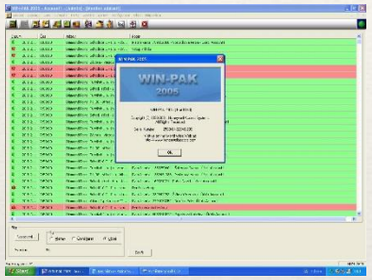
Souboj titánů – GDPR vs. bezpečnostní technologie

Mgr. Pavla Rajmanová



Ochrana osobních údajů

- **nařízení Evropského parlamentu a Rady č. 2016/679 - General Data Protection Regulation**
- reaguje na změny, zejména v oblasti informačních technologií (nové kategorie osobních údajů)
- účinnost 25.5.2018
- přímá působnost ve všech státech EU, některé otázky si státy mohou upravit samy - u nás **návrh zákona o zpracování osobních údajů** + změny dalších zákonů
- zvláštní úpravu mají poskytovatelé telekomunikační sítí, poskytovatelé platebních služeb apod.

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Působnost

- **Kdy nejde o zpracování:** ve chvíli, kdy zpracování provádí fyzická osoba výlučně v průběhu domácích činností (tj. ne v souvislosti s profesní nebo obchodní činností) => vedení osobního adresáře, využívání sociálních sítí
- **!POZOR!** - je vykládáno přísně, podle judikatury je zpracováním osobních údajů i zveřejnění cizích osobních údajů na osobních blozích a otevřených profilech na sociálních sítích

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Osobní údaj – co to je?

- veškeré informace o určené nebo URČITELNÉ fyzické osobě => vztahuje se i na nepřímou (zprostředkovanou) identifikaci (spojení více indentifikátorů z více zdrojů)
- **IDENTIFIKÁTORY**: jméno, bydliště, datum narození, lokační údaje, síťový identifikátor, genetické aspekty
- není rozhodující, zda je údaj pravdivý, měřitelný, zda jde o odhad (“nespolehlivý dlužník”), nerozhoduje ani formát informace (písemně, obrazový záznam, zvukový záznam - např. nahrávané telefonní hovory)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Působnost

- osobní = NA KOHO se vztahuje => na FYZICKÉ OSOBY
- podnikatelé? => pokud fyzické osoby, pak ano, vyjma údajů, které podnikatel určil ke zveřejnění, nebo jejich zveřejnění podléhá zákonu
- zesnulé osoby - NE,

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Identifikovatelnost osoby (subjektu údajů)

- **identifikovaná osoba** => Osoba, kterou správce nebo zpracovatel dokáže přímo odlišit od ostatních osob
- **identifikovatelná osoba** => pokud správce nebo zpracovatel nedokáže osobu odlišit sám, ale za pomoci dalších údajů, které jsou:
  - veřejně dostupné, nebo
  - je má k dispozici další subjekt
  - a za jejich pomoci lze rozumně očekávat nebo předpokládat, že osoba bude identifikovatelná
- např: IP adresa, MAC adresa, IMEI, RZ vozidla, číslo bankovního účtu, telefonní číslo, e-mailová adresa, číslo pojistné smlouvy, VIN vozidla, otisk prstu, struktura oční sítnice, a další biometrické hodnoty
- hlediskem je DOPAD DO SOUKROMÍ fyzické osoby (i podnikatele) - např. informace o udělení pokuty při podnikatelské činnosti

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zpracování osobních údajů - operace

- Shromáždění (např. formulážem, e-mailem, na recepci na vyžádání)
- Zaznamenání (do databází ACS, Docházky, PZTS)
- Uspořádání (dělení do účtů, oddělení)
- Strukturování (práva přístupů, kdy vidím osobní údaje držitelů)
- Uložení (tvorba nových držitelů karet, uživatelů PZTS, správa CCTV)
- přizpůsobení nebo pozměnění (HR, recepce, personální oddělení, pověřená osoba SVJ)
- Vyhledání (včetně náhledu na události v historii ACS, PZTS, CCTV)
- nahlédnutí (nemá právo nic měnit, ale vidí již zadané karty a uživatele)
- Použití (předávám data do dalších systémů)
- zpřístupnění přenosem (vzdálená správa, klientské SW, předávání databází, papírové seznamy)
- Omezení (měním údaje)
- výmaz nebo zničení (nejen skrze UI SW, ale i DB operace skrze Management studio)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zpracování osobních údajů

- **NENÍ - ad hoc přístup nezbytný k servisu poskytovaného softwaru, servisní zásah do databáze**

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Správce osobních údajů

- zpracovává osobní údaje
- určuje PROČ (= účel zpracování - evidence docházky,evidence ACS, snímání biometrických teplate, evidence dat v PZTS, CCTV, nabízení produktů, plnění smlouvy, apod.)
- určuje JAK (= jakými prostředky a postupy), skrze UI SW do databáze (na PC nebo v zařízení vlastním), v papírové podobě, atd.

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zpracovatel osobních údajů

- každý, kdo zpracovává osobní údaje místo správce (HR, recepční, technik atd.)
- na základě pověření správcem (smlouva) nebo ze zákona
- osoba odlišná od správce (např., bezpečnostní agentura obsluhující kamerový systém nákupního centra, technik zadávající investorovi data, facility agentura, pult PCO,) externí společnost zpracovávající mzdy, technická podpora)
- na rozdíl od správce NEURČUJE ÚČEL zpracování (proč jsou údaje zpracovány), pouze pracuje s daty

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Způsoby instalace systémů vs. zpracování a správa osobních údajů

- prostá koupě, instalace systému, zaškolení a předání koncovámu klientovi
- koupě, instalace, zadání osobních údajů pro koncového klienta (do databáze) a předání -> **zpracování**, doporučujeme uzavřít zpracovatelskou smlouvu (např. jako součást smlouvy o instalaci)
- koupě, instalace, servis v podobě správy databáze na vlastním zařízení nebo trvalý vzdálený přístup -> **zpracování,** také doporučujeme uzavřít písemnou smlouvu o zpracování
- Přeposílání databází pro analýzu, absahující osobní data -> **zpracování,** ale **!POZOR!** Na způsob předávání (šifrovaně, bezpečným způsobem. **NE** veřejná úložiště, či prostý mail, nebo flash bez zabezpečení

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zásady zpracování

- **zákonnost** = pouze z důvodů stanovených zákonem - čl. 6 a 9
- **korektnost a transparentnost** = otevřenost, zajištění co největší míry informovanosti osob, kterých se zpracování týká (čl. 12 - 14)
- **účelové omezení** = zákaz zpracovávat údaje za jiným účelem, než pro který byly shromážděny
- **minimalizace údajů** = vždy pouze takové údaje, které jsou v dané věci nezbytné, pouze v nutném rozsahu
- **přesnost** = přiměřená aktualizace, opatření k opravě nebo odstranění nepřesných údajů
- **omezení uložení** = povinnost vymazat nebo anonymizovat údaje, které již nejsou potřebné
- **integrita a důvěrnost** = povinnost údaje zabezpečit (čl. 32)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zákonnost zpracování

- **<u>právní důvody zpracování:</u>**
- souhlas osoby, jíž se osobní údaje týkají
- splnění smlouvy s osobou, jíž se údaje týkají
- splnění právní povinnosti (hlášení OSSZ, finančnímu úřadu, provádění srážek ze mzdy)
- ochrana životně důležitých zájmů osoby, jíž se údaje týkají nebo jiné fyzické osoby (zdravotní služby)
- úkoly prováděné ve veřejném zájmu (policie)
- úkoly prováděné při výkonu veřejné moci (katastr nemovitostí)
- **oprávněné zájmy správce** (dodržování pracovní doby,režimový přístup do prostor, ochrana majetku skrze PZTS, CCTV, svoboda podnikání apod.)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Oprávněné zájmy správce

- jeden z nejširších právních titulů
- **třeba definovat, co je oprávněným zájmem** (evidence pracovní doby, ochrana majetku) - tři skupiny oprávněných zájmů:
  - zájmy na výkonu základních práv a svobod
  - veřejné zájmy a zájmy širší komunity (dobročinnost, předcházení korupci, předcházení podvodům)
  - ostatní subjektivní zájmy správce
- je potřeba provést tzv. **balanční test** - tj. zda důsledky zpracování nemohou poškodit osoby, jichž se zpracování týká (hledisko - citlivost údajů, riziko pro osoby, jichž se týká, "rozumná očekávání" osob, jichž se týká => zda zásah do soukromí není příliš velký vzhledem k tomu, čeho chceme dosáhnout)
- **důležité je přijmout záruky bezpečnosti pro ochranu osob - např.následná anonymizace, pseudonymizace …**

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Typické příklady oprávněných zájmů

- **fyzická bezpečnost, IT bezpečnost,** ochrana majetku, evidence docházky s výstupem do mezd, přímý marketing, vymáhání právních nároků, ochrana před zneužitím služeb, monitorování zaměstnanců za účelem ochrany majetkových zájmů zaměstavatele atd.

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Bezpečnostní technologie

- využití osobních údajů v bezpečnostních systémech:
- a) prosté osobní údaje (identifikátory) - jméno, příjmení, adresní údaje, firemní zařazení
- b) výsledky technického zpracování fyzických, fyziologických nebo behaviorálních znaků - technologie rozpoznávající obličej (2D, 3D), otisk prstu, scan krevního řečiště, sken sítnice => zvláštní kategorie osobních údaj, **pokud jsou využívány k jedinečné identifikaci fyzické osoby** = PRO ÚČELY NAŘÍZENÍ JDE O BIOMETRICKÉ ÚDAJE

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Biometrické údaje - ZMĚNY

- dříve stanovisko ÚOOÚ č. 3/2009 - jednosměrné hashování mohlo vyjmout z kategorie citlivých údajů
- nyní změna - i nakládání s šablonami, do kterých jsou biometrické údaje převáděny, se považuje za nakládání s citlivými údaji - dle čl. 9 Nařízení

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Biometrické údaje

- změna oproti zákonu č. 102/2000 - mezi citlivé údaje byly řazeny biometrické údaje využívané k identifikaci a AUTENTIZACI
- nyní pouze biometrické údaje užívané k JEDINEČNÉ IDENTIFIKACI

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Využití biometrických údajů

- shromáždění v databázi za účelem identifikace (využití v docházkových a přístupových systémech) = > nakládání se zvláštní kategorií osobních údajů (ve starší terminologii “citlivé údaje”)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Jak realizovat?

- 1. vyhodnotit riziko
- 2. přijmout vhodná opatření ke snížení rizka

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Vyhodnocení rizika - zajímavosti

- různé metodiky (obojí dostupné online):
  - ICO (Velká Británie) - Conducting privacy impact assessments, code of practice
  - CNIL (Francie) - Methodology for Privacy Risk Management: How to implement the Data Protection Act
- **určit hrozby**, které jsou se zpracováním spojené (možnost porušení zabezpečení osobních údajů, nevhodné zpracování, nezákonné překročení stanoveného účelu zpracování, nepřesnost údajů, narušení důvěrnosti osobních údajů)
- **určit škodu,** která naplněním hrozeb může vzniknout (diskriminace, krádež identity, zneužití identity, finanční ztráta, poškození pověsti, prolomení pseudonymizace, hospodářské nebo společenské znevýhodnění)
- **určit, jak je pravděpodobné, že taková škoda vznikne** (počet osob zapojených do zpracování, počet třetích osob zapojených do zpracování, historie předchozích incidentů)
- **určit závažnost** takové škody (dopad na život osob, zranitelnost dotčených osob, možný dopad na jejich finanční a ekonomickou situaci)

- většinou analýza v podobě auditu

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Nutné kroky

- zpracování buď na základě zákona nebo **souhlasu** dotčené osoby (zaměstnance, zákazníka, člena SVJ atd,)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Nutné kroky

- **aktivuje** povinnost zpracovat posouzení vlivu na ochranu osobních údajů dle čl. 32
  - popis
  - posouzení nezbytnosti (argumenty, proč biometrický přístupový systém)
  - posouzení rizik pro práva osob
  - plánovaná opatření pro řešení rizik (bezpečnostní opatření, pseudonymizace apod.)
  - DOSUD NEJASNÉ - MĚL BY BÝT VYDÁN SEZNAM OPERACÍ, KTERÉ ZNAMENAJÍ VYSOKÉ RIZIKO A AKTIVUJÍ POVINNOST

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Nutné kroky

- nutnost ohlašovat porušení zabezpečení dozorovému orgánu, případně i osobám, jichž se týkají

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Řešení

- upřednostnění autentizačních (tj. verifikačních) systémů
- pečlivá příprava argumentace a dokumentace podle parametrů výše uvedených, možnost využití konzultací s ÚOOÚ (**došlo ke zrušení ohlašovací povinnosti**)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Kamerové systémy

- typicky na základě oprávněného zájmu zaměstnavatele
- prosté, nebo biometrické (s rozpoznáním obličeje, RZ vozidla)
- pozor - soustavný monitoring zaměstnanců v rozhodovací činnosti ÚOOU není připouštěn
- otázka záznamu obrazu nebo obrazu a zvuku?
- nutné oznámit (předpoklad schválení celoevropsky platných piktogramů)
- nutné poskytnout informaci dle čl. 13
- ZMĚNA - není ohlašovací povinnost

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Informační povinnost

- čl. 13 a 14 nařízení
- čl. 13 - informace, které poskytuje původní správce (tj. ten, kdo získal údaje přímo od osoby, jichž se týkají)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Praktické tipy

- informace umístit na webu, na dokumentech předávaných zákazníkovi uvést základní ifnormace + link na web, kde budou zpracovány podrobně
- je-li prostor monitorován kamerovým systémem - informaci jasně u vchodu do prostoru, s odkazem na další informace uvedené přímo v prodejně, a případně s návrhem obracet se na zaměstance, kteří poskytnou v listinné podobě - viz příklady

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Zabezpečení osobních údajů

- povinnost dle čl. 32 - ochrana před únikem dat a vznikem škody - PRAKTICKÝ VÝZNAM
- rizika:
  - náhodné nebo protiprávní zničení (rozbití služebního notebooku)
  - ztráta (ztráta služebního notebooku, telefonu, listin s údaji klientů
  - neoprávněné zpřístupnění (kdo má možnost nahlížet do databází, kdo má možnost vstupu do budovy, jakým způsobem je zajištěn přístup, kdo má klíče od registratur)
  - neoprávněný přístup (softwarová ochrana, hesla, šifrování, technické zabezpečení budov a místností)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Prostředky zabezpečení

- nastavení vhodné úrovně bezpečnosti
- prostředky:
  - důvěrnost systémů a služeb zpracování (pseudonymizace a šifrování, autentizace a autorizace osob majících přístup - různé úrovně oprávnění, softwarové řešení)
  - integrita systémů a služeb zpracování (ochrana před neoprávněným zničením, ztrátou nebo pozměněním - monitorování přístupu oprávněných osob, monitorování změn, které oprávněné osoby provedly, limitování přístupu pouze pro oprávněné osoby, hashování - softwarové řešení)
  - zajištění dostupnosti systémů a služeb (pro případ výpadku funkcionality - záložní zdroje, větší počet serverů - softwarové řešení)
  - zajištění odolnosti systémů a služeb (odolnost před selháním - softwarové řešení)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Podmínky přístupu osob k osobním údajům

- nutnost všechny osoby, které mají přístup k osobním údajů, proškolit a uložit jim povinnost, jak s osobními údaji nakládat a zakázat nakládání v rozporu s pokyny (pracovní smlouvou, dohodou o provedení práce, smlouvou s dodavatelem IT)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Dozorový úřad

- Úřad na ochranu osobních údajů
- možnost konzultací - čl. 36 (dříve ohlašovací povinnost, nyní možnost konzultovat před zahájením zpracování, pokud výsledkem analýzy je vysoké riziko)

Mgr. Pavla Rajmanová, 777331663, rajmanova@seznam.cz

Děkuji za pozornost