterou lze přímo nebo nepřímo, *samotnou či ve spojení s přiřazenými údaji*, identifikovat *nebo zjistit* prostředky, o nichž lze důvodně předpokládat, že je správce nebo jakákoli jiná fyzická nebo právnická osoba použije pro identifikaci dané osoby, zejména s odkazem na *jedinečný identifikátor* (identifikační číslo), lokalizační údaje, elektronický identifikátor nebo s odkazem na jeden či více zvláštních prvků její fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální nebo *genderové identity* nebo *sexuální orientace*

„osobní údaj“ - veškeré informace o subjektu údajů

Biometrika a osobní údaj

„biometrický údaj“ – znamená osobní údaj získaný ze specifického technického zpracování týkajícího se fyzických či fyziologických charakteristik nebo charakteristik chování jedince, které umožňují nebo potvrzují jeho jednoznačnou identifikaci (např. snímky obličeje nebo daktyloskopické údaje)

Ve verzi schválené EP je biometrický údaj považován za citlivý osobní údaj. V dosavadní verzi Rady toto není uvedeno (SK požaduje doplnit)



ANO, DOBA SE MĚNÍ, BERU SI RUKAVICE,
ABYCH NA PULITRU NEZANECHAL OTISK SVĚHO PALCE...

KRESBA: MIROSLAV KEMEL

Odpovědnost správce

1. Přijmout politiku a provedení vhodných opatření k zajištění zpracování o.ú. v souladu s Nařízením; schopnost tuto skutečnost prokázat

2. Opatření zahrnují zejména:

- a) vedení dokumentace
- b) provedení požadavků týkajících se bezpečnosti údajů
- c) vypracování posouzení dopadu na ochranu údajů
- d) splnění požadavků ohledně předchozího povolení nebo předchozí konzultace orgánu dozoru
- e) jmenování inspektora ochrany údajů

3. Zavést mechanismy pro ověření účinnosti provedených opatření. Je-li to přiměřené, provede ověření nezávislý interní nebo externí auditor

Odpovědnost správce je všeobecná a zajišťuje větší podporu organizaci při stanovení a zavádění odpovědnostní politiky zajišťující lepší ochranu osobních informací. Procedury zpracování údajů musí být v souladu s nařízením.

Tato povinnost má dvě části:

- přijetí vhodných a efektivních opatření k ochraně osobních údajů;
- doložení (dozorovému orgánu), že opatření jsou aplikována.

Společní správci

Kde správce určuje účel, podmínky a prostředky zpracování osobních údajů **společně s ostatními**, určí společní správci ve vzájemném ujednání, jakou odpovědnost každý z nich nese za plnění povinností vyplývajících z tohoto Nařízení, zejména pokud jde o postupy a mechanismy pro výkon práv subjektu údajů.

Zaměstnanci a pracovníci

musí být dobře obeznámeni:

- s otázkami soukromí,
- s legislativou pro ochranu údajů,
- s bezpečnostními opatřeními a
- s analýzou možných rizik vůči soukromí jednotlivců

Ohlašování případů narušení bezpečnosti

(viz Nařízení Komise (EU) 611/2013, 24.6.13)

Správce ohlásí orgánu dozoru narušení bezpečnosti osobních údajů, a to bez zbytečného odkladu, a je-li to možné, nejpozději **do 24 hodin** od chvíle, kdy toto narušení zjistil.

Zpracovatel je povinen informovat / upozornit správce o narušení bezpečnosti osobních údajů.

Zpracování osobních údajů dítěte

V souvislosti s nabídkou služeb informační společnosti přímo dítěti je pro účely tohoto nařízení zpracování osobních údajů dítěte **mladšího 13 let** zákonné pouze tehdy a do té míry, pokud byl souhlas vyjádřen nebo schválen rodičem dítěte nebo jeho zákonným zástupcem. Správce vyvine přiměřené úsilí o získání ověřitelného souhlasu s ohledem na dostupné technologie.

Ochrana údajů již od návrhu

(Privacy by design)

S ohledem na stav techniky a náklady provedení přijme správce **při určování prostředků zpracování a při samotném zpracovávání** vhodná technická a organizační opatření a postupy tak, aby dané zpracování splňovalo požadavky tohoto nařízení a zaručovalo ochranu práv subjektu údajů

Posuzování dopadu na ochranu údajů

(Data Protection Impact Assessment)

Posuzování dopadu na ochranu údajů (soukromí) může plnit úlohu „systému včasného varování“.

Efektivní nástroj pro informování managementu o všech rizicích při zpracování údajů.

Může také pomoci při přijímání opatření a rozhodnutí k předcházení pohromy při ochraně soukromí.

PRO-AKTIVNÍ PŘÍSTUP

Nenahrazuje povinnost auditů zaměřených na ochranu soukromí/údajů

Inspektor pro ochranu osobních údajů

ve státních úřadech povinně (může být sdílen více úřady)

právnícké osoby

- při zpracování údajů **o 5 tisících osobách za rok**, nebo
- hlavní činnost správce nebo zpracovatele obsahuje zpracování, které vyžaduje pravidelné a systematické monitorování osob, nebo
- při hlavní činnosti jsou zpracovávány citlivé osobní údaje, lokalizační údaje, údaje o dětech nebo údaje o zaměstnancích v rozsáhlých systémech

Zřízení této pozice může být polehčující okolností při rozhodování o sankci

Práva subjektů údajů

Informování subjektu údajů

Právo subjektu údajů na přístup k údajům

Právo na opravu

Právo na výmaz / Právo být zapomenut

Právo na přenositelnost údajů

Právo vznést námitku

Opatření založená na profilování

Podmínky vyjádření souhlasu

Důkazní břemeno **nese správce**.

Souhlasy pro různé skutečnosti musí být vzájemně **odlišitelné**.

Souhlas lze kdykoli **odvolat**.

Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.

Souhlas nepředstavuje právní základ pro zpracování – při značné nerovnováze postavení mezi subjektem údajů a správcem.

Získání souhlasu subjektu údajů bude náročnější.

Přednastavený souhlas nebude uznán za platný – musí být vyjádřena aktivní vůle.

Právo být zapomenut a právo na výmaz

Subjekt údajů má právo požadovat od správce výmaz osobních údajů a zdržení se dalšího šíření těchto údajů:

zejména v souvislosti s osobními údaji, které subjekt údajů zpřístupnil v dětském věku, pokud je splněn alespoň jeden z následujících důvodů:

- a) údaje již nejsou potřebné pro účely, pro které byly shromážděny ;
- b) subjekt údajů odvolá svůj souhlas, nebo
vypršela lhůta pro uchovávání údajů a neexistuje žádný další právní důvod pro zpracování údajů;
- c) subjekt údajů vznesl námitku proti zpracování osobních údajů;
- d) zpracování údajů není slučitelné s Nařízením z jiných důvodů.



Soudní dvůr EU ve věci Google Spain *vers.* EDPS a M.C.González

(C-131/12, ze dne 13.5.2014)

- operátor internetového vyhledávače je odpovědný za zpracování (je tedy správcem);
- jedinec má právo žádat, aby ve výsledku vyhledávání nebyly informace o něm, pokud zasahují do jeho soukromí. Operátor musí zajistit odstranění odkazu (linku) na takové informace.

Opatření založená na profilování

EP: „profilování“ - *jakákoli forma automatického zpracování osobních údajů, skládající se z hodnocení určitých osobních aspektů vztahujících se k fyzické osobě, zejména k analýze či odhadu pracovního výkonu fyzické osoby, její ekonomické situace, zdraví, osobních preferencí nebo zájmů, spolehlivosti nebo chování, lokalizace nebo pohybu;*

- 1.** Každá FO má právo, aby se na ni nevztahovalo žádné opatření, jež má vůči ní právní účinky nebo se jí významně dotýká, provedené pouze na základě automatizovaného zpracování určeného k vyhodnocení jistých rysů její osobnosti nebo analýze či předpovídání zejména plnění pracovních povinností, ekonomické situace, lokalizace, zdravotního stavu, osobních preferencí, spolehlivosti nebo chování této fyzické osoby.
- 2.** Automatické zpracování údajů za účelem vyhodnocení určitých rysů osobnosti FO se nesmí opírat pouze o zvláštní kategorie údajů.

Členské státy stanoví pravidla pro sankce, jež se budou ukládat za porušení ustanovení tohoto nařízení, a podniknou všechna opatření, která jsou zapotřebí k zajištění jejich provádění, včetně případů, kdy správce nedodrží svou povinnost jmenovat zástupce. **Stanovené sankce musí být účinné, přiměřené a odrazující.**

Orgán dozoru uloží

- písemné varování
- pokutu do výše 250 000 € nebo 0,5% ročního obratu
- pokutu do výše 500 000 € nebo 1,0% ročního obratu
- pokutu do výše 1 mil. € nebo 2% ročního obratu

Orgán dozoru

- pravomoci
- vzájemná spolupráce a pomoc
- účast na společných operacích
- jediné kontaktní místo (One-Stop Shop)
- nezávislost
- zvyšování povědomí veřejnosti

Evropská rada pro ochranu údajů

WP 29



Evropská rada + nové pravomoci

Otevřené problémy

Některé oblasti zpracování osobních údajů však nejsou v Nařízení řešeny (zůstávají v pravomoci států):

- národní bezpečnost
- žurnalistika a svoboda projevu
- zaměstnanost
- profesionální mlčenlivost
- odposlechy komunikací

Děkuji za pozornost

karel.neuwirt@centrum.cz

Logo partnera

