GDPR
v praxi

V Brně dne 5. prosince 2017

EU

- Nová EU směrnice **nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016** má nastoupit místo původní direktivy 95/46/EC, která byla od roku 1995 součástí EU zákonů o ochraně soukromí a lidských práv.
- Přímo účinné nařízení o ochraně osobních údajů (**GDPR** – General Data Protection Regulation)
  - *týká se **porušení ochrany osobních údajů** - ÚOOÚ*

- Směrnice o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informací v Unii (**směrnice NIS** – Network and Information Security incidents) – částečně již transponována do z. č. 181/2014 Sb., o kybernetické bezpečnosti
  - *týká se **narušení bezpečnosti sítí a informací*** – NBÚ

- Směrnice NIS – je určena pro subjekty poskytující služby v KI
- Nařízení GDPR – platí pro všechny společnosti v EU

NIS obecně

- Směrnice NIS nám do národní legislativy přináší nové typy povinných subjektů:
  - **Provozovatele základních služeb - PZS** (alternativa KII)
  - **Poskytovatele digitálních služeb - PDS** (online tržiště, internetové vyhledávače, Cloudy)

- Provozovatel základní služby - soukromý nebo veřejný subjekt z daného odvětví poskytující službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností, přičemž poskytování dané služby je závislé na ICT a případný kybernetický bezpečnostní incident by mohl způsobit významné narušení poskytování této služby.

- Provozovatel digitální služby - informační společnosti spočívající v provozování:
  - on-line tržiště (umožňující spotřebiteli nebo prodávajícímu on-line uzavírat s prodávajícím podnikatelem kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm)
  - internetového vyhledávače (umožňujícího provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem)
  - cloud computingu (umožňujícího přístup k rozšířitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet)

NIS pravidla

- Dopad na správce KII a VIS (zakotveno již v ZKB) a nově také na provozovatele KII a VIS
- Určování Provozovatele základní služby (PZS) novou vyhláškou.
- Povinnost hlášení incidentů pro KII, VIS, provozovatele významných sítí, ale i PZS a PDS.
- Ošetření svobodného přístupu k informacím
  (§10 - Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle ZKB, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím, se neposkytují.)
- Sankce se zvyšují z původních 100.000,- Kč na max. 5 000.000,- Kč
- Pozice manažera kybernetické bezpečnosti (MKB)

Otázky k GDPR

- **Co znamená zkratka GDPR?**
  Jedná se o zkratku z anglického General Data Protection Regulation, do češtiny se překládá jako Obecné nařízení o ochraně údajů. Objevuje se také alternativní označení Obecné nařízení o ochraně údajů Evropské Unie.

- **Kdy toto nařízení vstoupí v účinnost?**
  GDPR bylo přijato v květnu 2016, ale v účinnost vstoupí až 25. května 2018. Dvouleté „přípravné období“ poskytuje firmám dostatečný čas pro přípravu.

- **Koho se týká?**
  GDPR platí celosvětově pro jakýkoliv subjekt zpracovávající osobní údaje občanů EU. Jsou to tedy veškeré organizace napříč členskými státy EU, které sbírají, uchovávají a zpracovávají osobní údaje.

- **Co všechno se považuje za osobní údaje?**
  Jakákoliv informace o člověku (osobě). Například jméno, adresa, datum narození nebo kontaktní informace.

Otázky k GDPR

- **Je možné, že bude uživatel moci po zavedení GDPR ovlivnit zasílání nevyžádané pošty?**
  Pravděpodobně ano. Zatímco nyní můžete u dané společnosti zažádat, aby vám neposílali reklamní sdělení, po implementaci GDPR budou naopak společnosti muset žádat o povolení k zasílání těchto informací.
  Organizace také budou muset zajistit větší transparentnost při nakládání s osobními údaji. Dále už také nebude platit to, že mlčení znamená souhlas, že daná společnost může vaše data využít.

- **Jak uživatel zjistí, že firmy ukládají jeho osobní data?**
  Bohužel neexistuje centrální databáze, v níž by se uživatelé dozvěděli, které firmy uchovávají jejich data. Vždy je ale možné se konkrétní společnosti zeptat. GDPR nově dává uživatelům právo vědět, jaké informace o nich společnosti mají a jak s nimi nakládají. Možnost vyžádat si tyto informace se označuje jako „žádost o poskytnutí informace".

GDPR obecně

- Je platná **pro každou organizaci** nabízející zboží nebo služby v rámci členských států EU a manipulující s osobními údaji subjektů IT.
- Bezpečnostních opatření musí být implementovány **do technických a organizačních procesů a postupů již od počátku jejich přípravy**.
- Povinnost ohlášení případu **narušení OÚ**.
- Za ochranu dat je zodpovědný **celý dodavatelský řetězec**.
- Výklad:

  - Fakticky to znamená, že organizace by měly shromažďovat a zpracovávat pouze nezbytné informace sloužící k danému účelu.
  - Po zpracování by data měla být smazána či jinak zlikvidována.
  - Ochrana osobních údajů by měla být zahrnuta do všech firemních procesů a systémů (bezpečnost by měla být brána v potaz již od počátku vzniku informačního systému).
  - Za ochranu dat je zodpovědný celý dodavatelský řetězec od výrobce po dodavatele k zákazníkům (nebude možné přenášet zodpovědnost za zabezpečení osobních dat klientů například na dodavatele).
  - Znamená to, že firmy budou muset kontrolovat i své partnery, zda osobní údaje dostatečně zabezpečují.

Příklady osobních údajů

Příklady osobních údajů zahrnují:

- jméno a příjmení
- domácí adresa
- e-mailová adresa (například jméno.příjmení@firma.com)
- číslo identifikační karty
- lokační údaje (např. funkce využívající údaje o poloze v mobilním telefonu)
- adresa IP (Internetový protokol)
- ID souboru cookie
- identifikátor telefonu pro inzerenty,
- údaje ve vlastnictví nemocnice nebo lékaře (vedoucí k identifikaci určité osoby)

Příklady údajů, které nejsou pokládány za osobní, zahrnují:

- registrační číslo společnosti
- e-mailová adresa, jako je například info@firma.com
- anonymizované údaje

Zdroj:**https://ec.europa.eu/info/law/law-topic/data-protection**

Příklady zpracování osobních údajů

Příklady zpracování zahrnují:
automatizovanou či manuální formou

- řízení pracovníků a správa výplatní listiny
- přístup k databázi kontaktů s osobními údaji nebo konzultace takové databáze
- zasílání propagačních e-mailů
- skartace dokumentů obsahujících osobní údaje
- zveřejnění/umístění fotografie osoby na web
- uložení adres IP nebo adres MAC
- zaznamenávání videa (kamerové systémy)

GDPR pravidla

GDPR se použije na:

- společnost nebo subjekt, který zpracovává osobní údaje v rámci činností některé ze svých poboček usazených v EU bez ohledu na to, kde se údaje zpracovávají

- společnost, která je usazena mimo EU a nabízí zboží/služby (placené nebo zdarma) nebo monitoruje chování fyzických osob v EU

- MSP (malé a střední podniky) zpracovávající osobní údaje

- pravidla se vztahují pouze na osobní údaje o fyzických osobách, netýkají se údajů o společnostech ani jiných právnických osobách

GDPR definuje

- **správce údajů** - určuje účely, pro něž se osobní údaje zpracovávají, a také příslušné prostředky

- **zpracovatel údajů -** zpracovává osobní údaje pouze jménem správce (zpracovatel údajů je obvykle třetí strana nezávislá na společnosti)

- Někdo jiný (fyzická nebo právnická osoba nebo jiný subjekt) může zpracovávat osobní údaje vaším jménem, pokud existuje smlouva nebo jiný právní akt.

- Jmenovaný zpracovatel následně nemůže jmenovat jiného zpracovatele bez vašeho předchozího, konkrétního nebo všeobecného písemného povolení.

GDPR pravidla

- **Právo být zapomenut** – pokud jednotlivec již nechce, aby se jeho data dále z nějakého důvodu zpracovávala, má právo požadovat po zpracovateli, aby data byla smazána.
- **Jednodušší přístup k osobním datům** – jednotlivci budou mít více informací o tom, jak jsou jejich údaje zpracovávány. Tyto informace by měly být přístupné jednoduchým a srozumitelným způsobem.
- **Právo vědět o narušení bezpečnosti dat** – Firmy a organizace mají povinnost oznamovat u svých národních dohledových autorit narušení bezpečnosti dat, která mohou ohrozit soukromí jednotlivce.
- **Ochrana dat by design and by default** – Tento bod požaduje po zpracovatelích dat, aby bezpečnostní principy a požadavky zahrnuli do vývoje svých řešení, produktů a služeb. Základními principy jsou především – Anonymizace/Pseudonymizace/šifrování dat.
- **Posílení role státní regulační autority** – Za porušení nařízení může firmám hrozit pokuta od národní autority až 4% jejích celosvětového obratu nebo 20 milionů €.
- **Pozice pověřence pro ochranu osobních dat** (DPO) – je povinná pro **správce** nebo **zpracovatele** pokud mezi vaše hlavní činnosti patří rozsáhlé zpracování citlivých osobních údajů nebo rozsáhlé pravidelné a systematické monitorování fyzických osob (včetně monitorování chování jednotlivců - zahrnuje všechny formy sledování a profilování na internetu i pro účely behaviorálně cílené reklamy) a **orgány veřejné správy**

Pozice DPO

- **Pověřencem pro ochranu osobních údajů může být pracovník vaší organizace nebo jej lze smluvně zajistit externě na základě smlouvy o poskytování služeb.**

- **Pověřencem pro ochranu osobních údajů může fyzická osoba nebo organizace.**

- Pověřenec pro ochranu osobních údajů je přímo podřízen nejvyšším řídícím pracovníkům organizace.

Příklad:
Pověřenec pro ochranu osobních údajů není povinný pokud:

- jako místní praktický lékař zpracováváte osobní údaje svých pacientů

- jako malá advokátní kancelář zpracováváte osobní údaje svých klientů

GDPR sankce

- Za porušení nařízení může firmám hrozit pokuta od národní autority až 4% jejích celosvětového obratu nebo 20 milionů €.
- **Stupňovitý postup při sankcionování**

- varování

- napomenutí

- pozastavení zpracovávání osobních údajů

- pokuta

Pojem narušení (Breaches)

- **Směrnice 2009/136/ES**, kterou se mění **směrnice 2002/58/ES** o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

- do českého právního řádu byla směrnice 2009/136/ES transponována **zákonem č. 468/2011 Sb**., (zákon nabyl účinnosti dne 1. ledna 2012), kterým se mění **zákon č. 127/2005 Sb**., o elektronických komunikací

- **v zákoně o elektronických komunikacích** se tak objevuje „nový nástroj ochrany osobních údajů a soukromí“. Poskytovatelům služeb elektronických komunikacích (Provozovatelé telekomunikačních sítí a poskytovatelé internetových služeb) se výslovně stanoví povinnost řešit případy:

    1. **narušení bezpečnosti osobních údajů (tzv. Data Breach) - ÚOOÚ**

    2. **narušení bezpečnosti sítě (tzv. Security Breach) - ČTÚ**

Definice

- ***„narušením bezpečnosti osobních údajů“*** **-** Směrnice 2002/58/ES ve znění směrnice 2009/136/ES a Nařízení komise č. 611/2013

- ***„porušení ochrany osobních údajů“*** - zákon č. 127/2005 Sb., o elektronických komunikací

- ***„porušení zabezpečení osobních údajů“*** - obecné nařízení o ochraně osobních údajů (GDPR)

Citlivé osobní údaje

- Citlivé osobní údaje jsou:
  - rasový či etnický původ
  - politické názory
  - náboženské vyznání či filozofické přesvědčení
  - členství v odborech
  - zpracování genetických údajů
  - biometrické údaje za účelem jedinečné identifikace fyzické osoby
  - zdraví
  - sexuální život nebo sexuální orientace

Obecně platí, že zpracovávání výše uvedených typů osobních údajů je **zakázáno**.

Výjimku má např. ČSÚ při veřejném sčítání lidu.

Práva pro občany

- na informace o zpracovávání vašich osobních údajů
- získat přístup k vašim osobním údajům, které má někdo v držení
- požádat o opravu nesprávných, nepřesných nebo neúplných osobních údajů
- požádat o vymazání osobních údajů, pokud již nejsou nutné nebo pokud je jejich zpracovávání nezákonné
- vznést námitku proti zpracování osobních údajů pro účely marketingu nebo z důvodů týkajících se vaší konkrétní situace
- požádat o omezení zpracování vašich osobních údajů ve zvláštních případech
- získat své osobní údaje ve strojově čitelném formátu a předat je jinému správci („přenositelnost údajů“)
- požádat, aby rozhodnutí založená na automatizovaném zpracování, která pro vás mají účinky nebo se vás významně dotýkají a která jsou založena na vašich osobních údajích, prováděly fyzické osoby, ne jen počítače (v tomto případě máte právo vyjádřit svůj názor a rozhodnutí napadnout)

Připravenost na GDPR

KASPERSKY lab

CESTA KE SPLNĚNÍ POŽADAVKŮ OBECNÉHO NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ NEBOLI GDPR (GENERAL DATA PROTECTION REGULATION)

PŘIPRAVIT SE NA NAŘÍZENÍ GDPR

S blížícím se květnem 2018 se také krátí termín pro splnění nařízení GDPR, které v té době vstoupí v platnost.

Předpis se dotkne všech firem, které nakládají s osobními údaji občanů EU, a vyžádá si nové procesy a přísnější ochranu těchto dat.

Zatímco právní a IT oddělení po celé Evropě tvrdě pracují na tom, aby nastavila vhodné vnitřní předpisy ve svých organizacích, na jednotlivcích bude zajistit, aby tyto nové předpisy převedli do praxe při své každodenní práci. To bude vyžadovat zásadní změnu v tom, jak zaměstnanci na údaje ve svých organizacích nahlížejí a jak s nimi nakládají.

Následující kroky by měly všem pomoci připravit se na cestu ke splnění GDPR.

ZAČÁTEK

1 **Zjistěte, o co jde**

Zjistěte si, jaké oblasti GDPR jsou pro firmu nejdůležitější

2 **A teď konkrétně**

Vyhodnoťte osobní údaje, s nimiž přicházíte ve své roli do styku

3 **Zkontrolujte svá upozornění o ochraně osobních údajů**

Podle GDPR může být nutné lidem sdělit, co s jejich osobními údaji děláte.

4 **Mějte přehled o svých právech**

GDPR dává občanům EU větší práva v oblasti ochrany osobních údajů a vaši povinností je tato práva chránit. Pokud se řídíte platnými zákony o ochraně osobních údajů, budete už mít z velké části splněno

5 **Poskytujte informace**

Nastavte takové procesy, aby lidé věděli, jaké osobní údaje o nich shromažďujete.

6 **Stanovte právní základ**

Měli byste být schopni vysvětlit právní základ pro zpracování osobních údajů.

7 **Ověřte souhlas**

Zkontrolujte, jak momentálně získáváte souhlas se zpracováním údajů podle aktuální legislativy, a upravte proces podle požadavků GDPR.

8 **Myslete na děti**

GDPR věnuje zvláštní pozornost ochraně osobních údajů dětí. Nastavte systémy, které ověří věk, a používejte k získání souhlasu jazyk, kterému budou děti rozumět.

9 **Ucpěte díry**

Používejte zabezpečený IT systém, který dokáže odhalit, ohlásit a vyšetřit případné úniky osobních údajů.

10 **Vybudujte datovou pevnost**

Implementujte princip „privacy by design" – každý proces, který nakládá s osobními údaji, musí být navržen tak, aby údaje chránil.

11 **Poznejte svého DPO**

Za dodržování ochrany osobních údajů ve vaší organizaci bude odpovídat zmocněnec pro ochranu údajů (DPO). Pravidelně s ním konzultujte, jak práce pokračují.

12 **Myslete globálně**

Zmapujte, kde vaše organizace působí, a zjistěte si, pod který úřad pro dohled na ochranu osobních údajů spadáte.

KONEC: 25. KVĚTNA 2018 A POZDĚJI

Detailní popis 1

- 1 – **Zjistěte, o co jde** (Zjistěte si, jaké oblasti GDPR jsou pro firmu nejdůležitější)
- 2 – **Konkrétně** (Vyhodnoťte osobní údaje s nimiž přicházíte ve své roli do styku)
- 3 – **Zkontrolujte vaše upozornění o ochraně osobních údajů** (Dle GDPR může být nutné lidem sdělit, co s jejich osobními údaji děláte)
- 4 – **Mějte přehled o svých právech** (GDPR dává větší práva a vaše povinnost je tato práva chránit)
- 5 – **Poskytujte informace** (Nastavte takové procesy, aby lidé věděli, jaké osobní údaje o nich shromažďujete)
- 6 – **Stanovte právní základ** (Měli byste být schopni vysvětlit právní základ pro zpracování osobních údajů)
- 7 – **Ověřte souhlas** (Zkontrolujte, jak momentálně získáváte souhlas se zpracováním údajů podle aktuální legislativy a upravde podle GDPR)
- 8 – **Myslete na děti** (GDPR věnuje zvláštní pozornost ochraně osobních údajů dětí – nastavte systémy, které ověřil čas a používejte k získání souhlasu jazyk, kterému budou děti rozumět)
- 9 – **Utěsněte otvory** (Používejte zabezpečený ICT systém, který odhalí, ohlásí a vyšetří případné úniky osobních údajů)

Detailní popis 2

- 10 – **Vybudujte datovou pevnost** (Implementujte princip Privacy by Design – každý proces nakládající s osobními údaji musí být navržen k ochraně těchto údajů)
- 11 – **Poznejte svého DPO** (Za dodržování ochrany osobních údajů ve vaší organizaci bude odpovídat zmocněnec pro ochranu údajů – DPO, pravidelně konzultujte přípravu na GDPR)
- 12 – **Myslete globálně** (Zmapujte oblasti působení vaší organizace a zjistěte pod který úřad pro ochranu osobních údajů spadáte)

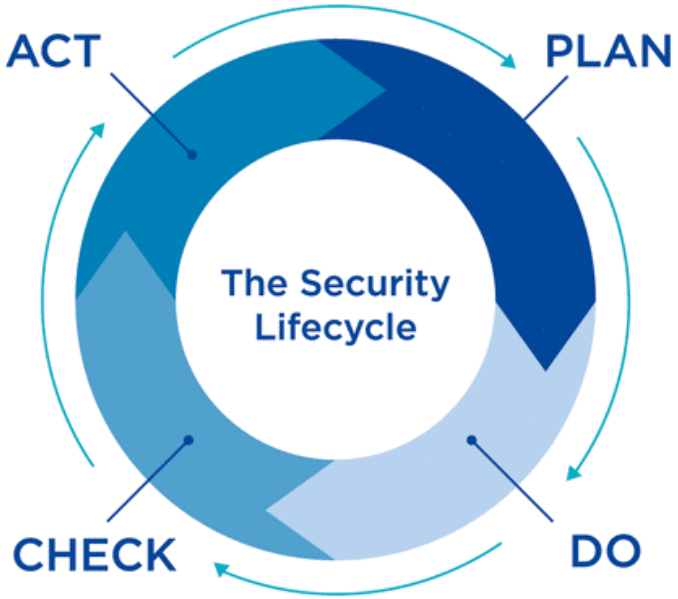
.

.

.

- x – **Podpora procesu přípravy na GDPR – jednoznačně to je zavedení ISMS!**

- Bezpečnostní životní cyklus



GDPR ochrana osobních údajů
General Data Protection Regulation

GDPR v praxi

- **Analýza současného stavu**
  - Datový audit evidence osobních údajů a způsobů zpracování
  - Návrh a doporučení pro dosažení souladu s nařízením GDPR
  - Plán realizace a řízení implementace nápravných opatření
  - Školení odpovědnosti při nakládání s osobními údaji
  - Směrnice a zavedení organizačních pravidel
- **Bezpečnost dat, aplikací a služeb -** Bezpečnostní audit IS, aplikací a služeb
  - Pseudonymizace a šifrování osobních údajů
  - Bezpečnost, dostupnost a odolnost používaných systémů
  - Havarijní plán při porušení ochrany osobních údajů
  - Pravidelné testování účinnosti bezpečnostních opatření
  - Posouzení vlivu na ochranu osobních údajů
  - Hlášení incidentů dozorovým orgánům

GDPR v praxi

- **Pověřenec pro ochranu osobních údajů (DPO)**

  Poradenství správcům a zpracovatelům o jejich povinnostech

  Posouzení vlivu na ochranu osobních údajů

  Monitoring souladu s nařízením GDPR a souvisejícími předpisy

  Odborná školení zaměstnanců zapojených do procesu zpracování

  Komunikace s dozorovými orgány a vedení konzultací

  Kontaktní místo pro subjekty osobních údajů

- **Řízení procesu GDPR -** GDPR není jednorázová akce

  Jednotlivé kroky vedoucí k úspěšnému a dlouhodobému plnění všech povinností vyplývajících z nového nařízení:

  - datový audit
  - analýza rizik
  - plán implementace
  - školení zaměstnanců
  - výkon funkce pověřence
  - zajištění požadované úrovně zabezpečení používaných aplikací a služeb

DPIA - („Dopadová analýza“)

- **DPIA - (Data Protection Impact Assessment)**

  je jedním opatřením posuzujícím vliv na ochranu osobních údajů.

DPIA představuje opatření definované v **čl. 35 GDPR** (Obecného nařízení o ochraně osobních údajů).

Pokud se organizace rozhodne zpracovávat osobní údaje, měla by posoudit, jakým způsobem toto zpracování může zasáhnout do svobod a práv lidí, tedy jak může ovlivnit jejich životy.

Příklad:

- bankovní systémy se scoringovými nástroji
- velké zdravotnické systémy
- velké kamerové systémy

DPIA **není** analýza rizik!

Metodika zpracování DPIA je vytvářena skupinou WP29.

DPIA - pokračování

- Nutnost DPIA provést:

  - systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických sob, které je založeno na automatizovaném zpracování …

  - rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10

  - rozsáhlé systematické monitorování veřejně přístupných prostorů

Lenost či neochota se zajímat o to, proč někdo chce mé osobní údaje a jak s nimi zachází, ve svém důsledku vede k tomu, že organizace se nestarají o ochranu osobních údajů v rozsahu, který by zajistil jejich dostatečnou ochranu.

DPIA – příklad metodiky

- **Jak na DPIA – příklad metodiky**
- 1. rozsah DPIA
  - seznam nositelů osobních údajů (subjekt údajů)
  - typ dokumentů
  - účel zpracování
  - souhlas udělený subjektem údajů
  - popis zpracování osobních údajů
  - posouzení nezbytnosti zpracování
  - bezpečnostní požadavky
  - definování přístupu k údajům
  - zpřístupnění údajů

DPIA – příklad metodiky 2

- 2. popis hodnoceného IS nebo služby
  - základní popis logické a fyzické architektury
  - struktura zpracovávaných informací
  - popis datových toků (manipulace s daty, distribuce dat)
  - popis rozhraní (zabezpečené rozhraní https, …)

Doporučeno:

- 3. popis operačních postupů
  (vytváření a manipulace se záznamy, plány zálohování a obnovy dat, ochrana metadat, …)
- 4. popis interakce se subjektem údajů
- 5. požadavky na soukromí a zabezpečení dat
  (zdrojem je analýza rizik)

Datová analýza

- Datová analýza se bude muset zaměřit na význam samotných dat a především na zjištění vazeb mezi daty.
- Až v kontextu těchto vazeb (mohou to být cizí klíče v databázových tabulkách, ale i logické vazby dat v databázích, anebo dokonce reference v dokumentech či logické vazby mezi dokumenty) identifikujete to, která data jsou osobní, resp. citlivá.

Procesní analýza

- Procesní analýza - v jejím rámci je třeba identifikovat, kdo, jakým způsobem a ke kterým osobním/citlivým datům přistupuje, resp. zpracovává je.
- Tato identifikace může být ještě složitější než datová analýza. Důvodem je, že procesy bývají poměrně složité a nejsou vždy podrobně popsány. Také je třeba do nich zahrnout i automatizované zpracování dat, tvorbu různých reportů, sestav a podobně.

GDPR
dopady

V Brně dne 26. června 2017

Cloud Computing

- Ochrana dat je již delší dobu v zahraničí tématem číslo jedna.
- V Česku se o této problematice začíná hovořit zejména v souvislosti s účinností nového Obecného nařízení o ochraně osobních údajů (GDPR).
- Obecně lze říci, že díky tlaku amerického a především západoevropského trhu jsou mezinárodní dodavatelé cloudových služeb v ochraně dat na velmi vysoké úrovni. Přesto se **nevyplatí** při ochraně dat bezvýhradně spoléhat na zvučné jméno dodavatele a je potřeba ve smlouvě konkrétní práva a povinnosti mezi zákazníkem a dodavatelem osobních údajů vymezit.
  V **čl. 28 GDPR** jsou uvedena ustanovení, která by ve smlouvě s dodavatelem neměla chybět.
- Dobře nastavené omezení náhrady škody ve smlouvě o poskytování cloudových služeb může být klíčovým nástrojem ochrany zákazníka.
  Výše omezení náhrady škody zpravidla odpovídá výši poplatku uhrazeného zákazníkem za poskytované služby za dobu 3 až 12 měsíců.
  V případě smluv s vyšším objemem poskytovaných cloudových služeb bývá často možné vyjednat s dodavatelem i vyšší limity náhrady škody.

Systémy ECM/DMS - definice

- **DMS** - Systémy ***správy dokumentů*** (DMS - Document management systems)
- **ECM** - Systém pro vytěžování, **správu dokumentů,** sdílení a bezpečnou ochranu papírových dokumentů a digitálního obsahu (ECM - Enterprise Content Management System)
- Definice osobních údajů v GDPR je poměrně široká, takže do ní spadají nejen na první pohled zřejmé údaje jako jméno, příjmení, adresa, číslo dokladu totožnosti, identifikační číslo, číslo kreditní karty, lokalizační data a podobně, ale i data, z nichž je možné **přímo nebo nepřímo identifikovat** fyzickou, ekonomickou, kulturní nebo společenskou identitu – což jsou také jakékoliv údaje o nákupech, využívaných službách, vlastněných zařízeních a podobně.
- Citlivé údaje jsou osobní údaje o rasovém, etnickém, národnostním původu, politických názorech, náboženském vyznání, data týkající se zdraví, sexuálního života a orientace, jakož i genetická a biometrická data.
- Data jsou uložena buď ve strukturované formě v databázích, nebo v nestrukturované formě většinou v ECM/DMS systémech
  (ale i ve file serverech, sdílených adresářích, v souborech na pracovních stanicích, v e-mailech a e-mailových schránkách).
  Patří sem i fyzické dokumenty (v papírové podobě).

Systémy ECM/DMS – implementace GDPR

Při implementaci GDPR je třeba zabezpečit naplnění práv subjektů osobních údajů a povinností správce:

- Právo na informace, jaké osobní údaje kdo a jak zpracovává;
- právo na opravu chybných osobních údajů;
- právo na smazání (právo být zapomenut);
- právo na odvolání souhlasu se zpracováním osobních údajů;
- právo na přenos údajů;
- povinnost informovat subjekty osobních údajů o „data breach“ – neoprávněném zpracování, přístupu nebo použití osobních údajů.

Systémy ECM/DMS

Z pohledu ECM/DMS a nestrukturovaných dat je třeba:

- Vědět, kdo, v jakých případech (procesech), jak a které dokumenty s osobními údaji používá, a na požádání tyto informace poskytnout;
- opravit chybné osobní údaje, pokud jsou například údaje uložené v atributech dokumentů;
- smazat všechny dokumenty, které obsahují v atributech nebo v samotném obsahu osobní údaje, a také všechny dokumenty, které se týkají osoby žádající o smazání;
- v případě odvolání souhlasu se zpracováním údajů omezit, resp. zakázat další zpracování všech dokumentů, které obsahují v atributech nebo v samotném obsahu osobní údaje, a také všech dokumentů, které se týkají dané osoby;
- poskytnout všechny dokumenty, které obsahují v atributech nebo v samotném obsahu osobní údaje, a také všechny dokumenty, které se týkají osoby žádající o přenos;
- v případě „data breach“ dokázat identifikovat, čí a které údaje byly postiženy, a v termínu informovat o této skutečnosti všechny subjekty, které byly „data breach“ dotčeny.

Systémy ECM/DMS – datová analýza

Datová analýza se bude muset zaměřit na význam samotných dat a především na zjištění vazeb mezi daty.

Až v kontextu těchto vazeb (mohou to být cizí klíče v databázových tabulkách, ale i logické vazby dat v databázích, anebo dokonce reference v dokumentech či logické vazby mezi dokumenty) identifikujete to, která data jsou osobní, resp. citlivá.

Příkladem mohou být třeba data o zařízeních a IP adresách, které přistupovaly na stránky vašeho e-shopu. Samy o sobě to osobní údaje nejsou, ale v kombinaci s údaji o času přístupů, resp. s daty z authentication cookies, to už osobní data mohou být. A tato data mohou být dokonce spojena přes reference i s konkrétními uživatelskými profily, v jejichž rámci ukládáte kromě přístupových/identifikačních údajů i údaje o dodací adrese, fakturační adrese, platební údaje a zákazníkovy objednávky – to už jednoznačně osobní údaje jsou.

Systémy ECM/DMS – procesní analýza

Procesní analýza - v jejím rámci je třeba identifikovat, kdo, jakým způsobem a ke kterým osobním/citlivým datům přistupuje, resp. zpracovává je.

Tato identifikace může být ještě složitější než datová analýza. Důvodem je, že procesy bývají poměrně složité a nejsou vždy podrobně popsány. Také je třeba do nich zahrnout i automatizované zpracování dat, tvorbu různých reportů, sestav a podobně.

Samostatnou kapitolou jsou dokumenty, které nejsou uloženy v ECM/DMS, případně jako nejjednodušší DMS je používán file server a sdílené adresáře.

Tady bude mimořádně těžké identifikovat, které dokumenty obsahují osobní, nebo dokonce citlivé údaje, resp. bude třeba implementovat SW, který identifikaci zabezpečí.

V tomto případě hovoříme o netriviálním vytěžení obsahu dokumentů a důkladné datové analýze. Obdobná situace platí pro obsah dokumentů na pracovních stanicích, e-mailech a e-mailových schránkách, v různých reportech a podobně.

Systémy ECM/DMS – požadavky GDPR

- GDPR **zpřísňuje požadavky** na obsah a formu souhlasu se zpracováním osobních údajů.
  Hlavně klade důraz na to, že souhlas musí jasně definovat konkrétní účel, pro který budou osobní data použitá, musí být jednoznačný, svobodný a poskytuje se pouze na dobu určitou. Už udělené souhlasy bude třeba harmonizovat. A právě ukládání souhlasů a sledování termínů platnosti souhlasů považuji za další oblast, pro niž je ECM/EMS ideální platforma.

- Za největší hrozbu GDPR je případ, kdy se zneužije pro konkurenční boj. Je jednoduché si představit, že budou posílána oznámení na konkurenční společnosti o tom, že nesplnily některé z práv nebo povinností. Případně po ohlášení „data breach“ některou společností se objeví další osoby „postižené data breach“, které oznámí úřadům, že nebyly informovány.

Systémy ECM/DMS – příprava na GDPR (shrnutí)

1. Posouzení (pro naplnění práv a povinností), zda organizace pracuje s osobními, resp. citlivými, daty.
2. Klíčová bude analýza dat a procesů za účelem identifikace, kdo, jak a s jakými daty pracuje.
3. Do datové analýzy je třeba zahrnout všechny formy dat, to znamená strukturovaná data, ale i nestrukturovaná data a stejně tak fyzické dokumenty.
4. Neméně důležitá bude příprava metodik, pravidel a postupů, které detailně popíší postup organizace při implementaci GDPR.
5. Pravděpodobně nevyhnutelná bude úprava procesů, resp. systémů tak, aby došlo k zabezpečení osobních a citlivých údajů a minimalizoval se potenciál toho, že dojde k „data breach“.
6. A nakonec bude třeba nad daty implementovat jednotlivá práva a povinnosti, tak aby organizace byla na GDPR připravená.

GDPR se dá chápat nejen jako povinnost nebo hrozba, ale i jako příležitost pro IT svět ke změně současného přístupu, kdy se shromažďují obrovské množství dat – často zbytečných a pouze kvůli tomu, že by se nám v budoucnosti mohla hodit. GDPR je způsob, jak se vrátit nohama zpátky na zem a pracovat jenom s potřebnými daty, a tím si vlastně **zjednodušit život**.

ePrivacy

ePrivacy

European seal for your privacy

ePrivacy

14. 4. 2017 - Pracovní skupina WP29 v dubnu 2017 schválila stanovisko k revizi směrnice 2002/58/ES o soukromí a elektronických komunikacích. Návrh nového nařízení **ePrivacy**, které předložila Evropská komise v lednu 2017, by měl poskytnout uživatelům elektronických komunikací vysokou úroveň ochrany soukromí a rovné podmínky pro všechny účastníky na trhu.

WP29 ve svém stanovisku kladně ohodnotila zvolenou formu nařízení namísto směrnice, dojde tak k **souladu s GDPR**.

Rozšíření oblasti působnosti na tzv. nové komunikační služby „**Over-the-Top**" (**OTT**) - typu Skype, WhatsApp, Gmail, Facebook, Viber, Messenger aj., které budou muset splňovat stejná kritéria jako telefonní operátoři, co se týče důvěrnosti komunikace uživatelů.

Citace ze stránek ÚOOÚ

Podstatou ePrivacy je, aby měli občané možnost vědomě odsouhlasit, že o nich smějí poskytovatelé elektronických komunikací shromažďovat data.

Ochrana soukromí bude zaručena nejen u obsahu, ale také u metadat, jako jsou například čas a místo hovoru.

Pokud uživatel neudělí souhlas se zpracováním těchto údajů, budou muset být tato data anonymizována nebo vymazána.
Výjimkou budou logicky případy, kdy jsou taková data potřebná pro samotný provoz služby či vyúčtování.

ePrivacy – dopady 1

Metadata
Ochrana soukromí se podle nařízení nemá vztahovat pouze na obsah elektronické komunikace, ale i na metadata, která z elektronické komunikace vyplývají.
Těmi mohou být například **údaje o čase, místě a trvání hovorů nebo údaje o navštívených internetových stránkách** apod.

V případě, že bude uživatel se zpracováním údajů souhlasit, mohou poskytovatelé telekomunikačních služeb tuto možnost využít ke komerčním účelům.
Příkladem takového využití je tvorba tepelných map zachycující přítomnost fyzických osob a identifikovat tak jejich dopravní pohyby v určitých směrech během určitého časového období. Orgány by tak tato data mohly využít pro vytvoření výstavby nových dopravních infrastruktur v závislosti na vytíženosti jednotlivých úseků.

Výjimkami pro účely zpracovávání metadat patří ta data, která jsou využívána z důvodu vyúčtování určitých služeb, odhalení podvodného užívání telekomunikačních služeb nebo je-li to nezbytné pro splnění povinných požadavků na kvalitu služby podle evropských předpisů.

ePrivacy – dopady 2

Cookies
V současné době je většina internetových stránek opatřena množstvím žádostí o souhlas uživatelů s používáním cookies, které představuje do jisté míry určitou personalizaci obsahu včetně identifikace jednotlivých uživatelů a jejich sledování.
Návrh nařízení ePrivacy by mělo nově uživatelům internetu umožnit **přehledněji kontrolovat svá nastavení sledování cookies** a další identifikátory.

Návrh nařízení s sebou přináší v souvislosti s používáním cookies jisté výjimky, a to v případech, kdy cookies nezasahují do soukromí uživatelů a zlepšují služby na internetu. Jedná se zejména o tzv. **cookies prvních stran**, která jsou uvedená na adresním řádku webové stránky a mohou jimi být např. možnosti zapamatování historie nákupu online.

Nicméně druhý typ cookies, tzv. **cookies třetích stran** (third party cookies), už do uvedené výjimky nespadá a k jeho sledování **bude vyžadován uživatelův souhlas**. Cookies třetích stran pocházejí z jiných webů jejichž položky jsou na navštívené stránce vloženy. Uživatelé internetových stránek budou mít možnost sledování cookies třetích stran instalovat v samotném zařízení a zároveň i prohlížeče a další aplikace umožňující přístup k internetu mají o této možnosti uživatele informovat.

ePrivacy – dopady 3

Ochrana proti nevyžádaným sdělením

Klíčový souhlas uživatele by měl v rámci elektronické komunikace platit i v případě reklamních sdělení či hovorů z call center formou přímého marketingu.

Za účelem ochrany proti spamům se budou muset v budoucnu poskytovatelé komunikačních služeb určitým způsobem identifikovat, ať už v podobě zobrazení čísla volajícího nebo uvést zvláštní kód, který označí skutečnost, že se jedná o marketingové volání.

V případě, že uživatel dá k zpracovávání údajů souhlas, musí mít zároveň možnost tuto volbu později i odvolat.

Shrnutí problematiky GDPR

Takže, co byste měli udělat proto, abyste byli co nejdříve v souladu s požadavky GDRP a moc vás to nestálo?

1. **Jmenujete pověřence pro ochranu osobních údajů (DPO)**, ten s vámi udělá soupis typů osobních údajů, které spravujete, za jakým účelem, po jak dlouhou dobu, a v jakých systémech**.** Zjistěte si, kdy opravdu musíte pověřence jmenovat.

2. **Zamyslete nad tím, co by se mohlo stát, kdyby došlo k úniku osobních údajů**, které zpracováváte, především jaký by to mohlo mít dopad do života osob.

3. **Zkontrolujete, že máte právní základ anebo platný souhlas** ze strany těch, jejichž osobní údaje zpracováváte, a pokud ne, tak je o souhlas požádejte.

4. **Vyhodnoťte úroveň zavedení jednotlivých bezpečnostní opatření organizační a technické povahy**. A pokud zjistíte, že některé údaje nejsou dostatečně chráněny, tak **zaveďte příslušná opatření**.

Takže opět platí – **zaveďte si ISMS!**

BRANDNEW

GDPR
certifikace

V Brně dne 30. listopadu 2017

enisa

ENISA

- ***ENISA*** **-** The European Union Agency for Network and Information Security
- ***www.enisa.europa.eu***
- **Recommendations on European Data Protection Certification**
- Datum vydání – listopad 2017 (Version 1.0)
- Obsahuje základní doporučený koncept postupu certifikace GDPR dle **čl. 42** a **43** GDPR
- Certifikace je postavena na normě (ČSN) **ISO/IEC 17067:2013** Posuzování shody - Základní principy certifikace produktu a směrnice pro certifikační schémata
- Norma popisuje základní principy certifikace produktu a poskytuje pokyny k pochopení, vypracování, provozování nebo udržování certifikačních schémat produktů, procesů a služeb.

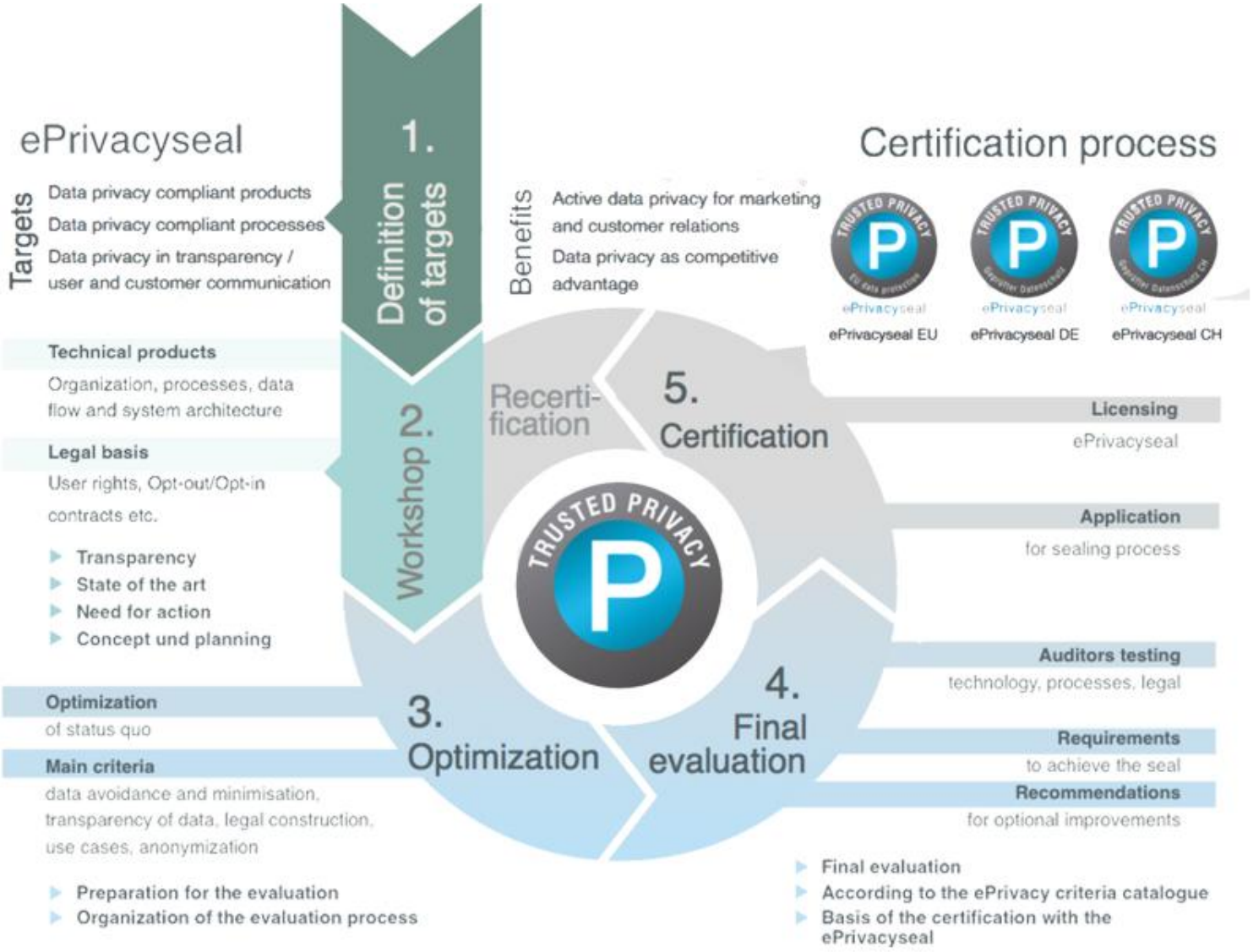
ENISA

- Certifikační schéma – pravidla, procedury a řízení pro potřeby CF.
- Doporučení pro CF schéma vychází z:
  - data subjects rights (čl. 15-22)
  - data security (čl. 32)
  - data protection by design and by default (čl. 25)
- Platnost certifikace je stanovena na 3 roky.
- Certifikační symbol (logo) dle směrnice 920/2014 (definuje elektronické symboly)
- Akreditace certifikační autority se řídí směrnicí 765/2008: Accreditation Regulation
- Akreditace dle:
  - autority pro ochranu dat - European Data Protection Board (EDPB)
  - mezinárodní autority (DPA) dle normy ISO/IEC 17067:2013

ENISA

- Certifikační kritéria:
  - dle ISO/IEC 27001 (ISMS)
  - dle ISO/IEC 27018 (PII)
  - EuroPrise
  - CNIL (francouzská varianta)
  - ICO
  - ePrivacy EU
- ePrivacy EU

ePrivacy


ePrivacyseal
Targets
Data privacy compliant products
Data privacy compliant processes
Data privacy in transparency / user and customer communication
1. Definition of targets
Technical products
Organization, processes, data flow and system architecture
Legal basis
User rights, Opt-out/Opt-in contracts etc.
2. Workshop
Transparency
State of the art
Need for action
Concept und planning
Optimization
of status quo
Main criteria
data avoidance and minimisation, transparency of data, legal construction, use cases, anonymization
3. Optimization
Preparation for the evaluation
Organization of the evaluation process
4. Final evaluation
Auditors testing
technology, processes, legal
Requirements
to achieve the seal
Recommendations
for optional improvements
Final evaluation
According to the ePrivacy criteria catalogue
Basis of the certification with the ePrivacyseal
5. Certification
Licensing
ePrivacyseal
Application
for sealing process
Recerti-fication
Benefits
Active data privacy for marketing and customer relations
Data privacy as competitive advantage
Certification process
ePrivacyseal EU
ePrivacyseal DE
ePrivacyseal CH
TRUSTED PRIVACY
P

ePrivacy - aplikovatelnost

- Aplikovatelnost na modely:
  - App providers
  - Big data applications and data providers
  - Cloud solutions
  - Connected cars
  - CRM systems
  - Digital platforms
  - eHealth
  - Face recognition/video analysis
  - Online trade/e-commerce
  - Online and Retail marketing
  - Social media
  - Telecommunications
  - TV/video
  - ….

Literatura

- ENISA (European Union Agency For Network and Information)
- **Recommendations on European Data Protection Certification**

  Good Practices and Recommendations on the Security of Big Data Systems
- 11/2017
- ISBN 978-92-9204-238-7