Všeobecné nariadenie o ochrane údajov

Pavol Sokol

10.05.2017

security.science.upjs.sk

GDPR

Nariadenie Európskeho parlamentu a Rady 2016/679 (všeobecné nariadenie o ochrane údajov, GDPR)

- účinnosť: **25.5.2018**

- predpoklad: nový zákon o ochrane osobných údajov

Základné zásady spracovania osobných údajov:

- zákonnosť, spravodlivosť a transparentnosť
- obmedzenie účelu
- minimalizácia údajov
- správnosť
- minimalizácia uchovávania
- integrita a dôvernosť

Zdroj: https://mspalliance.com/european-gdpr-explained-msps/
http://live.prolificnorth.co.uk/gdpr-is-creeping-closer/

Aké zmeny prináša GDPR?

Právny základ pre spracovanie osobných údajov

Rušia sa nasledujúce právne základy:

- právny základ podľa § 10 ods. 3 písm. d) ZoOOU „**priamy marketing v poštovom styku**“
- právny základ podľa § 10 ods. 3 písm. e) ZoOOU „**ďalšie spracúvanie už zverejnených osobných údajov**“
- právny základ podľa § 15 ods. 4 ZoOOU „**jednorazový vstup**“
- právny základ podľa § 15 ods. 7 ZoOOU „**monitorovanie priestorov prístupných verejnosti**“;

Zdroj: https://www.linkedin.com/pulse/professional-marketing-manager-kankanit-chutimaworaphan
http://www.zimcos.co.uk/services/cctv-installations/

Právny základ pre spracovanie osobných údajov

Nové právne základy

- bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné na **účely akademické, umelecké, literárne alebo žurnalistické účely.**

- Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený sprístupniť, poskytovať alebo zverejniť jej osobné údaje v rozsahu **titul, meno, priezvisko, pracovné, služobné alebo funkčné zaradenie, odborný útvar**, miesto výkonu práce, **telefónne číslo**, faxové číslo alebo **elektronická pošta** na pracovisko a identifikačné údaje zamestnávateľa ...

Zdroj: http://www.cep-probation.org/research-note/ https://blog.appery.io/2015/08/big-update-identity-integration-with-ldap-and-social-networks-new-ionic-components-angularjs-editor-upgrades-and-more/

Práva dotknutých osôb

Novou právnou úpravou sa rozšírili a spresnili jednotlivé práva dotknutých osôb, a to:

- právo na opravu
- **právo na výmaz (právo na zabudnutie)**
- právo na obmedzenie spracúvania
- **právo na prenosnosť údajov**
- právo namietať
- **právo namietať automatizované individuálne rozhodovanie a profilovanie**

Zdroj: https://www.howtogeek.com/221288/how-to-delete-a-table-in-word/

Zodpovedné osoby

- Čl. 37 ods. 1, písm. a) GDPR - spracúvanie vykonáva orgán verejnej moci alebo **verejnoprávny subjekt** s výnimkou súdov pri výkone ich súdnej právomoci

Zodpovedná osoba (Data protection officier, DPO):

- dobrá znalosť práva a ochrany osobných údajov
- nezávislosť
- monitoring + vzdelávanie
- zamestnanec / právnická osoba (napr. cez zmluvu o poskytovaní služieb)

Zdroj: http://aphaia.co.uk/en/data-protection-officer-outsourcing/

Oznamovanie bezpečnostných incidentov

Ktoré incidenty je potrebné oznámiť?

- porušenie ochrany osobných údajov (personal data breach)
- porušenie bezpečnosti

Kto musí oznamovať?

- každý prevádzkovateľ a sprostredkovateľ

Komu je potrebné incident oznámiť?

- Úradu na ochranu osobných údajov
- dotknutým osobám (niektoré prípady)

Do kedy je potrebné incident oznámiť?

- bez zbytočného odkladu, resp. do 72 hodín

Aké sú sankcie?

- 10 mil. € / 2% z globálneho ročného obratu spoločnosti

Zdroj: http://diginomica.com/2015/03/04/tackling-enterprise-digital-security-skills-crisis-22/

Súčasne bezpečnostné opatrenia

Zákon č.122/2013 Z.z. o ochrane osobných údajov

- primerané bezpečnostné opatrenia
- berúc do úvahy použiteľné technické prostriedky
- zabezpečiť aktualizáciu bezpečnostných opatrení

Vyhláška č.164/2013 Z.z.

- obsahuje zoznam konkrétnych bezpečnostných opatrení
- šifrovanie, firewall, pravidelné zálohovanie a pod.

Bezpečnostné opatrenia podľa GDPR

GDPR obsahuje požiadavky na:

- bezpečnosť spracúvania údajov (**všeobecné požiadavky**)
- štandardnú ochranu osobných údajov (**data protection by default**)
- špecificky navrhnutú ochranu osobných údajov (**data protection by design**)

Bezpečnosť spracúvania údajov

GDPR – čl. 32

Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom

- **na najnovšie poznatky**,
- **náklady na vykonanie opatrení**
- a na **povahu, rozsah, kontext a účely spracúvania**,
- ako aj **na riziká** s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb,

primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

- **pseudonymizácia a šifrovania** osobných údajov
- **trvalá dôvernosť, integrita, dostupnosť a odolnosť** systémov spracúvania a služieb (napr. AV ochrana, firewall)
- **včasná obnova** dostupnosti osobných údajov (napr. plán obnovy, zálohovanie údajov)
- **proces pravidelného** testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania

Štandardná ochrana osobných údajov

GDPR – čl. 25 (2) - data protection by default

- prevádzkovateľ vykoná **primerané technické** a **organizačné** opatrenia, aby zabezpečil, že štandardne sa spracúvajú len **osobné údaje**, ktoré sú **nevyhnutné** pre každý konkrétny účel spracúvania.

Uvedená povinnosť sa vzťahuje na:

- **množstvo** získaných osobných údajov,
- **rozsah** ich spracúvania,
- **dobu** ich uchovávania a
- ich **dostupnosť**.

Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje **neboli** bez zásahu fyzickej osoby **štandardne prístupné neobmedzenému počtu fyzických osôb.**

Špecificky navrhnutá ochrana osobných údajov

GDPR – čl. 25 (1) - data protection by design

prevádzkovateľ musí prijať **primerané technické** a **organizačné** opatrenia v čase:

- určenia prostriedkov spracúvania
- samotného spracúvania

vzhľadom na:

- najnovšie poznatky (state of the art)
- náklady na vykonanie opatrení
- povahu, rozsah, kontext a účely spracúvania osobných údajov
- riziká s rôznou pravdepodobnosťou a závažnosťou

Príklady:

- pseudonymizácia
- minimalizácia údajov

Anonymizácia vs. pseudoanonymizácia

Pseudoanonymizácia - je spracúvanie osobných údajov takým spôsobom, aby **osobné údaje** už **nebolo možné priradiť konkrétnej dotknutej osobe** bez použitia **dodatočných informácií**, ...

- primeraná pravdepodobnosť
- kľúč – oddelene od pseudoanonymizovaných osobných údajov

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx
Les	Mcv	xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx

Zdroj: http://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/

Posudzovanie vplyvu

- zvýšený štandard posudzovania rizík
- ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne **povedie k vysokému riziku** pre práva a slobody fyzických osôb, prevádzkovateľ **pred spracúvaním** vykoná **posúdenie vplyvu** plánovaných spracovateľských operácií na ochranu osobných údajov.

Prípady:

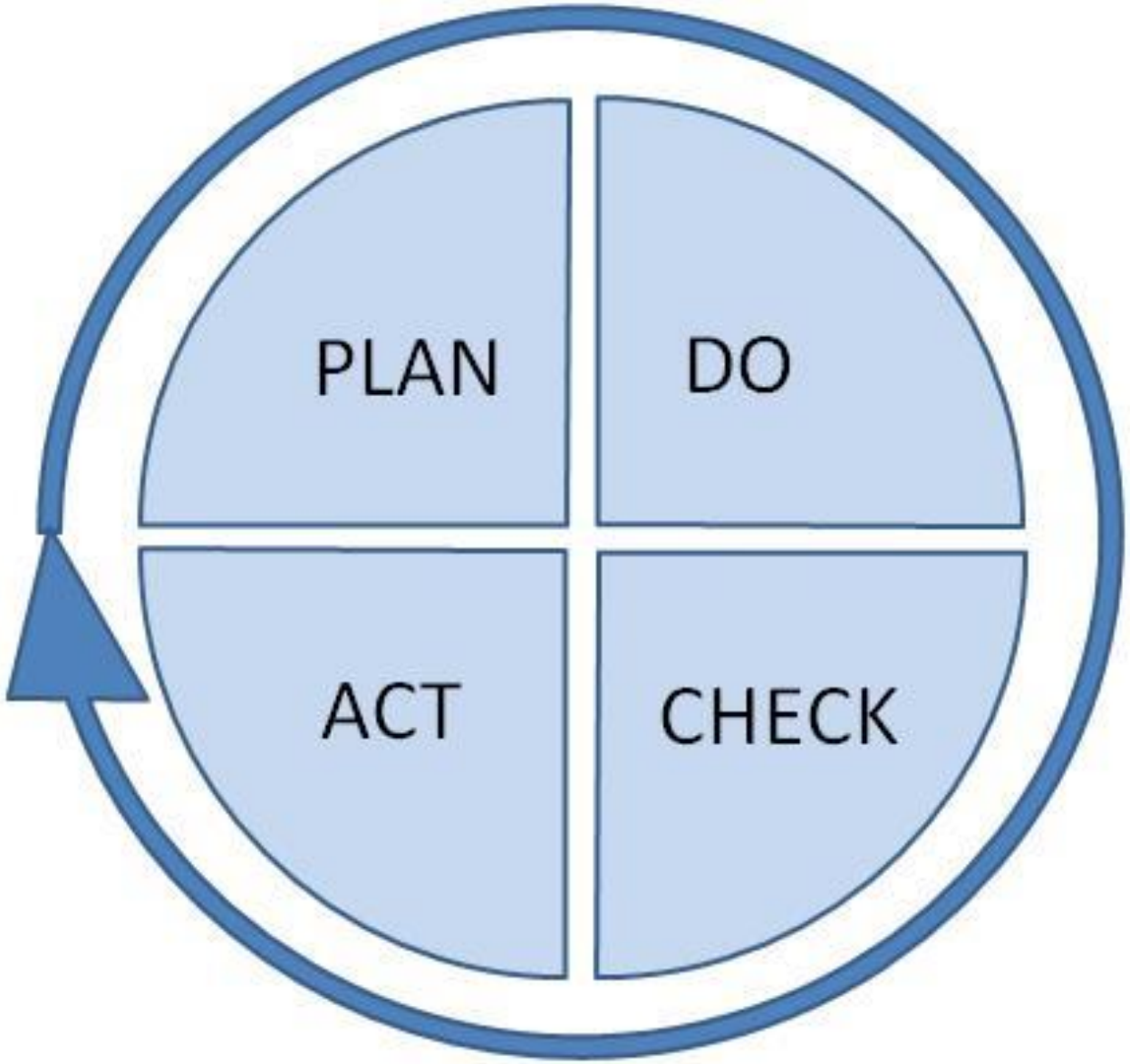
- **systematického a rozsiahleho hodnotenia** osobných aspektov
- spracúvania vo **veľkom rozsahu osobitných kategórií** údajov
- systematického **monitorovania verejne prístupných miest** vo veľkom rozsahu

Zdroj: http://www.gdprpro.co.uk/update-sources/

Prvé kroky?

Prvé kroky

- nie je to jednorazová záležitosť,
  ale neustále prebiehajúci proces
- „Data flow map“
- manažment hlásenia incidentov
- …



Zdroj: http://www.expertprogrammanagement.com/2010/10/the-plan-do-check-act-cycle-the-deming-cycle/

Ďakujem za pozornosť!

pavol.sokol@upjs.sk

security.science.upjs.sk