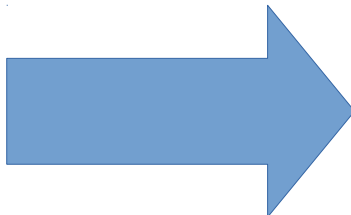


GDPR

Co je GDPR?

Zákon č. 101/2000 Sb.,
o ochraně osobních údajů
=
„ZOOÚ“

25. května 2018



Nařízení Evropského Parlamentu
a Rady EU č. 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
=
„GDPR“

Proč to?

- Dosavadní laxnost zpracovatelů
- Nadužívání a zneužívání souhlasů s lecčím
- Vydírání a monopol poskytovatelů služeb
- Zvýšení povědomí
- Max pokuta *10 mil. Kč* → *20 mil. €*
Rekordman:
2016: T-mobile **3,6 mil. Kč** za krádež **dat 1,2 mil. zákazníků**

Příklad Google

Co je osobní údaj

- = **veškeré informace o identifikované nebo identifikovatelné fyzické osobě (viz nařízení)**

„veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou osobou je osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na **jméno, identifikační číslo, lokační údaje, síťový identifikátor** nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo jiné společenské identity.“

- **Zvlášť citlivá data**

rasa/etnikum, náboženství, politické názory, genetika, biometrika, sexuální život/orientace, údaje dětí

- Pseudonymizace, sekundární identifikátory, zúžení výběru
- Netýká se právnických osob

Role

- **Subjekt**
- **Správce (může být zpracovatelem)**
FO nebo PO (orgán, agentura, ...), který sám nebo společně se zpracovatelem určuje účely a prostředky zpracování OÚ.
- **Zpracovatel (externí)**
FO nebo PO (orgán, agentura, ...), který pro správce technicky provádí zpracování.
- **Pověřenec (tzv. DPO)**
Monitoruje soulad, provádí interní audit, školí zaměstnance.
- **Dozorový úřad (ÚOOÚ)**
Dozoruje, přijímá podněty, poskytuje konzultace.

Zásady!

- Zákonnost, transparentnost
- Nezbytný rozsah pro daný účel
- Transparentnost
- Přesnost – právo na opravu
- Časové omezení uložení
- Důvěrnost, odpovědnost, adekvátní zabezpečení – schopnost toto i doložit!

Vše se přitom vede v rozumných mezích a při nejlepším svědomí a vědomí.

Právní tituly pro zpracování

- **Souhlas** (lze kdykoliv odvolat!)
- **Plnění smlouvy**
- **Právní povinnost**
- **Životně důležité zájmy** (např. při ošetření)
- **Veřejný zájem** nebo při výkonu veřejné moci
- Nezbytné pro účely **oprávněných zájmů** správce

Souhlas se zpracováním OÚ

- Srozumitelný
- Přiměřený
- Svobodný (samostatně, nezávisle, odmítnutelně)
- Vědomý (opt-in)
- Prokazatelný
- Pokud současně získané souhlasy nebyly již tehdy v souladu s GDPR, je třeba je do 2 let obnovit

Pozn:

Opt-out režim podle § 7 odst. 3 zákona č. 480/2004 Sb. spočívá v tom, že pokud podnikatel získá v souladu s právními předpisy na ochranu osobních údajů od svého zákazníka jeho elektronický kontakt v souvislosti s prodejem výrobku nebo služby, může využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jeho vlastních obdobných výrobků nebo služeb i bez výslovného souhlasu zákazníka.

Odpovědnost správce

- **„S přihlédnutím k různě pravděpodobným a různě závažným rizikům přijmout vhodná technická a organizační opatření.“**
- Analýza rizik (zpravidla zpracovává vedení, najatý auditor, či pověřenec)
- Povinnost doložit, že zpracování je v souladu s GDPR
- Revize opatření
- **Povinnost hlášení úniků okamžitě, nejdéle však do 72h od zjištění na ÚOOÚ**

Práva subjektu

- Totožnost správce
- Kontaktní údaje pověřence
- Účely zpracování
- Kategorie dotčených OÚ
- Doba uložení OÚ
- Poučení o právech
- Právo na výmaz („být zapomenut“)
- Právo na opravu

Právo na přístup k vlastním OÚ

- Subjekt má právo získat od správce potvrzení tom, které jeho údaje a v jakém rozsahu správce zpracovává.
- Správce má povinnost subjektu údajů poskytnout kopii zpracovávaných osobních údajů.
- Za další kopie lze požadovat přiměřený poplatek.

Právo na výmaz

Kdy ano?

- Pokud již nejsou zapotřebí
- Po odvolání souhlasu
- Subjekt vznesl námitky proti zpracování
- OÚ byly zpracovány protiprávně



Kde všude mazat?

- Databáze
- Souborové systémy
- Emaily
- Lokální PC
- Přenosná média
- Spisové služby
- Zálohy

Kdy ne?

- Existuje právní důvod
- Převyšující oprávněné důvody
- Veřejný zájem



Nohy na stůl
(po sepsání vyjádření)

Co je třeba zlepšit?

- Nízké povědomí o existenci OÚ
- Příliš mnoho aplikací pro zpracování OÚ a cest vedení útoku
- Mnoho zpracovatelů a příležitostí k úniku
- Vést záznamy o zpracování (neplatí pro PO s <250 zam. v případě, že údaje nejsou citlivé)
- provádět posouzení dopadu na ochranu osobních údajů (DPIA)
- jmenovat pověřence pro ochranu osobních údajů (DPO)
- Oddělit z pracovních smluv zpracování údajů zaměstnanců, nepodléhajících zákonné povinnosti (např. Fotky) do formy souhlasu na samostatný dodatek. **To platí pro všechny souhlasy, udělené před platností a v nesouladu s GDPR do 2 let.**

Vztah správce a zpracovatele

- **Správce** může zpracováním osobních údajů **pověřit zpracovatele**.
- Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít **smlouvu o zpracování osobních údajů**.
- Pro zpracovatele platí uvedené povinnosti obdobně.

Liberace od sankcí

- **§ 8 odst. 5 TOPO:** Právnícká osoba se trestní odpovědnosti zprostí, pokud vynaložila veškeré úsilí, které na ní bylo možno spravedlivě požadovat, aby spáchání protiprávního činu zabránila.

TOPO = Trestní odpovědnost právnických osob

Praktická cvičení

Vžití se do role útočníka – penetrační testy

- Co by mohl útočník udělat, aby se dostal k datům?
- **Motivace** k útoku je irelevantní (stalking, snahy o poškození,)
- Současný zaměstnanec = krytí **smlouvou o utajení, omezení práv**
- **Předpokládat i znalost systému** (bývalý zaměstnanec)
- **Situace:** jsem brigádník-křivák a chci poškodit Frantu Vomáčku z vedlejšího kroužku, nebo alespoň jeho rodiče. Jaké jsou moje možnosti? Jak mi v tom systém zabrání?
- **Situace:** jsem pedofil a chci vědět, kam chodí do školy konkrétní dítě, které jsem viděl s twirling hůlkou před DDM.
- **Situace:** při autonehodě zemřela moje přítelkyně a soud osvobodil řidiče, jehož dítě chodí do DDM. Chci se mu pomstít a posílat anonymní dopisy s vypátranými údaji.
- **Situace:** DDM mě vyhodil pro „nesmyslné“ porušování pravidel. Způsobím mu škodu a nechám popotahovat za únik dat. Půjdu omrknout, co bych provedl.

Volně ležící „třídnice“

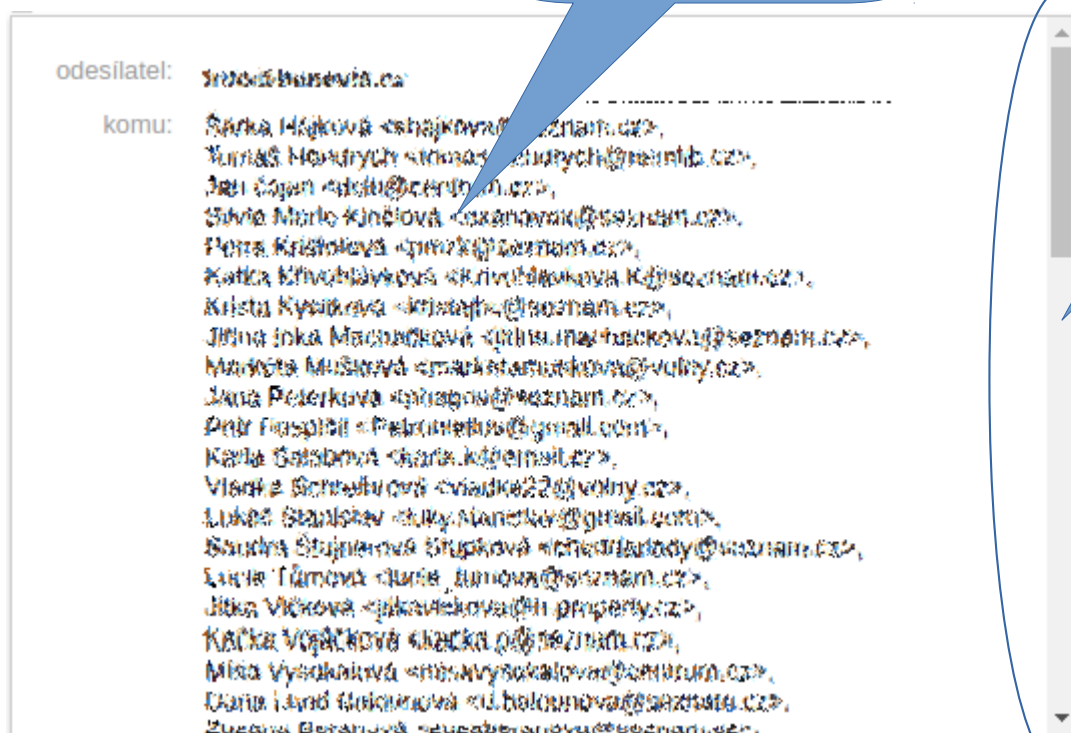
- Třídnice by měla být považována za soubor osobních údajů a neměla by se nechávat ležet bez dozoru.
- Třídnice by měla mít nenápadné desky pro případ „opuštění“.
- Měla by obsahovat jen nejnutnější údaje (jméno?), a zbytek v jiném dokumentu nebo v IS.
- Navrhoval bych úplné přesunutí třídnic do elektronického systému, jako to mají modernější ZŠ.

Volně přístupné kanceláře – hacker nemusí být jen programátor

- Odejdu např. na záchod = zamknu prázdnou kancelář
- Odcházím na oběd nebo domů = zamknu dokumenty do zamykatelné skříně
- Zamknu počítač (klávesová zkratka Win+L) (na PC musí být nastavené heslo)
- Účetní zpravidla používají šifrovací kartu

Hromadné emaily

Au!



Auuuu!

- Půlce města byl právě prozrazen váš email
- Druhá půlka ho získá tím, že jí bude přeposlán

ŘEŠENÍ:
Skrytá kopie ;)

Typický postup útoku pomocí řetězových emailů:

- 1) Vymyslím „přeposláníhodný email“ (pěkné fotky, nesmyslné zákony, udělej si test, 10 let neštěstí pokud nepřeпоšleš, nebezpečný virus se šíří, romové berou tajné dávky, ...).
- 2) Čekám, až ho podle zákona pravděpodobnosti někdo přepoše mě, jako součásti komunity.
- 3) Vyzobu si všechny emaily z přesměrování, můj program jim zkouší prolomit hesla podle slovníků nejběžnějších hesel
- 4) Po získání přístupu do některého emailu mám přístup např do: Google služby, Apple služby, školní IS, atd.; Většina uživatelů internetu navíc používá univerzální hesla ke všemu.
- 5) Prodej ukradené identity na černém trhu (cca 8\$ za 1 iTunes účet, a mnoho dalších komodit)

Co fotky?

- **Přímý marketing**
 - Lze považovat za **zpracování prováděné z důvodu oprávněného zájmu správce**
 - Musí být **přiměřený, neinvazivní, důvodné očekávání subjektu údajů**
 - Subjekt údajů musí být upozorněn na **právo vznést námitku**
- **Marketing na základě kvalifikovaného souhlasu subjekt údajů**
 - **Konkludentní v. kvalifikovaný souhlas**
 - **Informační povinnost**
 - Nenucení zákazníků k udělení souhlasu
 - **Archivace souhlasů**
- **Příklad z Finska: rozrastrování obličejů**
- **Příklad z Anglie: precedent – nelze vyjmout děti, kteří nesouhlasily**
- **Výjimka: reportážní účely – pokud je subjekt srozuměn, že je pořizován záznam (např. Pózuje), je to čistě pro účely reportáže ok; pro propagační účely však už není.**

Doporučená postup pro fotky

- Neuvádět jména!
- Obličeje rozrastrovat, nebo lépe nahradit smajlíky
- Pozor na odvolání souhlasu

