Obecné nařízení o ochraně osobních údajů aktuálně

Magistrát města Brna

11. 1. 2018

JUDr. Soňa Matochová, Ph.D.


8 data protection principles
1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection
ico.
Information Commissioner's Office

Osnova prezentace

- Proč je v současné době aktuální ochrana osobních údajů ?
- Je naše právo na soukromí dotčené v digitálním věku?
- Potřebujeme chránit naše soukromí? Jak to lze udělat?
- Kdy se vůbec Evropa začala zajímat o ochranu osobních údajů?
- Jak je to s právní úpravou osobních údajů v ČR?
- Jak lze charakterizovat připravovanou právní úpravu?
- Na jakých zásadách je založena? Do jaké míry je shodná s předcházející právní úpravou? Na koho se vztahuje?
- Co pro vás může Úřad pro ochranu osobních údajů udělat v souvislosti s novým nařízením?
- Dotazy a diskuse

Význam ochrany osobních údajů

„**Účinná ochrana údajů je zcela zásadní pro naši demokracii a je nosným pilířem pro další základní práva a svobody,“** (Viviane Redingová, místopředsedkyně Komise a komisařka odpovědná za spravedlnost, základní práva a občanství.)

- **„Potřebujeme nalézt rovnováhu mezi obavami o narušení soukromí a volným pohybem informací, který napomáhá tvorbě ekonomických příležitostí.“**

O jaká práva se jedná v oblasti ochrany osobních údajů?

Čl. 8 Listiny základních práv EU

Ochrana osobních údajů

- **1. Každý má právo na ochranu osobních údajů, které se ho týkají.**

- **2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.**

- **3. Na dodržování těchto pravidel dohlíží nezávislý orgán.**

O jaká práva se jedná v oblasti ochrany osobních údajů?

Čl. 16 Smlouvy o fungování EU

1. **Každý má právo na ochranu osobních údajů, které se jej týkají.**

2. Evropský parlament a Rada přijmou řádným legislativním postupem pravidla o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Dodržování těchto pravidel podléhá kontrole nezávislými orgány.

O jaká práva se jedná v oblasti ochrany osobních údajů?

Listina základních práv a svobod ČR

- **Právo na nedotknutelnost osoby a jejího soukromí**

(čl. 7 odst. 1)

- **Právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života**

(čl. 10 odst. 2)

- **Právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě**

(čl. 10 odst. 3)

Vývoj právní úpravy v Evropě v časové posloupnosti

Úmluva Rady Evropy o ochraně jednotlivců s ohledem na automatizované zpracování dat (Úmluva č. 108)

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Právní úprava ochrany osobních údajů v ČR

Zákon č. 101/2000 Sb., o ochraně osobních údajů

POZITIVNÍ PŮSOBNOST (§ 3 ZOOÚ)

Z. se vztahuje na osobní údaje, kt. zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby;

z. se vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky;

Právní řád ČR se použije přednostně na základě MPV, i když správce není usazen na území ČR;

Správce, kt. je usazen mimo území EU a provádí zpracování na území ČR, pokud se nejedná pouze o předání osobních údajů přes území EU.

Obecné nařízení o ochraně osobních údajů

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)

Charakteristika nařízení

- Kontinuita (zásady a klíčové instrumenty)
- Přesnější a podrobnější úprava práv subjektu údajů
- Propracovanější a náročnější pravidla pro správce a zpracovatele
- Sjednocený nezávislý dozor
- Prováděcí unijní i vnitrostátní předpisy, omezení rozsahu povinností/práv předpisy

Základy konstrukce ochrany osobních údajů v ON

- Zásady zpracování osobních údajů (rozšířené)
- Záměrná a standardní ochrana
- Přístup založený na riziku
- Panevropský (EU) dosah
- Nezávislý dozor
- Vymahatelnost

Zásady zpracování osobních údajů

- zákonnost, korektnost a transparentnost
- účelové omezení
- minimalizace údajů
- přesnost (osobních údajů)
- omezení uložení
- integrita a důvěrnost
- odpovědnost

Nové nástroje ochrany

- Pověřenec pro ochranu osobních údajů
- Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a oznamování téhož dotčeným subjektům údajů
- Mechanismus jediného kontaktního místa
- Mechanismus jednotnosti

Definice pojmů

Osobní údaj

veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, 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;

Definice pojmů

Zpracování

jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je 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;

Definice pojmů

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; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

Definice pojmů

Zpracovatel

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

Definice pojmů

Příjemce

fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

Definice pojmů

Souhlas subjektu údajů

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

Definice pojmů

Genetické údaje

osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

Definice pojmů

Biometrické údaje

osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

Definice pojmů

Údaje o zdravotním stavu

- osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

Definice pojmů

Pseudonymizace

zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě

Sjednocení dozoru

- Obecné nařízení výslovně upravuje nezávislost, podmínky pro členy, úkoly a pravomoci (vč. vyšetřovacích) dozorových úřadů a vzájemnou spolupráci dozorových úřadů,

- Evropský sbor pro ochranu osobních údajů jako subjekt Unie s právní subjektivitou k dosahování jednotnosti v prosazování a vymáhání pravidel (mechanismus jednotnosti)

- Jednotné sankce (podmínky ukládání správních pokut s horní hranicí 20 mil. EUR, nebo - pouze u podniků - 4% ročního obratu za předchozí finanční rok)

Pověřenec pro ochranu osobních údajů
KDE MUSÍ BÝT JMENOVÁN?

Pověřenec musí být organizací jmenován, pokud:

- zpracování provádí **orgán veřejné moci či veřejný subjekt** (bez ohledu na to, jaká data jsou zpracovávána)

- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují **rozsáhlé pravidelné a systematické monitorování subjektů údajů**

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

- Ostatní organizace mohou pověřence jmenovat dobrovolně na základě vlastního uvážení

Pověřenec pro ochranu osobních údajů
JAKÉ KVALIFIKAČNÍ PŘEDPOKLADY MUSÍ SPLŇOVAT?

GDPR stanovuje pro obsazení role pověřence, že

"…musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39."

Pověřenec na ochranu osobních údajů POŽADAVKY

Požadavky stanovené Pracovní skupinou WP29 :

- znalost národního a unijního práva v oblasti ochrany dat a hluboké znalosti Obecného nařízení (GDPR)
- praktické zkušenosti aplikace požadavků ochrany dat
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat
- znalost dané oblasti podnikání a organizace
- schopnost propagovat kulturu ochrany dat v organizaci

Děkuji za pozornost!