Olga Přikrylová
IT Security konzultant / ITI

7. 3.
2017

AUTOCONT

Seminář k GDPR

Ochrana osobních údajů

Program - co nás dnes čeká?

- Osobní údaje vs. ochrana fyzických osob
- GDPR
- Povinnosti (právnické osoby)
- Zákonné zpracování
- Práva (fyzické osoby)
- Procesy, smlouvy, dokumenty a záznamy
- DPO
- Životní cyklus osobních údajů vs. bezpečnost
- Příklady opatření (technických, organizačních)
- Dotazy/diskuze

Musíme osobní údaje nějak zvlášť chránit?

1950: Evropská úmluva o ochraně lidských práv a základních svobod

1981: Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat

1993: Ústava (ČR)

1995: směrnice EU (mezinárodní úprava)

2000: zákon o ochraně OÚ (národní úprava ČR)

2016: nařízení EU (mezinárodní úprava)

- Mezinárodní významný den:

28. leden (2017) - Den ochrany osobních údajů

Jaké „osobní údaje“ zpracováváte?

- Osobní údaje

(OÚ)

- Zvláštní kategorie osobních údajů

(citlivé OÚ)

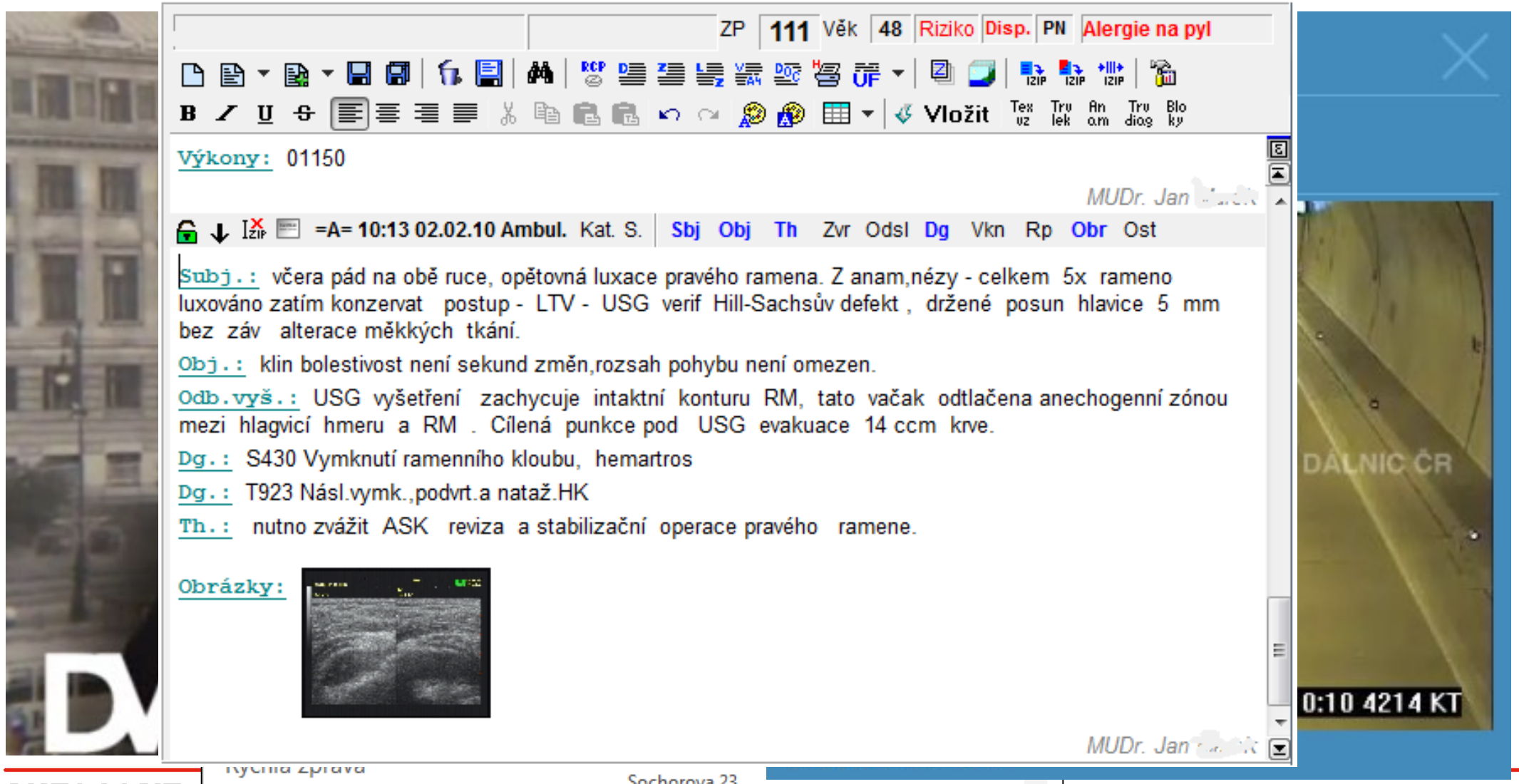
Co to vlastně je „osobní údaj“ (OÚ)?

Dle GDPR:	Dle zákona č. 101/2000 Sb.:
- informace o identifikované nebo identifikovatelné fyzické osobě, - lze přímo či nepřímo identifikovat na základě jména, identifikačního čísla, lokačních údajů, prvků fyzické, fyziologické (biometrické), genetické, psychické, ekonomické, kulturní nebo společenské identity, e-mail, on-line identifikátorů (IP adresa) nebo cookies	- informace týkající se určeného nebo určitelného subjektu údajů - lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu

Co to je „citlivý údaj“?

Dle GDPR:	Dle zákona č. 101/2000 Sb.:
Zvláštní kategorie osobních údajů - např. o zdravotním stavu - podrobnější právní úprava ponechána na členských zemích	- o národnostním, rasovém nebo etnickém původu, - politických postojích, členství v odborových organizacích, - náboženství a filozofickém přesvědčení, - odsouzení za trestný čin, - zdravotním stavu (tělesném a duševním, vč. lék. záznamů) a sexuálním životě, - genetický a biometrický údaj umožňující přímou identifikaci nebo autentizaci SÚ

Kontrolní otázka: poznáte osobní/citlivé údaje?



Olga.Prikrylova@autocont.cz
Sochorova 23
616 00 Brno

Co znamená zkratka „GDPR“?

- Nařízení EU 2016/679
  - o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a
  - o volném pohybu těchto údajů a
  - o zrušení směrnice 95/46/ES
- Nařízení X směrnice

GDPR - od kdy platí?

- Nařízení nabývá účinnosti již **25. května 2018**
- Správce (a zpracovatel) má cca **1 rok** na zavedení všech „povinných opatření“
- K datu účinnosti musí správci/zpracovatelé splňovat požadavky GDPR (přinejmenším v rozsahu, který je pro ně závazný)
- K datu účinnosti mohou být správcům/zpracovatelům OÚ uděleny sankce

GDPR - co hrozí?

Při nedodržení nebo porušení požadavků GDPR sankce

- až do: **20 000 000 Euro (540 000 000 Kč)**
- nebo **4 %**

z ročního (celosvětového) **obratu** firmy

- *Pro srovnání:*
  - *dosavadní pokuty ÚOOÚ mohou dosáhnout max. 10 miliónů (Kč)*

GDPR - pro koho platí?

- Kdokoliv (i mimo EU), kdo zpracovává nebo shromažďuje OÚ občanů členských zemí EU
  - veřejný sektor
  - soukromý sektor, **zejména** pokud zpracování OÚ souvisí:
    - s nabídkou zboží nebo služeb
    - s monitorováním chování fyzických osob
- Výjimky:
  - zpravodajské služby
  - policie
  - apod.
- Nařízení prakticky stírá rozdíl mezi správcem a zpracovatelem!

Jste správcem nebo zpracovatelem?

- **Správce**:
  - osoba (práv.) určující účel a prostředky zpracování OÚ
  - osoba (práv.) zodpovědná za jejich ochranu

  Např.: obchodní firma s vlastním e-shopem, zdravotnické zařízení, obecní úřad.

- **Zpracovatel**:
  - osoba (práv.) pověřená správcem zpracovávat OÚ
  - nově stejná odpovědnost jako správce
  - nově ustanovena povinná písemná smlouva mezi správcem a zpracovatelem

  Např.: dodavatelská firma provozující pro obchodní firmu e-shop, informační systém, cloudové služby, outsourcing, zpracování mezd (jakékoliv služby, při nichž dochází ke zpracování OÚ)

Na velikosti nezáleží!!!

Správce vs. zpracovatel

Písemná smlouva

Povinnosti správců/zpracovatelů

- **Odpovědnost**
- **Smluvní vztahy**
- **Původ OÚ**
- **Účel/y zpracování**
  - test kompatibility
- **Minimalizace**
- **Omezení doby zpracování**
- **Pseudonymizace**
- **DPO**
- **Vedení záznamů**
- **Hlášení incidentů**
- **Hodnocení vlivu**
- **Zákonnost**
- **Zabezpečení**
- **Přenositelnost**

Co nařízení nařizuje správci i zpracovateli?

– Musí být schopen prokázat, co je v jeho případě „odpovídající“ prostředek na základě analýzy rizik!

Povinnosti vůči subjektům údajů

OÚ = majetek fyzické osoby

- Bezplatnost (výjimky)
- Informovanost o opatřeních
- Srozumitelné informace:
  - rozsah
  - místa uložení/zpracování
  - doba zpracování
  - příjemci
  - třetí strany
  - zabezpečení
- Hlášení incidentů
- Zajištění práv SÚ:
  - právo na přístup k OÚ
  - požadavek na opravu/úpravu
  - omezení zpracování
  - vznesení námitky (= zvláštní režim pro OÚ)
  - nesouhlas se zpracováním
  - výmaz (právo být zapomenut)
  - přenositelnost

+ povinnost informovat o požadavku SÚ další správce/zpracovatele

Povinnosti vůči ÚOOÚ

úřad pro ochranu osobních údajů
the office for personal data protection

- **Záznamy** „o činnostech zpracování OÚ“
- Hlášení incidentů (do 72 hodin)
- „Odpovídající“ opatření
- Analýza rizik OÚ
- Posouzení vlivu
- Komunikace s ÚOOÚ (schválení kodexu, závazných pravidel apod.)

Kdy je zpracování OÚ zákonné?

Pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- **subjekt** OÚ **udělil souhlas**
- **zpracování** OÚ **je nezbytné** pro:
  - splnění smlouvy
  - splnění právní povinnosti
  - ochranu životně důležitých zájmů subjektu OÚ nebo jiné fyzické osoby
  - splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci
  - účely oprávněných zájmů
    (netýká se zpracování prováděného OVM při plnění jejich úkolů)

Souhlas

Schopnost správce (nebo zpracovatele) vždy:

- doložit, že subjekt údajů udělil souhlas se zpracováním
- získat a po celou dobu zpracování uchovávat průkazný souhlas se zpracováním

Souhlas musí být:

- svobodný
- určitý
- informovaný
- srozumitelný
- jednoznačný

ÚOOÚ a oblasti „zákonného“ zpracování OÚ

- výčet zákonných agend a s nimi souvisejících postupů týkajících se zpracování OÚ

Oblasti zpracování osobních údajů

Ústavní zakotvení ochrany osobních údajů, právo na ochranu soukromí	Pojišťovnictví
Archivnictví	Policejní postupy, veřejný pořádek, vnitřní a vnější bezpečnost
Bankovnictví, finance	Poskytování informací veřejnou správou, veřejné rejstříky a evidence
Daňové řízení	Pracovněprávní vztahy, zaměstnanost
Doprava	Předávání osobních údajů do zahraničí
Elektronická veřejná správa (e-government)	Rodná čísla
Elektronické komunikace	Rozhlasové a televizní poplatky
Evidence obyvatel, matriky a notáři	Sociální zabezpečení
Kamerové systémy	Statistická zjišťování
Kasina	Školství
Katastr nemovitostí	Územní samospráva
Nevyžádaná obchodní sdělení	Volby
Osobní doklady	Zdravotnictví

Přestávka na kafe

Novinka

– Nařízení zavádí (a v konkrétních případech vyžaduje) novou roli:

DPO

Data Protection Officer

(pověřenec pro ochranu OÚ)

Kdy musí být jmenován DPO?

Správce a zpracovatel jmenují pověřence pro ochranu OÚ vždy, když:

- zpracování provádí OVM či veřejný subjekt

  (s výjimkou soudů jednajících v rámci svých soudních pravomocí)

- hlavní činností správce nebo zpracovatele je:
  - rozsáhlé pravidelné a systematické monitorování subjektů údajů
  - rozsáhlé zpracování zvláštních kategorií údajů
  - rozsáhlé zpracování OÚ týkajících se rozsudků v trestních věcech a trestných činů

K čemu je DPO?

- **(dobře) radí**
  - poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům o jejich povinnostech v souvislosti se zpracováním OÚ
  - poskytování poradenství na požádání při posouzení vlivu na ochranu OÚ, a monitorování jeho uplatňování
- **monitoruje**
  - soulad s tímto nařízením, dalšími předpisy EU v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany OÚ, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů
- **spolupracuje s ÚOOÚ**
- **působí jako kontaktní místo** pro:
  - ÚOOÚ v záležitostech týkajících se zpracování, včetně předchozí konzultace, případně vedení konzultací v jakékoli jiné věci
  - pro subjekty zpracovávaných OÚ

Kvalifikační předpoklady DPO

Obecná definice:

- profesní kvality, zejména:
  - odborné znalosti práva a praxe v oblasti ochrany OÚ
- schopnosti plnit úkoly DPO

Zajištění role:

- vlastní zaměstnanec
  - pracovní smlouva – odpovědnost dle zákoníku práce
- externista
  - smluvní ujednání s dodavatelem služby

Povinnosti DPO?

Pověřenec může dostávat i jiné úkoly (kumulovaná funkce)

- Nesmí:
  - být ve střetu zájmů
  - dostávat žádné pokyny týkající se výkonu jeho úkolů
- Může:
  - mít tým více pracovníků pracujících jako tým může účinněji poskytovat služby svým klientům
  - být pověřen úkolem vést záznamy o činnostech zpracování
- Musí:
  - jasně rozdělit úkoly v pověřencově týmu
  - určit jednoho pracovníka jako hlavní kontakt a osobu „pověřenou“ péčí o zákazníka
  - brát patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování

Vedení záznamů o činnostech zpracování OÚ

Povinný obsah:

- jméno a kontaktní údaje správce a zpracovatele + DPO
- účely zpracování + důsledky (je-li založeno na profilování)
- kategorie subjektů údajů
- kategorie osobních údajů
- kategorie příjemců
- informace o předávání osobních údajů (třetí země)
- lhůty pro výmaz jednotlivých kategorií údajů
- technická a organizační opatření

Dokumentace a záznamy:

- smlouvy se správci/zpracovateli/dodavateli služeb (vč. DPO)
- záznamy z analýzy rizik
- posouzení vlivu
- auditní záznamy (manipulace s OÚ)
- souhlasy SÚ
- informace pro subjekty
- šablona pro hlášení incidentů (třem subjektům)
- šablony pro uplatnění práv SÚ
- dokumentovaná technická a organizační opatření
- …

Ohlašování bezpečnostních incidentů

- Proces pro hlášení:
  - evidence všech incidentů
  - odpovědná osoba za hlášení
  - co hlásit (vyhodnocení + metodika)
  - doporučení, jak zmírnit nežádoucí účinky
- V případě:
  - narušení ochrany OÚ -> ÚOOÚ (do 72 hodin)
  - vznik bezprostředního rizika -> subjektu OÚ (jakmile je to proveditelné / neprodleně)

Posouzení vlivu

- v případě zamýšleného zpracování OÚ = předem!
- na základě analýzy rizik
- pokud zůstávají významná rizika (nebo nebyla přijata opatření k jejich zmírnění), konzultace s ÚOOÚ!
- pozor na lhůty k vyjádření ÚOOÚ (v řádu týdnů!)

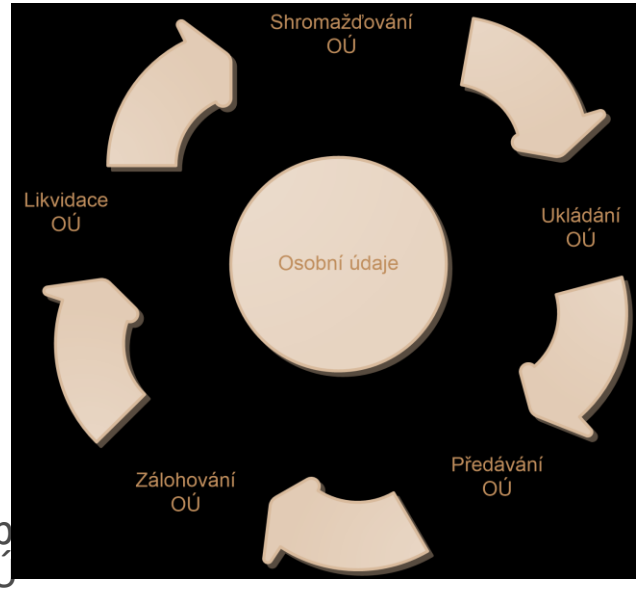
Prostředky zajištění bezpečnosti

Správce (nebo zpracovatel) musí zajistit:

- **důvěrnost**
- **integritu**
- **dostupnost**

osobních údajů „odpovídajícími“ prostředky

Požadavky na ochranu OÚ v jejich životním cyklu



- **zákonnost při shromažďování a zpracování** OÚ
  - např. pořizování, získávání, shromažďování OÚ – nejen v elektronické formě
- **ochrana OÚ ukládání, sdílení a zpracování** OÚ
  - např. e-maily, sdílená úložiště, lokální ukládání dat, třídění, profilování, změny a poskytování OÚ
- **ochrana při přenosu** OÚ
  - např. v rámci interní komunikace, externí komunikace, předávání OÚ jiným sub správcům/zpracovatelům, třetím stranám, zajištění práva na přenositelnost OÚ
- **ochrana při zálohování** (příp. archivaci) OÚ
  - např. zajištění dostupnosti, zálohování, obnovitelnosti, bezpečného úložiště/zabezpečených médií pro ukládání záloh s OÚ, bezpečná archivace
- **bezpečná likvidace** OÚ
  - např. zajištění bezpečné (neobnovitelné) skartace nosičů dat, práva subjektu OÚ na výmaz OÚ

Záměrná a standardní ochrana OÚ

- **Stanovení vhodných opatření:**
  - před zpracováním
  - při zpracování samotném

  (pseudonymizace, minimalizace údajů, nezbytné záruky)

- **Vhodná technická a organizační opatření k zajištění:**
  - standardně jsou zpracovávány pouze OÚ pro každý konkrétní účel nezbytné
  - standardně bez zásahu člověka nejsou OÚ zpřístupněny neomezenému počtu fyzických osob

  (týká se množství shromážděných OÚ, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti)

Prostředky zajištění **zákonnosti** zpracování OÚ

- Audit procesů
  - pořizování/získávání OÚ
  - právní základ zpracování
  - ukládání/zpracování (kde všude se OÚ vyskytují)
  - přenosu
  - předávání
  - likvidace
  - získávání souhlasu
  - informovanosti subjektů (před a po)
  - smluvních ujednání
  - opatření
- Určení rolí (DPO, ...) vč. povinností a odpovědnosti

Prostředky ochrany OÚ při **ukládání a zpracování**

- Audit opatření:
  - úložiště (např. e-maily, sdílená úložiště, lokální ukládání dat)
  - šifrování (transparentní, ad-hoc, řízení klíčů, hesel)
  - přístupy (identifikace osoby provádějící zpracování)
  - oprávnění manipulovat s OÚ
  - auditní záznamy (logování, přístup k logům, ochrana proti změnám, lhůty)
  - pravidla sdílení
  - postupy v případě změny
  - externí zpracovatelé (smluvní vztahy)
- Šifrování
- Řízení identit

Prostředky zajištění **ochrany při přenosu** OÚ

- Audit opatření:
  - interní komunikace,
  - externí komunikace,
  - přenos OÚ jiným subjektům, správcům/zpracovatelům,
  - předávání třetím stranám,
  - zajištění práva na přenositelnost OÚ
- Autentizace/autorizace
- Šifrování
- Elektronický podpis
- Pseudonymizace/anonymizace

Prostředky zajištění **dostupnosti** OÚ

- Zálohování
  - vč. obnovitelnosti ☺
  - v požadovaných intervalech (RTO, RPO)
  - redundance, záložní systémy, replikace, datová centra,
  - bezpečné úložiště záloh/zabezpečení médií
- Archivace
  - integrita
  - bezpečnost
  - lhůty

Prostředky zajištění **bezpečné likvidace** OÚ

- Audit procesu
  - převzetí požadavku na výmaz OÚ
  - posouzení oprávněnosti (vyjádření výsledku SÚ do 1. měsíce)
  - informování příjemců (zpracovatelů, třetích stran)
- Implementace do IS/databáze
  - zvláštní (omezený režim) zpracování OÚ – příznak!
  - výmaz části nebo všech OÚ
  - příznak požadavku (na výmaz, nesouhlas s dalším zpracováním)
- Bezpečné, tzn. neobnovitelné smazání dat (shredder) v PC/IS
- Bezpečná skartace fyzických nosičů dat

Prokázání souladu

- Závazná podniková pravidla (schvaluje ÚOOÚ)
- Kodexy chování (připravuje, příp. schvaluje ÚOOÚ)
- Osvědčení – certifikace (v gesci ÚOOÚ)

Jak zajistíte soulad – **procesy, organizační opatření**?

- role, resp. outsourcing výkonu činností externího „pověřence pro ochranu OÚ“
- audit procesů, organizačních a technických bezpečnostních opatření, dokumentace
- analýza rizik OÚ (vč. využívání cloudu)
- audit shody nakládání s OÚ s požadavky GDPR
- posouzení vlivu
- návrh, schválení a uvedení procesů do souladu s nařízením EU
- tvorba dokumentace vč. organizačních a technických opatření
- změny, aktualizace a uvedení záznamů (ochrana OÚ, práva subjektů) do souladu
- vzdělávání (poučení, školení)

Jak zajistíte soulad – **technická opatření**?

- ochrana OÚ před škodlivými kódy (anti-x)
- detekce a prevence průniku – IDS/IPS
- testy zranitelnosti
- šifrování OÚ (dat, databází, PKI/CA)
- evidence přístupu a práce s OÚ (IdM, RMS)
- evidence manipulace s daty (DMS, DLP, MDM)
- monitoring/sledování chování (logování a vyhodnocování logů, WAF, SIEM)
- řízení přístupu (AAA)
- atd.

Přestávka na 2. kafe

Jak na to prakticky? **Analýza rizik OÚ**

- Inventura OÚ, tzn. (identifikace výskytu analyzovaných informačních aktiv)
- Kategorizace (+ klasifikace OÚ)
- Hrozby
- Zranitelnost
- Rizika
- Návrh základních opatření na snížení rizik

= podklad pro posouzení vlivu

Jak na to prakticky? **Audit shody s GDPR**

- Interview s **odpovědnými fyzickými osobami**:
- Procesy
- Organizační opatření
- Technická opatření
- Posouzení shody (etalon – GDPR, shoda/neshoda)
- Výsledná zpráva z auditu
- Návrh (doporučení) auditora

Jak na to prakticky? **Outsourcing role**

- Smluvní ujednání:
  - rozsah
  - období
  - četnost/frekvenci činností
  - forma a způsob vedení záznamů/evidence
  - forma a způsob reportingu
  - kontaktní a zodpovědné osoby
  - součinnost
- Odpovědnost:
  - sledovat, kontrolovat, vyhodnocovat, navrhovat, doporučovat, reportovat a upozorňovat na anomálie, nedostatky, nesoulad, hrozby, zranitelná místa či vzniklá rizika ohrožující bezpečnost OÚ
- Kumulace rolí

Příklady technických opatření

Dotazy?

AutoCont CZ a.s. / Hornopolní 3322/34 702 00 Ostrava / www.autocont.cz

Olga Přikrylová
IT Security konzultant / ITI

+420 723 320 815
olga.prikrylova@autocont.cz