General Data Protection Regulation (GDPR)

Myšlienky tak dobré, až musia byť povinné

Alternatívny pohľad na problematiku GDPR, ktorý ste doteraz nevideli a nepočuli

NETHEMBA

NETHEMBA

Kto som?

- IT bezpečnostný expert (CISSP) zameraný na IT bezpečnosť s viac než 20 ročnou praxou (z toho 10+ rokov v mojej vlastnej IT security firme - Nethemba s.r.o.)
- Digitálna bezpečnosť je hlavným zameraním našej spoločnosti (www.chrantesvojesukromie.sk, www.chrantesvesoukromi.cz)
- Verím, že ľudia si zaslúžia absolútne digitálne súkromie (vrátane ochrany všetkých finančných transakcií)
- Voluntaryista - všetky vzťahy musia byť vzájomne dobrovoľné - nemôžeme dospelých ľudí do čohokoľvek proti ich vôli -> GDPR by malo byť vnímané ako konkurenčná výhoda a nie ako povinnosť vynucovaná štátom

NETHEMBA

Čo je GDPR?

- The General Data Protection Regulation (GDPR) (Regulácia (EÚ) 2016/679) je regulácia, ktorou Európsky Parlament, Rada Európskej Únie a Európska komisia posilňuje a zjednocuje ochranu dát pre všetkých občanov v rámci Európskej Únie (EÚ)
- Regulácia bola prijatá 27. apríla 2016. Vymožiteľnou sa stáva od 25. mája 2018
- Porušovanie pravidiel regulácie vás môže stáť pokutu až do 20 000 000 EUR alebo až do 4% z vášho ročného celosvetového obratu z predchádzajúceho finančného roka (v prípade podniku)

NETHEMBA

Je GDPR zlé?

Samozrejme, že v rámci GDPR existuje mnoho zaujímavých konceptov a myšlienok, ktoré by mohli zlepšiť zabezpečenie súkromia obyvateľov EÚ.

- Zásadné otázky však znejú:
  - Sú tieto súkromné / bezpečnostné opatrenia ekonomicky efektívne? Dávajú ekonomický zmysel?
  - Môžeme si z morálneho hľadiska dovoliť externalizovať náklady na GDPR na daňových poplatníkov alebo dátové subjekty / kontrolórov / spracovateľov bez ich súhlasu?
  - Môžeme morálne definovať nové práva a externalizovať všetky náklady na ich vynucovanie na daňových poplatníkov ?

NETHEMBA

GDPR zvyšuje náklady pre každého

- Predstavte si nasledujúcu situáciu:
  - Nízko-nákladová spoločnosť poskytuje svoje lacné služby alebo produkty zákazníkom, ktorí preferujú najnižšiu cenu namiesto ochrany súkromia
  - Pretože je GDPR v EÚ globálne vynucované aj pre malé spoločnosti s obmedzeným rozpočtom, zvýšia sa ich náklady a tým aj finálne ceny. Znamená to, že ich zákazníci, ktorí sa primárne zaujímali o najnižšiu cenu (nie súkromie) dostanú vyššie ceny
  - Je to spravodlivé voči týmto nízko-nákladovým spoločnostiam a ich klientom (ktorým je ich súkromie ľahostajné)?

GDPR berie ľuďom možnosť rozhodnúť sa medzi ochranou súkromia a inými benefitmi.

Ochrana súkromia je dôležité, avšak je nesprávne ho vynucovať u všetkých ľudí, obzvlášť ak sa množstvo z nich rozhodne ho vymeniť za iné výhody.

NETHEMBA

Kde sú hranice nášho súkromia?

- Mnoho regulácií vyžaduje od používateľa zbieranie dát a ich ochranu
- Nanešťastie možnosť "Nie, ďakujem. Neželám si vaše dáta" mnoho správcov dát neposkytuje
- GDPR by malo ľudí povzbudzovať k používaniu anonymných platobných kariet, anonymných SIM kariet,... kde sa znižuje riziko spojené s deanonymizáciou alebo únikom informácií
  - to je však zakázané zákonom AML (Anti Money Laundering legislation)
  - čo indikuje zjavnú kolíziu medzi GDPR a AML
- Vláda nám dovoľuje určitý druh anonymizácie, ale v obmedzenom rozsahu - aj napriek GDPR chce vláda monitorovať naše telefonáty alebo platby (kvôli "terorizmu" alebo "daňovým podvodom")

NETHEMBA

GDPR predstavuje nové "pozitívne" práva

"Pozitívne práva" - nie sú inciované vzájomnou zmluvou:

- Právo na prístup dotknutej osoby
- Právo na vymazanie / Právo byť zabudnutý
- Právo na nápravu
- Právo na obmedzenie spracovania
- Právo na prenos údajov
- Právo na námietku

Všetky náklady na "pozitívne práva" sú externalizované na daňových poplatníkov (bez ich súhlasu) a nemôžu byť potlačené dobrovoľnými vzájomnými dohodami(!)

Vždy, keď vytvárate nové pozitívne právo, vytvárate zároveň aj povinnosť pre daňových poplatníkov zaplatiť všetky náklady s ním spojené

NETHEMBA

Obrovské GDPR pokuty

GDPR umožňuje ukladať pokuty za niektoré porušenia:

- Až do výšky 4% z celosvetového ročného obratu a 20 miliónov eur (napr. porušenie požiadaviek, týkajúcich sa medzinárodných prevodov alebo základných princípov spracovania, ako sú podmienky pre súhlas)
- Až do výšky 2% z celosvetového ročného obratu a 10 miliónov eur (napr. chýbajúce šifrovanie, zanedbaná povinnosť pri notifikácii štátu/ klienta, chýbajúci úradník pre ochranu osobných údajov ..)

NETHEMBA

"Existenčná" hrozba GDPR pokút

Vytvára stimul pre medzinárodné spoločnosti k opusteniu prostredia EÚ, špeciálne v prípade, kedy sú ich interné náklady na dodržiavanie GDPR príliš vysoké, a vysoké pokuty v dôsledku nedodržiavania GDPR nevynútiteľné.

- Majú stále povinnosť chrániť občanov EÚ alebo platiť pokuty za ignorovanie tejto povinnosti, ale mimo EÚ môže byť technicky ťažké vymáhať akékoľvek sankcie
- Otázkou je - ako chce EÚ znemožniť, aby medzinárodné spoločnosti mimo EÚ museli chrániť on-line údaje zákazníkov EÚ bez toho, aby hrozilo riziko "cenzúry" pre všetky spoločnosti, ktoré to robiť podľa GDPR nebudú ?

Môžeme očakávať ďalšiu internetovú cenzúru všetkých internetových stránok medzinárodných spoločností poskytujúcich svoje produkty / služby občanom EÚ, ktorí sa rozhodnú neuplatňovať pravidlá GDPR?

(Áno, toto sa už v skutočnosti stalo so spoločnosťami na online hazard!)

NETHEMBA

Oznámenie o porušení

Riadiaci pracovníci musia nahlásiť väčšinu porušení priamo Úrad na ochranu osobných údajov. Nahlásenie musí byť vykonané bezodkladne a ak je to možné, tak do 72 hodín od varovania.

- Otázka znie "Je možné v tomto prípade veriť štátu"?
  - Podľa štatistík došlo k mnohým porušeniam a únikom informácií priamo v vrátane Slovenského národného bezpečnostného úradu(!)
  - Pre mnoho spoločností, ktoré nedôverujú vláde a jej schopnosti ochrániť dáta občanov, môže byť bezpečňejšie incidenty vôbec nenahlasovať (a riskovať s tým súvisiacu pokutu)
  - Nahlasovanie (=odhalenie tejto informácie vláde) môže byť rovnako reputačným rizikom (ako v prípade nedávneho Uber incidentu)

Vzhľadom na riziko poškodenia dobrého mena a neschopnosť vlády chrániť citlivé údaje občanov, môžu mnohé spoločnosti kalulovať s tým,

či ekonomicky dáva zmysel informovať štát o prípadných porušeniach alebo vôbec nie.

NETHEMBA

Šifrovanie vždy pomáha

Zapnutie šifrovania je v týchto dňoch jednoduché pre väčšinu počítačov, smartfónov, serverov a mnoho ďalších zariadení.

- Zvýši to váš súlad s GDPR
- Zníži strop najvyššej možnej pokuty, ktorú môže udeliť Úrad na ochranu osobných údajov
- V niektorých prípadoch vďaka nemu nemáte povinnosť notifikovať postihnutých používateľov v prípade porušenia (Úrad pre ochranu osobných údajov však treba kontaktovať)
- Ak vám skutočne záleží na súkromí vašich používateľov, všetko šifrujte

Mali by spoločnosti používať Tor/I2P siete & anonymné prehliadanie webových stránok?

NETHEMBA

GDPR "slobodný a výslovný súhlas" sa vzťahuje len na dotknuté osoby

- GDPR špecifikuje že"**Súhlas musí byť daný dobrovoľný, špecifický, informovaný, jednoznačný a EXPLICITNÝ**" od všetkých dotknutých osôb
- Nikto však nežiadal pracovníkov a spracovávateľov údajov o ich "dobrovoľný a slobodný súhlas" s GDPR legislatívou, ktorá je im vnútená bez ich súhlasu!

NETHEMBA

Právo na vymazanie / právo byť zabudnutý

Ďalšie "pozitívne právo", kde sú všetky náklady s ním spojené externalizované na daňových poplatníkov.

- Zbytočné v prípade, kedy je to možné riešiť vzájomnými dohodami medzi vlastníkmi údajov a správcami / spracovateľmi údajov
- Ak niektorí ľudia vyžadujú "byť zabudnutí", mali by preferovať takých správcov a spracovávateľov informácií, ktorí umožňujú zmazanie / zabudnutie osobných údajov
- Je nemorálne zabezpečovať a poskytovať toto právo a externalizovať výdavky na všetkých občanov, najmä ak väčšine je ochrana súkromia ukradnutá.

Ako chcete presadzovať legislatívu GDPR (najmä právo na zabudnutie), ak sa správcovia / poskytovatelia údajov rozhodnú šifrované údaje svojich používateľov ukladať do verejného blockchainu namiesto svojej lokálnej databázy?

Zakáže EÚ uchovávať akékoľvek citlivé dáta do verejného blockchainu?

NETHEMBA

Právo na prenos údajov

Ďalšie "pozitívne právo", kde sú všetky náklady s ním spojené externalizované na daňových poplatníkov.

Zbytočné v prípade, kedy je to možné riešiť vzájomnými dohodami medzi subjektami údajov a správcami / spracovateľmi údajov

- V prípade, že ľudia vyžadujú "prenesiteľnosť údajov" mali by prefereovať spracovávateľov údajov, ktorí takéto služby poskytujú - a samozrejme, toto by mala byť ich konkurenčná výhoda - nie je potrebné vynucovať takéto právo štátom(!)
- Je nemorálne vynucovať toto právo a externalizovať výdavky na všetkých občanov, najmä ak sa o to väčšina z nich nezaujíma.

NETHEMBA

Súkromie "by design" a "by default"

- Koncept "najmenších privilégií" (minimalizácia uložených / spracovávaných dát)
- GDPR podporuje"pseudonymizáciu" osobných údajov:
  - “Spracovanie osobných údajov takým spôsobom, že citlivé údaje už nie je možné priradiť konkrétnemu subjektu bez použitia ďalších informácií.”
- Čo tak úplne prestať používať bankové účty a prepnúť sa na skutočne anonymné kryptomeny (napríklad Monero)?
- Výrazne tak eliminujete riziko úniku citlivých informácií spojených s rizikom porušenia bankového účtu :-)

NETHEMBA

Sú anonymné kryptomeny "priateľské" s GDPR?

Dôvody:

- Anonymizujú finančnú situáciu občana
- Chránia proti úniku informácií z bankového účtu
- Minimalizujú počet potrebných citlivých parametrov v platbe

NETHEMBA

"Verejný záujem" v GDPR

Mnoho častí GDPR sa odvoláva na "verejný záujem". Ale neexistuje nič také, ako "záujem verejnosti"!

- **Ayn Rand:** Keďže neeexistuje nič také ako "verejnosť" s rovnakým názorom, pretože verejnosť je len niekoľko jednotlivcov, takže akýkoľvek konflikt "verejného záujmu" so súkromnými záujmami znamená, že záujmy niektorých ľudí musia byť obetované na úkor záujmov, či prianí ostatných. Pretože koncept je tak jednoznačne nedefinovateľný, jeho využitie spočíva len na danej schopnosti skupiny ľudí vyhlásiť že “The public, c’est moi” (Verejnosť som ja.)— a udržiavať si nárok pod hrozbou násilia.
- Legislatíva "verejného záujmu" (a akákoľvek distribúcia násilne zabavených peňazí človeka medzi ľudí, ktorí sa o ne nezaslúžili) sa zneužíva k uzurpovaniu si nedefinovanej, nedefinovateľnej, neobjektívnej, svojvoľnej moci niektorých vládnych činiteľov.

NETHEMBA

GDPR "nejasné" definície

- GDPR legislatíva obsahuje množstvo nejasných definícií:
  - "veľký objem dát", "veľké organizácie", "veľké množstvo zasiahnutých osôb"...
  - "primeraná" starostlivosť
- Nejasné definície v legislatíve vedú vždy ku korupcii a svojvoľnej interpretácii zo strany štátnych úradníkov.

NETHEMBA

GDPR obmedzuje “profilovanie”

A takisto dáva dátovým subjektom výrazné práva ako sa vyhnúť rozhodnutiam založeným na profilovaní.

- V súčasnej dobe väčšina väčších spoločností profiluje dáta automaticky (napr. pri cielenom marketingu, či cenotvorbe), vrátane všetkých sociálnych sietí
- Z technického hľadiska mže byť zložité zistiť, či je použité automatizované "profilovanie" (ste ako daňový poplatník, ochotný platiť štátnych úradníkov, aby vykonávali detekciu "automatizovaného profilovania" na všetkých weboch?)
- Nemalo by to byť regulované v žiadnom prípade štátom
- Pokiaľ existujú nejakí používatelia, ktorí nesúhlasia s automatizovaným profilovaním, mali by to byť tí, ktorí sú ochotní zaplatiť extra poplatok za služby, ktoré nevykonávajú automatické profilovanie a trh by im mal poskytnúť riešenie.

NETHEMBA

Záver

GDPR je príliš **komplexné** a **príliš drahé nariadenie** pre väčšinu firiem na to, aby ho dokázali správne a do hĺbky nasledovať. GDPR je nejasný, preto očakávajte korupciu s ním spojenú.

Nové technológie a metódy pomôžu spoločnostiam zachovať súlad s GDPR, rovnako ako poskytnú aj možnosť bojkotovať túto legislatívu bez rizika penalizácie. **GDPR má vyššiu prioritu** ako obojstranné dobrovoľné dohody medzi dátovými subjektami a správcami / spracovávateľmi.

GDPR **externalizuje všetky náklady** na daňových poplatníkov (tvorba a vynucovanie legislatívy) a dátových správcov / spracovávateľov, čo vedie k zvyšovaniu ich výdavkov vo všetkých situáciách (dokonca aj v tedy, keď ochranu súkromia nepokladá žiadna strana za prioritu)

Ďakujem za pozornosť!

NETHEMBA

info@nethemba.com