Nařízení EU (GDPR)

RNDr. Igor Němec

Praha hotel Troja, 16. 5. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Cíl semináře

GDPR solutions

Komplexní pochopení problematiky zpracovávání osobních údajů

- Celé nařízení není samoúčelné
- Problematika není ani tak složitá jak by napovídal rozsah textu GDPR
- Odstranění řady fám a nepřesností, které se šíří sdělovacími prostředky

Není to jenom teorie, ale budeme to umět prakticky uchopit

- Co je potřeba udělat i když plním zákon na ochranu osobních údajů
- Jaké dokumenty musíme vypracovat
- Na co nesmíme zapomenout

O čem to vlastně celé je?

- Zpracovávat osobní údaje lze na základě předem stanoveného **účelu**, **zákonným** způsobem a to umět **doložit.**

Obsah přednášky

GDPR solutions

Úvod do problematiky

- Ochrana soukromí
- Historie ochrany osobních údajů
- Nařízení GDPR
- Základní principy GDPR

Správce jeho povinnosti

- Záznamy o zpracování
- Posouzení vlivu na ochranu osobních údajů
- Podniková pravidla
- Předběžná konzultace s úřadem, na ochranu osobních údajů
- Pověřenec ochrany osobních údajů
- Sankce
- Dotazy

Soukromí

GDPR solutions

- **Soukromí** je osobní oblast jednotlivce nebo skupiny (například rodiny). V češtině zahrnuje potřebu a právo chránit informace o své osobě, jakož i vlastní tělo a čas, vlastní prožitky a území před zveřejňováním a především před zneužíváním.

Ochrana soukromí

- Ochrana soukromí a jeho respektování vychází z uznání, že každý člověk má přirozenou důstojnost a každému náleží rovná práva.

ve smyslu informačním:

Právo rozhodnout o tom, komu zpřístupníme informace, které se nás týkají a právo bránit se užívání a šíření takových informací bez našeho souhlasu

Listina lidských práv a svobod

- Článek 7:

  (1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

- Článek 10:

  (2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

  (3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Listina lidských práv a svobod

GDPR solutions

- Článek 13:

  Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Soukromí v zákonech

- **Trestní zákoník 40/2009 Sb. Paragrafy 180 – 184:**
  - neoprávněné nakládání s osobními údaji
  - poškození cizích práv (uvedení v omyl)
  - porušení tajemství dopravovaných zpráv (listovní komunikace, elektronická komunikace, počítačová data)
  - porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (fotografie, film)
  - pomluva (sdělování nepravdivých údajů)

Soukromí v zákonech

- **Občanský zákoník 89/2012 Sb.**
  - § 84 – 90 přímo hovoří o zákazu zasahování do soukromí a šíření podobizny či písemnosti osobní povahy, stejně tak zvukového či obrazového záznamu bez svolení člověka.
  - § 89 – 89 současně hovoří o případech, ve kterých je možné výše zmíněné záznamy pořizovat a používat i bez souhlasu člověka, jako je např. využití těchto záznamů při chránění jiných práv nebo právem chráněných zájmů jiných osob

Co hrozí?

GDPR solutions

- **Krádež identity** - vydávání se za někoho jiného na základě:
  - ukradených listin a dokumentů
  - získání cizí počítačové identity (např. zneužití přístupových údajů)

Historie ochrany oú

- Švédský zákon o svobodném přístupu k informacím z roku 1776 (stanovil i princip, že vláda nemá zpracovávat žádné informace nad rámec oprávněných zájmů)
- **Úmluva o ochraně lidských práv a základních svobod** (4. 11. 1950)
- Hessensko – první německý zákon na ochranu osobních údajů (1970)
- Spolkový zákon z 27. 1. 1977 (Německo)
- **Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů**
- **Zákon č. 101/2000 sb. O ochraně osobních údajů**
- **GDPR (General Data Protection Regulation) = Obecné nařízení o ochraně osobních údajů, vydané Evropským parlamentem a Radou EU v roce 2016**

GDPR

GDPR solutions

- **GDPR** (General Data Protection Regulation) = Obecné nařízení o ochraně osobních údajů, vydané Evropským parlamentem a Radou EU **v roce 2016**
- Účinné od 25. května 2018

- Přináší řadu nových povinností a nových sankcí (jako např. až 20 mio Euro / 4% celosvětového obratu, transparentnost, vedení záznamu činnosti o zpracování, ohlášení porušení zabezpečení či úniku, pověřenec)

- Jednotné pro celou Evropu
- **Přímo aplikovatelné** – nejsou třeba žádné další předpisy, zákony, výklady ..

A další předpisy

GDPR solutions

- Adaptační zákon pro GDPR
- Implementace směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů
- Důležitá pravidla
  - Věk dítěte pro souhlas se zpracováním os. údajů v souvislosti s nabídkou služeb informační společnosti: **od 13 let**
  - **Veřejný subjekt**: ministerstva a další ústřední orgány státní správy a jim podřízené úřady, veřejné sbory, ozbrojené sbory, veřejné školy, kraje, obce, komory, soudy (kromě soudního rozhodování), ČNB, NKÚ, Veřejný ochránce práv atd.

GDPR solutions

Účel, zákonnost, doložit

GDPR – věcná působnost

GDPR solutions

- Vztahuje se na zcela nebo částečně **automatizované** zpracování osobních údajů a na **neautomatizované** zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny
  - automatizované zpracování – zpracování elektronickými prostředky (PC)
  - neautomatizované (manuální) – zpracování v „papírové“ podobě

GDPR – věcná působnost

- **Nevztahuje se na** zpracování osobních údajů prováděné fyzickou osobou v průběhu **výlučně osobních či domácích činností**
  - např. vytváření vlastních adresářů nebo seznamů
  - takto shromážděné údaje však by neměly být předmětem obchodní činnosti

- **Nevztahuje se** na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a **kontaktních údajů** právnické osoby.

GDPR – osobní působnost

- Upravuje práva a povinnosti některých subjektů, zejm. pak **subjektu údajů**, **správců a zpracovatelů** osobních údajů

  - **Správcem** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

  - **Zpracovatelem** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

GDPR – smlouva správce - zpracovatel

Smlouva stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce;

b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost;

c) přijme všechna náležitá opatření k zabezpečení dat;

d) podá informaci o případném zapojení dalšího zpracovatele;

e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;

f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36 (Zabezpečení zpracování), a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo EU nebo členského státu nepožaduje uložení daných osobních údajů;

h) poskytne správci možnost auditu, včetně inspekcí, prováděné správcem nebo jím pověřeným auditorem;

GDPR – místní působnost

- Nařízení dopadne na každého správce nebo zpracovatele osobních údajů, který má provozovnu v EU

- Nová úprava bude platit i pro správce nebo zpracovatele, kteří nejsou usazeni v EU, ale **nabízejí zboží nebo služby subjektům údajů v EU nebo monitorují jejich chování**

GDPR – další základní pojmy

Zpracování osobních údajů = jakákoliv operace s osobními údaji

- Shromáždění, Zaznamenání, Nahlédnutí, Uchovávání, Strukturování, Uložení, Uspořádání, Pozměnění, Šíření, Zpřístupnění, **profilování** .....

Anonymní data nejsou osobními údaji

- je třeba přihlédnout ke všem prostředkům identifikace, které lze rozumně předpokládat s ohledem na
  - stav technologie,
  - vynaložený čas,
  - náklady a
  - oprávněné potřeby / zájmy dalších správců ...

Osobní údaj = jakékoliv informace o **fyzické osobě** z níž lze tuto osobu identifikovat

- Jméno, příjmení, pohlaví, věk, telefon, e-mail, fotografie, adresa, **IP adresa**, uživatelské jméno ....

Zvláštní kategorie osobních údajů

- rasa, etnický původ, politické názory, náboženské a filosofické přesvědčení, členství v odborech, genetické a **biometrické údaje**, zdravotní stav, sexuální orientace ..

GDPR – osobní údaj ?????

- 1944/2009 Nejvyšší správní soud

- I. Služební hodnocení policisty podle § 15 zákona č. 186/1992 Sb., o služebním poměru příslušníků Policie České republiky, zpravidla obsahuje osobní a citlivé údaje, a je proto vyloučeno z působnosti zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
- II. **Jméno a příjmení fyzické osoby v kombinaci s číslem občanského průkazu není osobním údajem ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů.**

GDPR - kdy lze zpracovávat osobní údaje?

- GDPR stanoví předpoklady, které musí být splněny, aby mohly být zpracovávány osobní údaje

- Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány
- korektně
- na základě legitimního **účelu**
- **zákonným** způsobem
- transparentním způsobem

GDPR - účel

GDPR solutions

- **Povinnost zpracovávat osobní údaje pouze pro konkrétní a legitimní účely**

- Osobní údaje musí být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely
- Nutno stanovit účel na začátku zpracování
- Ke každému účelu se váže právní titul zpracování
- Další zpracování – nový účel musí navazovat na původní, nutno mít také právní titul

GDPR – s účelem souvisí

GDPR solutions

- **Minimalizace**
  - Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány
- **Přesnost**
  - Osobní údaje musí být přesné a v případě potřeby aktualizované
  - Nutno zvažovat rizika pro subjekty údajů a povahu zpracovávaných údajů
- **Doba uchovávání**
  - Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu **ne delší, než je nezbytné** pro účely, pro které jsou zpracovávány
  - Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely
  - Pouze za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů

GDPR - zákonnost

- subjekt údajů udělil **souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů
- zpracování je nezbytné pro **splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
- zpracování je nezbytné pro splnění **právní povinnosti**, která se na správce vztahuje
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
- zpracování je nezbytné pro účely **oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě

GDPR – zákonnost - souhlas

- **Souhlas**
  - Jakýkoli **svobodný, konkrétní, informovaný a jednoznačný** projev vůle

  - Kdy **není svobodný**:
    - „s uzavřením této smlouvy souhlasíte se zpracováním ...“
    - souhlas jako zaškrtávací pole a nelze pokračovat bez zaškrtnutí
    - se zákazníkem není uzavřena smlouva pokud souhlas neposkytne
  - Kdy **není konkrétní**
    - Není jasný účel „.. tímto souhlasíte se zpracováním pro interní potřebu ...“
    - Není jasný správce „.. tímto souhlasíte se zpracováním veškerými třetími stranami ...“
  - Kdy **není jednoznačný**
    - Není jasně oddělen od jiných prohlášení
    - Byl dán mlčením/implicitně
    - Je začleněn do nepřehledného textu

GDPR – zákonnost - souhlas

- **Souhlas**
  - Kdy **je informovaný** (Článek 13 odstavec 1)
  - Dotčená osoba musí být schopna posoudit, jaké má pro ní zpracování důsledky ..
    - kdo je správce, kdo je DPO + kontaktní údaje
    - jaký jsou účely
    - jaké jsou oprávněné zájmy
    - kdo jsou příjemci nebo kategorie příjemců
    - Případně úmysl předat data do 3. země

- Správce musí být schopen po celou dobu zpracování souhlas **doložit!!!**

GDPR – zákonnost - souhlas

- **Souhlas u dětí**
  - **U on-line služby nabízené dítěti a souhlas u dítěte mladšího 16 let ?!**
  - Souhlas musí schválit nebo vyjádřit osoba s rodičovskou zodpovědností
  - Správce musí vyvinout **přiměřené úsilí** k ověření souhlasu rodiče

- Pozn.: Souhlas nositele rodičovské zodpovědnosti by neměl být nutný v případě preventivních či poradenských služeb nabízených přímo dětem.

- **Souhlas o zpracování zvláštní kategorie údajů**
  - Musí být výslovný

GDPR – zákonnost – souhlas ve škole

- **Příklady:**

- údaje požadované při účasti žáků a studentů v soutěžích, olympiádách, SOČ apod., pokud reprezentují školu (jméno a příjmení, datum narození).
- zveřejnění výtvarných a obdobných děl žáků na výstavě v galerii
- údaje o žácích, studentech, pedagogických pracovnících poskytované cestovním kancelářím
- publikace fotografií žáků za účelem marketingové propagace školy (reklamní letáky apod.)
- údaje zpracovávané v souvislosti s pořádáním letních škol a podobných akcí

GDPR – zákonnost – souhlas ve škole

- **Příklad:**

- „Souhlasím po dobu školního roku x/y se zveřejněním fotografií mého dítěte pořízených během akcí mateřské školy na webových stránkách školy, pokud nebude podobizna dítěte spojena s jeho jménem.“

GDPR – zákonnost - smlouva

- **Smlouva**
  - Osobní údaje, které jsou nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů
  - V souvislosti úmyslem smlouvu uzavřít
  - Týká se pouze zpracování prováděné za **účelem** splnění závazku nebo jeho uzavření, zásadní je identifikace cíle závazku

- **Souhlas není potřeba** pokud se nejedná o
  - Zpracování zvláštní kategorie osobních údajů
  - Předání údajů třetím osobám pro marketingové účely

GDPR – zákonnost - zákon

- **Plnění právních povinností správce**
  - Zpracování nezbytné pro splnění **právní povinnosti, kterou správci ukládá zákon**
  - Povinnost musí být stanovena ze zákona, může být ale konkretizována prováděcím právním předpisem
  - Musí se jednat o právní povinnost stanovenou právem EU nebo právním předpisem ČR

GDPR – zákonnost – důležité zájmy

- **Životně důležité zájmy subjektu údajů**
  - Pokud zpracování zjevně nemůže být založeno na jiném právním základě
  - Situace, kdy je třeba zpracovat osobní údaje subjektu údajů za účelem předejití újmy na životě subjektu údajů nebo jiné osoby
  - Např. záchrana života, humanitární účely, katastrofy atd.

- **Není nutno získat dodatečný souhlas**

GDPR – zákonnost – třetí strana

- **Oprávněné zájmy správce či třetí strany!**
  - Nemusí se jednat jen o ochranu určitého práva nebo právem chráněného zájmu, správce si může určit vlastní, subjektivní oprávněný zájem
  - Lze uplatnit pouze za předpokladu, že nad těmito oprávněnými zájmy nepřevažují zájmy nebo základní práva a svobody subjektu údajů

GDPR – zpracování zvláštních kategorií

- **Zakazuje se**
- zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

GDPR – zpracování zvláštních kategorií

- **Výjimka:**
  - Zpracování je ze zákona v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany
  - S **výslovným** souhlasem
  - Je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas
  - Zpracování provádí v rámci svých **oprávněných činností** a s vhodnými zárukami neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt
  - Zpracování se týká osobních údajů **zjevně zveřejněných subjektem údajů**
  - Zpracování je nezbytné pro účely **preventivního** nebo pracovního lékařství

GDPR – zpracování zvláštních kategorií

- **Další výjimka:**
  - Zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví
  - zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu se zákonem

- Zpracování osobních údajů týkajících se **rozsudků v trestních věcech** a trestných činů či souvisejících bezpečnostních opatření se může provádět pouze pod dozorem orgánu veřejné moci.
- Jakýkoli **souhrnný rejstřík** trestů může být veden pouze pod dozorem orgánu veřejné moci.

GDPR – zvláštní kategorie - škola

- **Příklady:**

- poruchy učení
- údaje o omezeních ve stravování či specifické stravovací plány (které mohou mít souvislost jak se zdravotním stavem, tak např. s filozofickým či náboženským přesvědčením)
- sociální situace v rodině

GDPR – integrita a důvěrnost

GDPR solutions

- Osobní údaje musí být zpracovávány způsobem, který zajistí náležité **zabezpečení** osobních údajů
- Ochrana pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

GDPR – integrita a důvěrnost

GDPR solutions

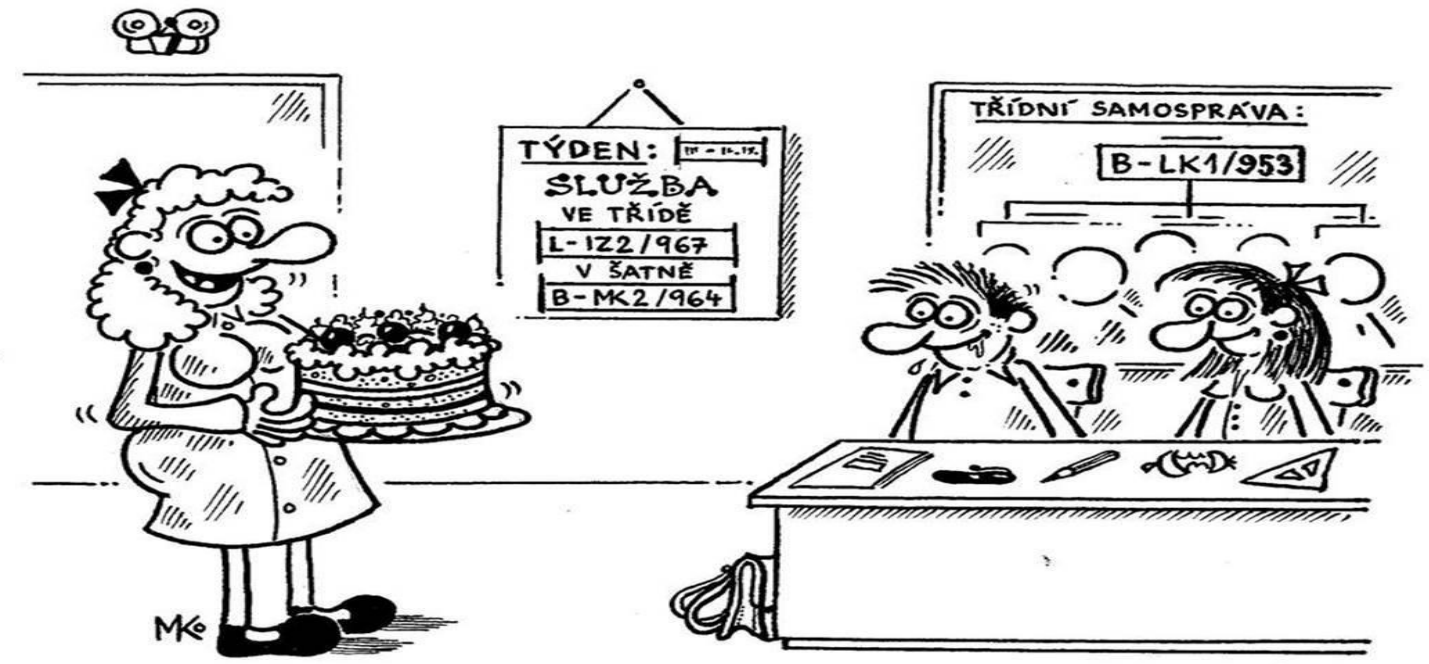
- **Povinnost zabezpečit osobní údaje**
  - Správce a zpracovatel osobních údajů jsou povinni tyto údaje chránit
  - Za tímto účelem musí zavést vhodná technická a organizační opatření (přiměřeně k rizikům)
  - Správce a zpracovatel při zavádění opatření přihlédnou také ke stavu techniky, nákladům na jejich zavedení, povaze, rozsahu, kontextu a účelům zpracování osobních údajů
- Pokud je to vhodné, správce a zpracovatel osobních údajů zajistí
  - Pseudonymizaci a šifrování osobních údajů
  - Neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
  - Obnovitelnost a dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů
  - Pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření
- **Hlásit úřadu incident do 72 hodin!**

GDPR – integrita a důvěrnost

- **Hlásit úřadu incident do 72 hodin!**

- Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, **ledaže je nepravděpodobné**, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

GDPR – integrita a důvěrnost



„DNES, MILÉ DĚTI, PROŽÍVÁME OPRAVDU RADOSTNÝ DEN: NAŠE ŠKOLA DOSTALA POCHVALU OD ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ - A VAŠE SPOLUŽAČKA **I-XB1/963** DNES SLAVÍ NAROZENINY!"

GDPR - transparentnost

- Všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků

GDPR – právo na informace

- **Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů (Článek 13)**

- **KDY?:** V okamžiku získání osobních údajů
- totožnost a kontaktní údaje správce nebo zástupce; kontaktní údaje pověřence; účely zpracování a právní základ pro zpracování; oprávněné zájmy správce nebo třetí strany; příjemce nebo kategorie příjemců; **úmysl správce předat osobní údaje** do třetí země nebo mezinárodní organizaci.
- doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
- **existence práva odvolat kdykoli souhlas**, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
- **existence práva podat stížnost** u dozorového úřadu;

GDPR - právo na informace

- **Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů (Článek 13)**

- skutečnost, zda poskytování osobních údajů je **zákonným či smluvním požadavkem**, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;
- skutečnost, že dochází k **automatizovanému rozhodování**, včetně profilování a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

To vše neplatí pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má!

GDPR - právo na informace

- **Informace poskytované v případě, že osobní údaje nejsou získány od subjektu údajů (Článek 14)**

- **KDY?** :
  - **v přiměřené lhůtě** po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
  - **nejpozději** v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
  - nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

- Nepoužije se když je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů (např. ÚZIS).

GDPR - právo na přístup

GDPR solutions

- Správce poskytne **kopii** zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů **může správce účtovat přiměřený poplatek** na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

- Právem získat kopii uvedenou v odstavci nesmějí být nepříznivě dotčena práva a svobody jiných osob.

GDPR - právo na přístup

- Je třeba stanovit postupy, které by usnadnily výkon práv subjektů:

Správci by měla být uložena povinnost reagovat na žádosti subjektu údajů bez zbytečného odkladu a nejpozději **do jednoho měsíce a uvést důvody v případě, že nemá v úmyslu těmto žádostem vyhovět.**

GDPR – další práva subjektu údajů

- Právo na výmaz **(„právo být zapomenut“)**
  - Jestliže správce osobní údaje zveřejnil a je povinen je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace
  - Ustanovení umožňuje jednotlivcům, aby na základě jejich žádosti provozovatelé webových prohlížečů odstranili některé osobní údaje z vyhledávače a zároveň informovali správce údajů, kteří údaje zpracovávají, aby vymazali veškeré odkazy na tyto osobní údaje včetně jejich kopií
- **Právo na omezení zpracování**
- **Právo na přenositelnost údajů**

Právo na přenositelnost údajů

GDPR solutions

- Subjekt údajů má **právo získat** osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a **právo předat** tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:
  - zpracování je založeno na souhlasu;
  - zpracování je založeno na smlouvě;
  - **a** zpracování se **provádí automatizovaně**.
- Při výkonu svého práva na přenositelnost údajů má subjekt údajů **právo** na to, aby osobní údaje byly **předány přímo jedním správcem správci druhému**, je-li to technicky proveditelné.
- Právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

GDPR – další práva subjektu údajů

GDPR solutions

- Subjekt údajů **má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování**, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká pokud to není:
  - nezbytné k uzavření nebo plnění smlouvy
  - povoleno ze zákona
  - založeno na výslovném souhlasu subjektu údajů

GDPR – další práva subjektu údajů

Uvedená práva lze omezit, upravit právem členského státu či právem EU

- Již nyní v zákonech v gesci MZ ČR existují konkrétní omezení některých práv subjektu údajů.
- Typickým příkladem je omezení práva na výmaz stanovením lhůt pro vedení zdravotnické dokumentace či pro anonymizaci osobních údajů v případě NZIS dle zákona č. 372/2011 Sb., o poskytování zdravotních služeb a podmínkách jejich poskytování (zákon o zdravotních službách) a navazující prováděcí vyhlášky.

GDPR – desatero pro lékaře

GDPR solutions

- Tato ordinace zpracovává Vaše osobní údaje jen pro účely poskytování zdravotní péče pacientům.
- Pro zpracování osobních údajů není třeba Váš souhlas.
- Správcem osobních údajů je lékař/ka – vedoucí tuto ordinaci. Na zpracování osobních údajů se dále podílí zdravotní personál ordinace, který zajišťuje činnosti související s poskytováním zdravotní péče včetně jejího vykazování.
- Rozsah osobních údajů je dán:
  - právními předpisy (jméno, příjmení, datum narození, rodné číslo, adresa pacienta, rozsah poskytované zdravotní péče včetně léčivých přípravků);
  - informacemi pacienta, případně jeho rodinných příslušníků (zdravotní stav), které slouží pro kvalitu zdravotní péče.
- Doba, po kterou jsou Vaše osobní údaje v této ordinaci uchovávány, je stanovena právními předpisy, které upravují podmínky poskytování zdravotní péče a po jejím ukončení podmínkami upravujícími povinnosti ošetřujícího lékaře/ky včetně jeho oprávněných zájmů pro případ možného sporu s pacientem.

GDPR – desatero pro lékaře

GDPR solutions

- Vaše osobní údaje jsou předávány a zpřístupňovány jen subjektům, které mají zákonné oprávnění se na zpracování osobních údajů podílet (zdravotnické zařízení, zdravotní pojišťovna, Státní ústav pro kontrolu léčiv apod.) nebo na základě požadavku pacienta.
- Vaše osobní údaje jsou bezpečně uchovávány a nejsou zpřístupňovány, a to ani elektronicky bez identifikace přistupující osoby a případného oprávněného žadatele o informaci.
- Vaše osobní údaje nejsou předávány do třetích zemí (mimo EU).
- Pokud pacient bude uplatňovat některé ze svých práv podle GDPR, musí tak učinit písemně a řádně se identifikovat. Požadované sdělení mu bude poskytnuto mimo ordinační dobu, aby nebyl narušen výkon zdravotní péče v této ordinaci.
- Pokud pacient zjistí, že je porušeno GDPR, má právo podat stížnost u Úřadu pro ochranu osobních údajů.

GDPR – odpovědnost správce

- **S přihlédnutím** ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným **rizikům** pro práva a svobody fyzických osob, jež s sebou zpracování nese, **zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření**, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů. **A to být schopen doložit!**

GDPR – doložit soulad!

GDPR solutions

- **Směrnice**
- **Záznamy o činnostech zpracování**
- **Posouzení vlivu**
- **Osvědčení**
- **Kodex**
- **Závazná podniková pravidla**

GDPR – doložit soulad!

GDPR solutions

Povinnost vést záznamy o činnostech zpracování má téměř každý

nemusí:

- **Pokud** podnik nebo organizace zaměstnávající méně než 250 osob, ledaže zpracování, které provádí,
  - pravděpodobně představuje riziko pro práva a svobody subjektů údajů,
  - zpracování **není příležitostné** nebo
  - zahrnuje zpracování **zvláštních kategorií údajů** nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

- **Jinak** každý správce či zpracovatel a jejich případný zástupce musí vypracovávat dokument, který obsahuje:

GDPR

GDPR solutions

Co znamená „**pravidelný**“?

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanovených časech
- neustále nebo pravidelně se vyskytující

GDPR – doložit soulad!

GDPR solutions

Záznamy o činnostech zpracování

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
- účely zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace a doložení vhodných záruk;
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
- je-li to možné, obecný popis **technických a organizačních bezpečnostních opatření**.

GDPR – doložit soulad!

GDPR solutions

Zabezpečení zpracování

- Správce a zpracovatel jsou povinni **přijmout taková opatření**, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

GDPR – doložit soulad!

GDPR solutions

- Správce nebo zpracovatel je povinen **zpracovat a dokumentovat přijatá a provedená technickoorganizační opatření k zajištění ochrany osobních údajů** v souladu se zákonem a jinými právními předpisy
- V rámci těchto opatření správce nebo zpracovatel posuzuje **rizika** týkající se
- a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
- b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
- c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
- d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány

GDPR – doložit soulad!

GDPR solutions

V oblasti **automatizovaného zpracování osobních údajů** je správce nebo zpracovatel povinen také

a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
c) **pořizovat elektronické záznamy**, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a
d) zabránit neoprávněnému přístupu k datovým nosičům.

GDPR – doložit soulad!

GDPR solutions

- **Povinnost vypracovat posouzení vlivu na ochranu osobních údajů má subjekt údajů u** zpracování, které na základě své povahy, rozsahu a účelu mohou představovat vysoké **riziko** z hlediska práv a svobod subjektů údajů (generální klauzule)

- Posouzení vlivu je nutné zejména v těchto případech
  - **Systematické a rozsáhlé** vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí
  - **Rozsáhlé** zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů
  - **Rozsáhlé systematické** monitorování veřejně přístupných prostorů
- **Dozorový úřad** sestaví a zveřejní seznam druhů operací, které podléhají požadavku na posouzení vlivu

GDPR – doložit soulad!

GDPR solutions

- **Povinnost vypracovat posouzení vlivu na ochranu osobních údajů**

- Posouzení zahrnuje alespoň
  - Systematický popis zamýšlených operací zpracování a účely zpracování
  - Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů
  - **Posouzení rizik** pro práva a svobody subjektů údajů Plánovaná opatření k řešení těchto **rizik**, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením

- **Doporučení WP29, kdy provádět Posouzení vlivu (návod):**

Posouzení vlivu (DPIA)

GDPR solutions

1. provádí se hodnocení nebo bodování (fyzických osob), včetně profilování a předpovídání,
2. provádí se automatické rozhodování, které má právní nebo podobně závažný dopad,
3. provádí se systematické monitorování, včetně monitorování veřejně přístupných prostor,
4. provádí se zpracování citlivých údajů nebo údajů vysoce osobní povahy,
5. provádí se zpracování v rozsáhlém měřítku,
6. provádí přiřazování nebo slučování datových souborů (e kombinace nebo propojování dat různých zpracování),
7. provádí se zpracování údajů týkajících se zranitelných subjektů údajů,
8. dochází k použití nebo využití nových technologických nebo organizačních řešení,
9. provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů - pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy.

Posouzení vlivu (DPIA)

GDPR solutions

Posouzení vlivu obsahuje:

1) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,
2) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
3) posouzení rizik pro práva a svobody subjektů údajů
4) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob,

Posouzení vlivu (DPIA)

GDPR solutions

https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

„windows“

Posouzení vlivu (DPIA)

Článek 35 odstavec 10 GDPR

- **pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno** jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu

§ 10 Adaptační zákon

Výjimka z povinnosti posouzení vlivu na ochranu osobních údajů

Před zahájením zpracování osobních údajů, které je upravené právním předpisem, není nutno provádět posouzení vlivu takového zpracování na ochranu osobních údajů.

závazná podniková pravidla

GDPR solutions

- Závazná podniková pravidla vymezují přinejmenším:
  - použití obecných zásad pro ochranu údajů;
  - práva subjektů údajů v souvislosti se zpracováním jejich oú a prostředky jejich výkonu;
  - přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii;
  - způsob poskytování informací subjektům údajů;
  - úkoly všech pověřenců nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu v rámci skupiny a sledování školení a vyřizování stížností;
  - postupy pro vyřizování stížností;
  - **mechanismy**, které mají zajistit ověřování souladu (audity ochrany údajů a metody zajištění opravných opatření);
  - **mechanismy** pro podávání zpráv dozorovému úřadu;
  - **mechanismus** spolupráce s dozorovým úřadem;
  - vhodnou odbornou přípravu v oblasti oú pro pracovníky

GDPR – doložit soulad!

- **Povinnost předchozí konzultace s orgánem dozoru**

  - V případě, pokud by z posouzení vlivu vyplynulo, že zpracování je **vysoce rizikové** a zároveň platí, že správce je toho názoru, že riziko nelze zmírnit přiměřenými prostředky

  - Pokud se dozorový úřad domnívá, že by zamýšlené zpracování porušilo toto nařízení, zejména pokud by správce nedostatečně určil či zmírnil riziko upozorní na to správce, případně zpracovatele a může uplatnit kteroukoliv ze svých pravomocí (např. i uložit dočasné nebo trvalé omezení zpracování)

Rizika zpracování

GDPR solutions

- Fyzické osoby by měly být upozorněny na to, jaká **rizika**, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva.

- Nutno posoudit zda zpracování osobních údajů představuje **riziko** nebo **vysoké riziko** pro práva a svobody subjektu údajů.

Rizika zpracování

- GDPR je postaveno **na rizikově orientovaném** přístupu

- Správce a zpracovatel osobních údajů musí hodnotit zamýšlené činnosti a procesy zpracování údajů z hlediska rizik, které z těchto činností a postupů plynou pro **práva a oprávněné zájmy subjektů údajů**
- Správci a zpracovatelé **jsou povinni** na základě identifikovaných a zhodnocených rizik zavést přiměřené kontrolní mechanismy a opatření, které zajistí dodržování povinností stanovených GDPR a ochranu subjektů údajů

Rizika zpracování

- GDPR je postaveno **na rizikově orientovaném** přístupu
- Praktickým dopadem **rizikově orientovaného** přístupu je nutnost zpracovávat a aktualizovat analýzu rizik, ať už jako
  - východisko pro přijetí opatření pro zajištění souladu s GDPR a pro zajištění bezpečnosti osobních údajů,
  - pro účely zhodnocení nutnosti provést posouzení vlivu na ochranu osobních údajů, a nebo
  - z důvodu plánování činnosti a kontrol pověřence pro ochranu osobních údajů.
- Výhodou **rizikově orientovaného** přístupu je možnost prioritizace úkolů podle jejich důležitosti

Identifikace rizik

- Proces nalézání, rozpoznávání a popisování rizik
- Identifikace rizik by měla být systematická, celkovou odpovědnost za zajištění procesu identifikace rizik by mělo mít vrcholové vedení
- Předpoklady: znalost organizace, strategických a operativních cílů a činnosti organizace, právního, společenského, politického a kulturního prostředí, v kterém působí
- Rizika podléhají změně, stejně jako cíle a prostředí organizace (vnitřní o vnější)

Způsoby identifikace rizik

- Control self assesment (CSA)
- Dotazníková šetření a průzkumy
- Workshopy zaměřené na identifikaci rizik

Identifikace rizik

GDPR solutions

- Identifikovaná rizika je třeba klasifikovat a zaznamenat do registru rizik (viz dále analýza rizik)
  - popis rizika
  - přiřazení vlastníka rizika (primárně odpovědný za řízení rizika)
  - posouzení inherentního rizika (úroveň rizika bez jeho ošetření) – dopad, pravděpodobnost, skóre
  - informace o opatřeních, která jsou na riziko aktuálně aplikována
  - hodnota zbytkového rizika (zbývající úroveň rizika po jeho ošetření)
  - zhodnocení, zda je riziko přijatelné
  - informace o dalších opatřeních, která mají být přijata
  - Informace o způsobech monitorování rizika

- Klasifikovat (třídit) rizika lze podle různých kritérií

Analýza rizik

Různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by **zpracování mohlo vést k**

- diskriminaci,
- krádeži či zneužití identity,
- finanční ztrátě,
- poškození pověsti,
- ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím,

Analýza rizik

Dále by zpracování mohlo vést k

- jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, prostřednictvím analýzy nebo odhadu aspektů týkajících se
- pracovních výsledků,
- ekonomické situace,
- zdravotního stavu,
- osobních preferencí nebo zájmů,
- spolehlivosti nebo chování,
- místa pobytu a pohybu,
- situace kdy jsou zpracovávány osobní údaje zranitelných osob, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů.

Reakce na rizika

- Ošetření – zavedení nebo posílení vnitřní kontroly
- Tolerování – akceptace rizika (informovaná a důvodná, rizika nízké závažnosti)
- Přenesení rizika – přenesení nebo sdílení rizika s třetí stranou (např. pojištění, outsourcing nemusí nutně znamenat přenesení rizika – viz např. správce a zpracovatel osobních údajů)
- Vyhnutí se riziku – ukončení činnosti, která je riziková (podstoupená rizika nejsou úměrná přínosům)

GDPR – Pověřenec ochrany oú

Obecné nařízení chápe pověřence jako klíčového hráče v novém systému správy dat a stanoví podmínky jeho

jmenování,

pracovního zařazení

jakož i jeho úkoly.

GDPR – Pověřenec ochrany oú

GDPR solutions

Které organizace musí jmenovat **pověřence**?

- Jmenovat pověřence je povinné, pokud:
  - zpracování provádí orgán veřejné moci či **veřejný subjekt** (bez ohledu na to, jaká data jsou zpracovávána)
  - **hlavní činnosti** správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují **rozsáhlé, pravidelné a systematické** monitorování subjektů údajů
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

GDPR – Pověřenec ochrany oú

GDPR solutions

Co znamená „**rozsáhlý**“?

- Obecné nařízení nedefinuje. WP29 doporučuje při určování, zda zpracování je rozsáhlé, vzít v úvahu zejména následující faktory:
  - počet dotčených subjektů údajů – buď v absolutním vyjádření nebo podílem na relevantní populaci
  - objem zpracovávaných dat a/nebo rozsah datových položek
  - doba trvání nebo nepřetržitost zpracovatelské činnosti
  - územní rozsah zpracovatelské činnosti

GDPR – Pověřenec ochrany oú

GDPR solutions

Příklady rozsáhlého zpracování:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové tramvajenky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

GDPR – Pověřenec ochrany oú

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů individuálním právníkem

GDPR – Pověřenec ochrany oú

GDPR solutions

Co znamená „**systematické monitorování**“?

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

GDPR – Pověřenec ochrany oú

Mohou organizace jmenovat pověřence společně? Pokud ano, za jakých podmínek?

Ano. Skupina podniků může jmenovat jediného pověřence, pokud bude „snadno dosažitelný“.

Jediný pověřenec může být jmenován pro několik orgánů veřejné moci nebo veřejných subjektů s přihlédnutím k jejich organizační struktuře a velikosti. Pro zdroje a komunikaci platí stejná kritéria.

GDPR – Pověřenec ochrany oú

GDPR solutions

Lze jmenovat externího pověřence?

Ano. Pověřencem může být pracovník správce nebo zpracovatele (interní pověřenec) nebo může úkoly plnit na základě smlouvy o poskytování služeb.

Vykonává-li funkci pověřence externí poskytovatel, pak úkoly pověřence mohou být plněny týmově jednotlivci pracujícími pro daného externistu, přičemž odpovědnost nese určená vedoucí kontaktní osoba pověřená péčí o klienta.

GDPR – Pověřenec ochrany oú

Zveřejňování a sdělování kontaktních údajů pověřence

Obecné nařízení požaduje, aby správce nebo zpracovatel:

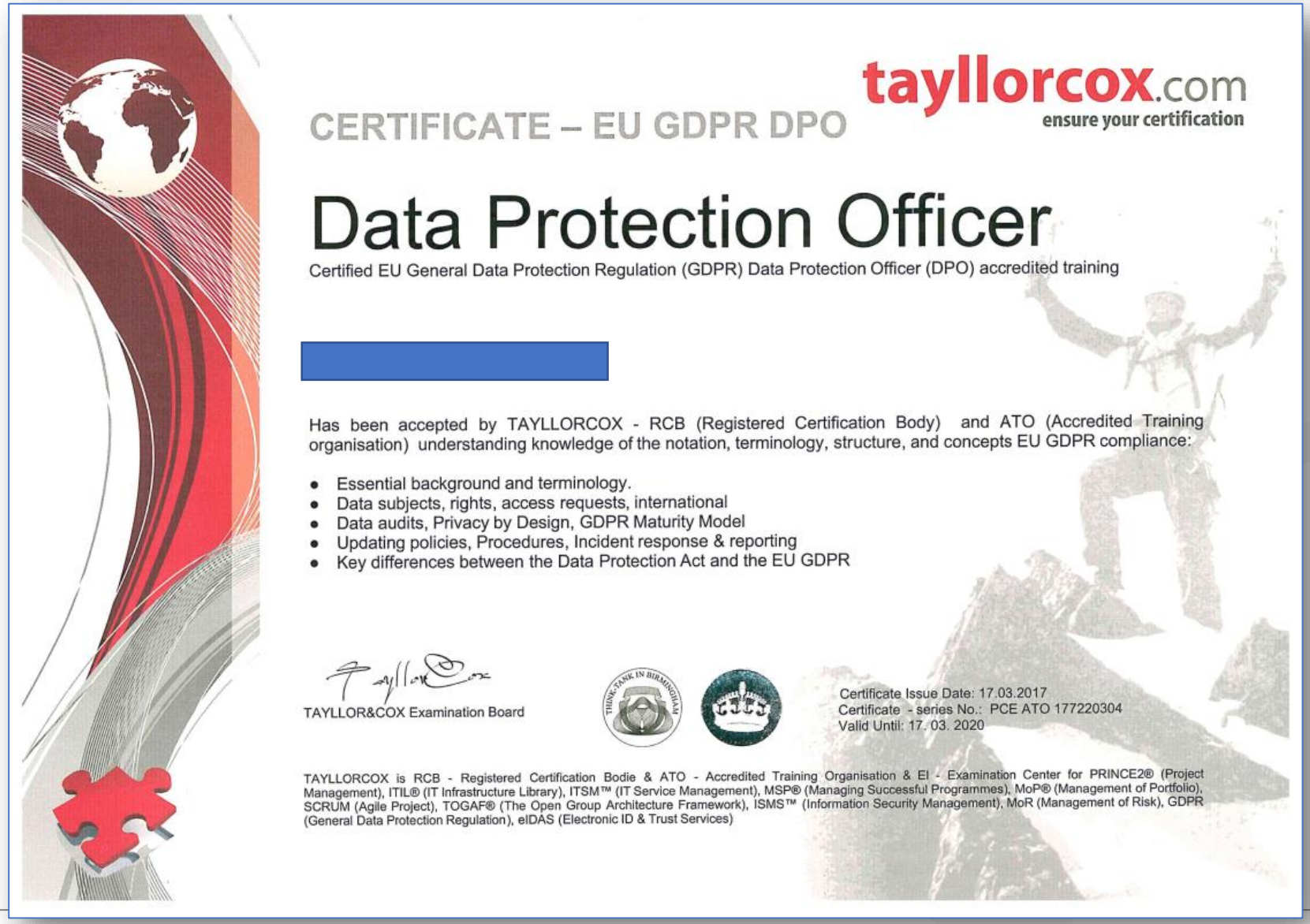
- zveřejnil kontaktní údaje pověřence
- sdělil kontaktní údaje pověřence příslušnému dozorovému úřadu

GDPR – Pověřenec ochrany oú

GDPR solutions

Jaké profesní kvality by pověřenec měl mít?

- znalost národního a unijního práva v oblasti ochrany dat a praktické zkušenosti včetně hluboké znalosti Obecného nařízení
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat
- znalost dané oblasti podnikání a organizace
- schopnost propagovat kulturu ochrany dat v organizaci



CERTIFICATE – EU GDPR DPO

tayllorcox.com
ensure your certification

Data Protection Officer

Certified EU General Data Protection Regulation (GDPR) Data Protection Officer (DPO) accredited training

[redacted]

Has been accepted by TAYLLORCOX - RCB (Registered Certification Body) and ATO (Accredited Training organisation) understanding knowledge of the notation, terminology, structure, and concepts EU GDPR compliance:

- Essential background and terminology.
- Data subjects, rights, access requests, international
- Data audits, Privacy by Design, GDPR Maturity Model
- Updating policies, Procedures, Incident response & reporting
- Key differences between the Data Protection Act and the EU GDPR

TAYLLOR&COX Examination Board

Certificate Issue Date: 17.03.2017
Certificate - series No.: PCE ATO 177220304
Valid Until: 17. 03. 2020

TAYLLORCOX is RCB - Registered Certification Bodie & ATO - Accredited Training Organisation & EI - Examination Center for PRINCE2® (Project Management), ITIL® (IT Infrastructure Library), ITSM™ (IT Service Management), MSP® (Managing Successful Programmes), MoP® (Management of Portfolio), SCRUM (Agile Project), TOGAF® (The Open Group Architecture Framework), ISMS™ (Information Security Management), MoR (Management of Risk), GDPR (General Data Protection Regulation), eIDAS (Electronic ID & Trust Services)

GDPR – Pověřenec ochrany oú

GDPR solutions

Jaké jsou záruky umožňující pověřenci plnit úkoly **nezávislým** způsobem? Co znamená „**konflikt zájmů**“?

Existuje několik záruk umožňujících pověřenci konat nezávisle:

- žádné pokyny od správce nebo zpracovatele týkající se výkonu úkolů pověřence
- nemožnost propuštění nebo sankcionování v souvislosti s plněním úkolů
- zajištění správcem nebo zpracovatelem, aby žádné pověřencovy úkoly nebo povinnosti nevedly ke střetu zájmů

GDPR – Pověřenec ochrany oú

GDPR solutions

Co znamená „**monitorování souladu**“?

Existuje několik záruk umožňujících pověřenci konat nezávisle:

- shromažďovat informace za účelem zjišťování zpracovatelských činností
- analyzovat a prověřovat právní soulad zpracovatelských činností
- informovat, radit a vydávat doporučení správci nebo zpracovateli

GDPR – Pověřenec ochrany oú

Je pověřenec **osobně odpovědný** v případě nesouladu s požadavky ohledně ochrany osobních údajů?

Ne. Pověřenci nejsou osobně odpovědni za nesoulad s požadavky ochrany osobních údajů. Je to správce nebo zpracovatel, kdo musí zajistit a doložit, že zpracování probíhá ve shodě s Obecným nařízením. Dodržování předpisů pro ochranu osobních údajů je odpovědností správce nebo zpracovatele.

GDPR – Pověřenec ochrany oú

GDPR solutions

Jaká je role pověřence v souvislosti s **posudky vlivu na ochranu osobních údajů** a se **záznamy o činnostech zpracování**?

Poradit, mimo jiné v následujících věcech:

- zda je potřeba, případně není potřeba, vypracovat posouzení vlivu na ochranu osobních údajů
- jakou metodiku při zpracování posouzení vlivu uplatnit
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry jsou v souladu s požadavky na ochranu osobních údajů

GDPR – Pověřenec ochrany oú

Jaká je role pověřence v souvislosti s **posudky vlivu na ochranu osobních údajů** a se **záznamy o činnostech zpracování**?

Povinnost!?

Článek 35 odstavec 2:

- Při provádění posouzení vlivu na ochranu osobních údajů si **správce vyžádá posudek** pověřence pro ochranu osobních údajů, byl-li jmenován.

GDPR – co dělat až se vrátíme domů?

GDPR solutions

- Zjištění současného stavu - audit
- Vypracování záznamů o činnostech zpracování
- Vypracování Srovnávací analýzy (do jaké míry jsme v souladu s GDPR) včetně analýzy současných rizik.
- Návrh dalšího postupu
  - Pověřenec?
  - DPIA?
  - Záznamy o zpracování?
  - Směrnice

GDPR – co dělat až se vrátíme domů?

GDPR solutions

Zjištění současného stavu

- Co: jaké osobní údaje jsou zpracovávány
- Kdo: kdo přichází s osobními údaji do styku
- Proč: za jakým účelem osobní údaje zpracováváme
- Forma: zpracování je elektronické nebo v papírové formě
- Právo na zpracování: zpracování je na základě smlouvy nebo zákona
- Doba uchování: kdy data skartujeme

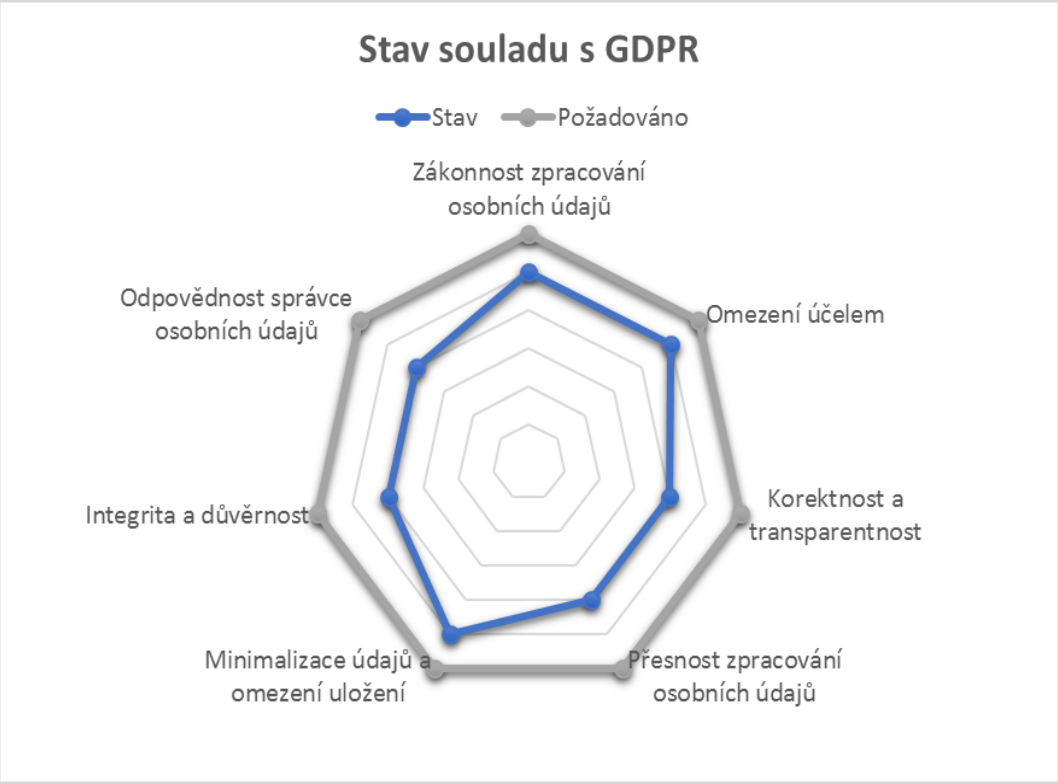
GDPR – smlouva správce - zpracovatel

GDPR solutions

Nutno provést:

- **kontrolu uzavřených smluv** s informačními společnostmi, na základě nichž se zpracovávají osobní údaje prostřednictvím informačního systému provozovaného externím dodavatelem – zejména kontrola rozsahu, účelu a doby zpracování

GDPR – co dělat až se vrátíme domů?



- **Srovnávací analýza**

- Model procesní vyspělosti CMM:
  - Neexistence (Stupeň 0);
  - Náhodně (Stupeň 1);
  - Opakovatelně (Stupeň 2);
  - Definovaně (Stupeň 3);
  - Měřitelně (Stupeň 4);
  - Optimalizovaně (Stupeň 5).

GDPR – CMM

- **Neexistence (Stupeň 0)**
  - Opatření/Proces organizace neřeší. Organizace si neuvědomuje potřebu ochrany OÚ.
- **Náhodně (Stupeň 1)**
  - Opatření/Proces je řešen nahodile. Organizace si uvědomuje potřebu ochrany OÚ. Povědomí o potřebě bezpečnosti vychází výhradně z individuální iniciativy. Ochrana OÚ se řeší nárazově a není nijak měřena
- **Opakovaně (Stupeň 2)**
  - Opatření/Proces je řešen intuitivně ale opakovaně. Zodpovědnost za ochranu OÚ spočívá na určené roli, ačkoli její pravomoci jsou omezeny. Povědomí o potřebě ochrany je neurčité a omezené.
- **Definovaně (Stupeň 3)**
  - Opatření/Proces je definován a dokumentován. Existuje povědomí o bezpečnosti a je podporováno ze strany vedení organizace. Jsou definovány procesy ochrany OÚ a dodržují se. Jsou určeny osoby zodpovědné za ochranu OÚ, ale neděje se tak permanentně.
- **Měřitelně (Stupeň 4)**
  - Opatření/Proces je měřen z pohledu efektivity. Zodpovědnost a úkoly spojené s ochranou OÚ jsou jasně stanoveny, řízeny a uplatňovány.
- **Optimalizovaně (Stupeň 5)**
  - Ochrana OÚ je předmětem společné zodpovědnosti IT a obchodního managementu a je zařazena v cílech bezpečnosti organizace. Požadavky na ochranu OÚ jsou jasně definovány, optimalizovány a jsou součástí schváleného bezpečnostního plánu.

GDPR – sankce

- Každý dozorový úřad zajistí, aby ukládání správních pokut ohledně porušení tohoto nařízení bylo v každém jednotlivém případě **účinné, přiměřené a odrazující**.
- Za porušení některých ustanovení lze uložit správní pokuty až do výše **20 000 000 EUR**, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.
- nesprávné nakládání s osobními údaji může založit vznik **trestní odpovědnosti právnické osoby** dle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob. Trestný čin dle § 180 zákona č. 40/2009 Sb., trestního zákoníku – neoprávněné nakládání s osobními údaji - není mezi vyloučenými trestnými činy vypočtenými v § 7 zákona a tedy každá společnost tak musí počítat s aktivací trestní odpovědnosti a nastoupení hrozící sankce.

GDPR - FAQ

GDPR solutions

Cloud:

Je uložení osobních údajů na cloudu možné?

Archivace:

Jak je to s archivací, když máme povinnost dbát na přesnost osobních údajů?

GDPR - kuriozity

Článek 11 odstavec 2:

Je-li v případech uvedených v odstavci 1 tohoto článku správce s to doložit, že není schopen identifikovat subjekt údajů, informuje o této skutečnosti subjekt údajů, pokud je to možné. V takovýchto případech se neuplatní články 15 až 20, s výjimkou případů, kdy subjekt údajů za účelem výkonu svých práv podle uvedených článků poskytne dodatečné informace umožňující jeho identifikaci.

Čteme to stejně?:

Je-li správce s to doložit, že není schopen identifikovat subjekt údajů, informuje o této skutečnosti subjekt údajů, pokud je to možné.

Závěrečné shrnutí

GDPR solutions

- 1) Musíme si uvědomit a zkontrolovat, zda zpracováváme data jen na základě legitimního předem stanoveného **účelu**
- 2) Osobní údaje lze zpracovávat **zákonným způsobem**, tedy na základě:

  Souhlasu subjektu údajů nebo

  Plnění **smlouvy** nebo

  Plnění právní povinnosti (**zákona**)

Závěrečné shrnutí

GDPR solutions

- 3) S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným **rizikům** pro práva a svobody fyzických osob, jež s sebou zpracování nese, **zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření**, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů. **A to být schopen doložit!**
- Způsobů, jak **doložit** dodržení plnění GDPR nařízení nabízí několik. Je to vypracování dokumentů, z nichž některé podle počáteční analýzy se ukážou jako povinné a jiné jsou dobrovolné. Jsou to:

Závěrečné shrnutí

- **Směrnice –** doporučuji, pokud není vypracován jiný dokument
- **Záznamy o činnostech zpracování –** doporučuji vždy (článek 30)
- **Posouzení vlivu –** může se ukázat, že je povinné (pokud se jedná o rizikové a rozsáhlé zpracování)

Dobrovolné:

- **Osvědčení –** zatím nelze získat (článek 42)
- **Kodex –** (článek 40)
- **Závazná podniková pravidla –** (článek 47)

Závěrečné shrnutí

GDPR solutions

- Zkontrolovat, zda máme s případnými **zpracovateli** uzavřenou zpracovatelskou smlouvu, nebo zda už u zavřených smluv máme „doložku“ o podmínkách zpracování osobních údajů, jak přímo vyjmenovává GDPR (článek 28).

Závěrečné shrnutí

- A nesmíme zapomenout na povinnou informovanost o právech subjektu údajů, jako je např. právo kdykoliv odvolat souhlas se zpracováním, pokud byl dán, nebo právo podat stížnost u dozorového úřadu na webových stránkách, pokud je máme, nebo v čekárně, v obchodních podmínkách apod. (článek 13, 14).
- Posoudíme, zda potřebujeme anebo přímo musíme jmenovat pověřence.

Závěrečné shrnutí

GDPR solutions

- A na závěr: Jelikož v některém z vypracovaných dokumentů máme proškolení zaměstnanců, tak se pustíme do zorganizování školení těch, kteří se nezúčastnili tohoto semináře ….

GDPR !?

GDPR solutions

Účel, zákonnost, doložit

www.gprsolutions.cz

Splendidissima condicione utimur!

GDPR
solutions

info@gdprsolutions.cz

tel.: 608 311 933

www.gdprsolutions.cz

Děkuji za pozornost!

© 2018 RNDr. Igor Němec

Tento seminář pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz