GDPR
General Data Protection Regulation

a jeho podpora
v softvéri COMPEKO

Apríl 2018

Compeko

Program

- **Cieľ a zmysel**
- **Legislatíva ...**
- **Ako splniť požiadavky GDPR**
- **Špecifiká pri používaní účtovných programov**
- **Špecifiká pri zákazkovom spracúvaní UCT, MZD, ...**

- **Diskusia (**priebežne**)**

Compeko

Cieľ a zmysel

- Nové nariadenie o ochrane osobných údajov (GDPR) je evolučným pokračovaním a nahradením už zastaralej legislatívy upravujúcej ochranu osobných údajov v Európe.
- Jeho hlavným cieľom je:
  - zaviesť **jednotné pravidlá** pre ochranu osobných údajov občanov Európy bez ohľadu na to, kto ich spracúva (teda i subjekty mimo EÚ) najmä v „kybernetickom“ svete
  - dať občanom EÚ výrazne **väčšie práva** pri kontrole toho, čo sa s ich údajmi deje
  - Stimulovať spracovateľov a sprostredkovateľov na prijatie zmysluplných, potrebných a technicky realizovateľných opatrení a postupov na **primeranú ochranu** spracúvaných a ukladaných osobných údajov
  - Stimulovať spracovateľov a sprostredkovateľov k takým postupom, aby zbierali, spracúvali a ukladali **iba tie osobné údaje**, ktoré sú skutočne k splneniu vymedzeného cieľa **potrebné** a to iba na minimálnu nutnú dobu.

Compeko

Cieľ a zmysel

- V čom sa líši od súčasnej legislatívnej úpravy?
  - Nariadenie nie je priamo realizovateľné, ale vyžaduje si konkretizáciu v národných legislatívnych úpravách (napr. zákon o ochrane osobných údajov)
  - Nariadenie má účinnosť od 25.5.2018 a nie je zrušiteľné žiadnym ustanovením národnej legislatívy, t.j. má účinnosť aj bez podpory národnej legislatívy
  - Zavádza množstvo nových termínov a pojmov
  - Rozširuje pojem „osobný údaj“ (chránený údaj) na akýkoľvek údaj, ktorý umožní priamo alebo nepriamo identifikovať konkrétnu fyzickú osobu (okrem doterajších údajov to môže byť aj IP adresa, údaje o pohybe, lokalizačné údaje, údaje o pobyte, rôzne profily – typy nákupov, náboženské prejavy, fotografia tváre, rohovky, biometrické údaje, ...)
  - Zavádza špeciálnu ochranu osobných údajov detí a maloletých osôb
  - Vo vymedzených prípadoch je povinnosť zriadiť pozíciu inšpektora na ochranu dát
  - Zavedenie oznamovacej povinnosti pri bezpečnostnom incidente voči príslušným inštitúciám ale aj voči dotknutým osobám
  - Posilnenie práv dotknutých osôb (výpis, oprava dát, prenos dát, zabudnutie)
  - Zavedenie kontroly na cezhraničný prenos osobných dát
  - Kto chce spracúvať osobné údaje, musí jasne deklarovať účel spracovania a uchovávania a na tento musí získať jasný a **vedomý** súhlas dotknutej osoby

Compeko

... legislatíva

Základný legislatívny rámec :

- Nové všeobecné **nariadenie** EÚ 2016/679 o ochrane osobných údajov prijaté Európskym parlamentom aj Radou Európy General Data Protection Regulation (GDPR) sa bude priamo vzťahovať na každý subjekt, ktorý spracúva a ukladá údaje občanov EÚ a vstúpi do účinnosti 25. mája 2018.
- **Sankcie** za nedodržanie požiadaviek nariadenia sú až 20 mil. Eur alebo 4% celosvetového obratu – berie sa vyššia suma.
- Smernica EÚ 2016/680 (**policajná smernica**) o ochrane FO pri spracúvaní osobných údajov v trestnom konaní, prevencii, ...

- Zákon 18/2018 Z.z. o ochrane osobných údajov ... Zverejnený v zbierke zákonov 30.1.2018

Compeko

... legislatíva

Koho sa GDPR týka:

- Každej firmy, každého podnikateľa aj živnostníka, ktorý v rámci svojej činnosti spracúva, ukladá prenáša ... osobné údaje.
- §3 ods. 1) – 4)

Koho sa GDPR netýka:

- FO v rámci výlučne osobnej alebo domácej činnosti
- SIS a VSS
- NBÚ
- §3 ods. 5)

... legislatíva

Kedy môžem spracúvať osobné údaje:

- Toto rieši zákon 18/2018 Z.z. v §6 - §18 a ide o vymedzenie nutnosti, podmienok, zásad a tiež výnimiek. Napr.:
- Zásada zákonnosti
- Obmedzenie účelu
- Minimalizácia osobných údajov
- Zásada správnosti
- Zásada minimalizácie uchovávania
- Zásada zodpovednosti
- Spracúvanie osobitných kategórií osobných údajov
- Spracúvanie údajov v súvislosti s vyšetrovaním trestnej činnosti ...

... legislatíva

Práva dotknutej osoby :

- §22 Právo na opravu osobných údajov
- §23 Právo na výmaz osobných údajov
- §24 Právo na obmedzenie spracúvania osobných údajov
- §25 Oznamovacia povinnosť (prevádzkovateľa) v súvislosti s opravou, vymazaním ... (voči príjemcovi)
- §26 Právo na prenosnosť osobných údajov
- §27 Právo namietať spracúvanie osobných údajov
- §28 Automatizované individuálne rozhodovanie vrátane profilovania

... legislatíva

Posúdenie vplyvu ... :

- §42
- Povinnosť vykonať posúdenie je vtedy, ak existuje reálne vysoké riziko porušenia práv fyzických osôb
- Povinnosť konzultovať postupy so zodpovednou osobou, ak bola určená
- V prípade komplikovaného spracovania s vysokým rizikom môže prevádzkovateľ požiadať úrad o konzultáciu

... legislatíva

Zodpovedná osoba :

- §44 Určenie zodpovednej osoby, ak
  - Údaje spracúva orgán verejnej moci
  - Ak ide o operácie, ktoré si vyžadujú systematické monitorovanie dotknutých osôb vo veľkom rozsahu
  - Ide o spracovanie osobitných kategórií osobných údajov
- Zodpovedná osoba:
  - Prevádzkovateľ a sprostredkovateľ sú povinní vytvoriť zodpovednej osobe vhodné podmienky na výkon jej činnosti
  - Poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi
  - Monitoruje súlad procesov s platnou legislatívou v oblasti ochrany osobných údajov
  - Spolupracuje s úradom
  - Plní úlohu kontaktného miesta pre úrad

... legislatíva

Úrad na ochranu osobných údajov:

- §50 a ďalšie
  - Úrad je rozpočtovou nezávislou organizáciou
  - Plní úlohu dozorného orgánu nad ochranou osobných údajov
  - Monitoruje uplatňovanie zákona 18/2018
  - Vyjadruje sa k návrhom relevantných zákonov
  - Poskytuje konzultácie
  - Metodicky usmerňuje prevádzkovateľov
  - Preveruje zákonnosť spracúvania osobných údajov
- Má právo
  - Nariadiť poskytnutie informácií
  - Vstupovať do priestorov
  - Nariadiť, aby prevádzkovateľ alebo sprostredkovateľ vyhoveli žiadosti dotknutej osoby
  - Nariadiť pozastavenie prenosu údajov
  - ....
- Udeľuje akreditácie certifikačným subjektom

Compeko

... legislatíva

Vývoz údajov :

- §48 prenos údajov do tretích krajín alebo medzinárodných organizácií
  - Ak Komisia rozhodla, že príslušná krajina má zodpovedajúcu úroveň ochrany osobných údajov
  - Ak také rozhodnutie neexistuje, je potrebné mať primerané záruky ochrany osobných údajov
  - Vždy sa vyžaduje písomný informovaný súhlas dotknutej osoby

... legislatíva

Povinnosti prevádzkovateľa z rôznych častí zákona:

- **Prijať primerané opatrenia na naplnenie cieľa GDPR**
- **Povinnosť určenia zodpovednej osoby**
- **Za výber sprostredkovateľa zodpovedá prevádzkovateľ**
- **Predchádzanie k neoprávnenému prístupu k osobným dátam**
- **Zavedenie anonymizácie osobných údajov**
- **Zabezpečenie prevencie pred únikom dát**
- **Zabezpečenie realizácie práva na zabudnutie (vymazanie dát)**
- **Zabezpečenie realizácie práva na výpis / prenos dát**
- **Zabezpečenie realizácie ďalších práv dotknutých osôb**
- **Monitorovanie aktivít pri práci s osobnými údajmi**
- **Schopnosť identifikovať, analyzovať a dokumentovať bezpečnostné incidenty s povinnosťou ich bezodkladného ohlásenia úradu a dotknutým osobám**

Ako splniť požiadavky GDPR

Čo treba spraviť, aby boli požiadavky GDPR splnené?

- **Vytvoriť internú smernicu pre narábanie s dátami, ktorá má pre všetkých pracovníkov a spolupracovníkov daného subjektu stanoviť:**
  - **Ktoré dáta sú chránené a ktoré nie**
  - **Posúdenie nutnosti spracúvania osobných údajov vzhľadom na naplnenie cieľa**
  - **Analýza vplyvu spracúvania osobných údajov na ich ochranu, možnosť vzniku incidentu, ...**
  - **Aké procesy a postupy uplatňovať pri práci s chránenými dátami (preberanie a odovzdávanie písomností, mailov, tvorba vlastných poznámok, ...)**
  - **Ako realizovať jednotlivé požiadavky GDPR (napr. ako realizovať právo na zabudnutie, ako realizovať právo na výpis / prenos dát, ako realizovať iniciatívne vymazanie nepotrebných dát, ...(**
  - **ako spracúvať a narábať s protokolmi o zrealizovaní požiadaviek GDPR (napr ako uchovávať protokoly o vymazaní údajov – protokol tiež obsahuje chránené dáta)**
  - **Aké technické podporné prostriedky sa majú používať (akú podporu pre procesy GDPR poskytujú rôzne softvérové produkty používané v organizácií, ako sa aktivujú dané podporné procesy, kto je za aktiváciu zodpovedný, ...)**
- **Treba stanoviť, ako sa priebežne kontroluje dodržiavanie internej smernice**
- **Treba stanoviť, kedy a ako sa interná smernica má aktualizovať, dopĺňať, ...**
- **Byť pripravený na kontrolu dodržiavania ustanovení GDPR ktorýmkoľvek Európskym komisárom**
- **Inšpiráciou môže byť odporučenie WP29** **(http://www.minedu.sk/data/files/7916.pdf)**

Compeko

Ako splniť požiadavky GDPR

Desatoro GDPR

1. Oboznámiť sa s GDPR a pochopiť zásady
2. Zostaviť pracovný tím (IT, právnik, manažér, ...)
3. Analýza používania osobných údajov
4. Identifikácia informačných systémov (to nie je program, aplikácia, ...!)
5. Analýza rizík a opatrení na ich zmiernenie alebo elimináciu
6. Zadefinovanie nových požiadaviek
7. GAP analýza (ako sa dopracovať k želanému stavu)
8. Implementácia GDPR do praxe
9. Vyhotovenie dokumentácie nie len pre účely kontroly
10. Trvalé monitorovanie a aktualizácia postupov a procesov

Compeko

Špecifiká pri používaní účtovných programov

Pri používaní účtovných programov platí:

- **Dôvod spracovania je v zákonoch (o účtovníctve, DPH, ...) a teda na spracovanie v tomto rozsahu nepotrebujeme súhlas dotknutej osoby**
- **Rozsah spracúvaných údajov by mal byť revidovaný iba na tie, ktoré skutočne pre splnenie zákonných požiadaviek potrebujeme**
- **Retenčná doba záznamov alebo jednotlivých údajov vyplýva z povinnej doby uchovania určenej zákonmi (účtovné doklady – 10 rokov, ...)**
- **Údaje, ktoré sme získali pre tento účel nemôžme použiť na iný účel (cielená reklama ...)**
- **Podpora pre realizáciu práv dotknutých osôb sa nedá zabezpečiť „zvonka“, ale dané procesy MUSÍ zabezpečovať príslušný účtovný program alebo aspoň musí dovoliť vykonať také manuálne úpravy dát, ktoré je možné považovať za realizáciu práv (napr. anonymizácia) a to aj v zaúčtovaných a archivovaných dátach.**
- **Bez jasnej podpory a informácie zo strany tvorcu programu je takmer nemožné splniť požiadavky GDPR.**

Špecifiká pri zákazkovom spracovaní UCT, MZD, ...

Pri zákazkovom spracovaní UCT, MZD, ... platí:

- **Prevádzkovateľom nie je účtovná firma, ale jej zákazník, a teda je jeho povinnosťou vypracovať posúdenie rizika v spolupráci s danou účtovnou firmou (sprostredkovateľom).**
- **Účtovná firma môže mať ústretovo pripravené vlastné informácie o spôsobe realizácie požiadaviek GDPR (informácia o uložení dát, zabezpečení proti zneužitiu, strate, zničeniu, informácia o používanom SW a jeho podpore procesov GDPR,....)**
- **Klient a účtovná firma musia spolu doriešiť otázky odovzdávania podkladov a výsledkov spracovania, aby aj tieto prenosové cesty boli bezpečné v zmysle GDPR a tieto mať podchytené zmluvne**
- **Podpora pre realizáciu práv dotknutých osôb sa nedá zabezpečiť „zvonka“, ale dané procesy MUSÍ zabezpečovať príslušný účtovný program alebo aspoň musí dovoliť vykonať také manuálne úpravy dát, ktoré je možné považovať za realizáciu práv (napr. anonymizácia) a to aj v zaúčtovaných a archivovaných dátach.**
- **Bez jasnej podpory a informácie zo strany tvorcu programu je takmer nemožné splniť požiadavky GDPR.**

Compeko

Záver

Compeko