GOPAS

Přehled GDPR

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory2012 | MVP:Security | CEH | CHFI | CISA | CISM | CISSP |
ondrej@sevecek.com | www.sevecek.com |

GOPAS: info@gopas.cz | www.gopas.cz | www.facebook.com/P.S.GOPAS

1

Odkazy

- GDPR
  - http://ec.europa.eu/justice/data-protection/reform/index_en.htm
- Article 29 Work Group
  - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- European Data Protection Board
  - https://edpb.europa.eu/edpb_en
- UOOU CZ
  - https://www.uoou.cz/
- UOOU SK
  - https://dataprotection.gov.sk/uoou/

GOPAS

2

Cíle a poznámky

- "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" :-)
- Cíle
  - kontinuita ke Směrnici 95/46/EC (9)
  - zjednodušení a sjednocení stavu
  - detailnější a preciznější definice
  - bez registrace
  - normální businessy nepotřebují DPO
  - volné zpracování a předávání údajů po GDPR státech
    - zpracování/předání podle souhlasu
- Poznámky
  - žádné nové druhy osobních údajů (IP, ...)
  - hlášení incidentů
  - proaktivní zabezpečení a dokumentace
    - anonymizace, pseudonymizace, šifrování, testování a validace
    - "posouzení vlivu na zpracování osobních údajů"
    - zpracovatelské logy

GOPAS

3

Strachy a rizika

- Nikdo pořádně neví, jestli nebude potřebovat DPO
- Proaktivní dokumentace, namátkové kontroly, předání přístupových logů
  - do 72 hodin
  - pokuty až 20 000 000 EUR a/nebo až 4% celosvětového obratu
- Existující údaje
  - buď byly získány ve shodě s GDPR
  - nebo si znovu vyžádáme souhlasy
  - nebo je zahodíme
- Bez zvláštního "významného" souhlasu nelze zpracovávat ani předávat data do ne-GDPR organizací (44 - 49)

GOPAS

4

Nařízení a Směrnice

- Nařízeni (Regulation)
  - zabývá se organizacemi v "Digital Single Market"
  - vydáno 4.5. 2016
  - účinnost od 25.5. 2018
  - **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
  - nahrazuje CZ zákon č. 101/2000 Sb.
  - nahrazuje SK zákon č. 122/2013 Sb.
- Směrnice (Directive)
  - justice a policejní složky
  - vydáno 4.5. 2016
  - musí být transformována (transposed) do národních zákonů do 6.5. 2018
  - **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

GOPAS

5

Identifikované nebo identifikovatelné osoby (26)

- Kombinace údajů rozhoduje o identifikovatelnosti
  - + míra újmy při úniku
- Pouze fyzické osoby ve vztahu k organizacím (2.2c)
  - vyjma anonymních dat (26)
  - vyjma mrtvých (27)
  - vyjma osobního zpracování
- Chrání fyzické osoby na území EEA (European Economic Area) (3.1) (3.2) (22) (23) (24)
  - EU + Island, Lichtenštejnsko, Norsko
- Proti jakékoliv organizaci zpracovávající jejich osobní údaje
  - území EEA, i mimo území EEA, služby na území EEA, ...
  - mimo Air Passenger Name Record (PNR) a Terrorist Finance Tracking Program (TFTP)
  - + Švýcarsko, Kanada, Argentina, britské "ostrůvky"
  - + US Privacy Shield (Safe Harbor)
- Elektronické nebo papírové informace (15)

GOPAS

6

Osobní údaje

- Obecné osobní údaje (4.1)
  - jméno, pohlaví, věk, datum narození, rodné číslo, manželství
  - IP adresa, telefon, fotka, email, facebook ID
  - cookie, geolokační data
  - organizační údaje - email, telefon, IČO/DIČ
- Citlivé (zvláštní) údaje
  - rasa, politika, odbory, mentální schopnosti, zdraví (4.15), sexuální orientace, kriminální historie
  - genetické údaje, biometrické, ruční ("biometrický") podpis (4.14)
    - biometrické přihlašovací údaje prohlásil CZ UOOU za necitlivé
  - údaje o dětech (16 let a méně podle národní úpravy)
    - CZ 13, SK 16
  - vyžaduje DPO při rozsáhlém zpracování

GOPAS

7

Práva subjektů

- Být informován o zpracování v jasné a pochopitelné formě
  - souhlas daný, specifický a informovaný (4.11)
  - férové metody získávání souhlasu (32) (42)
- Přístup k vlastním údajům
  - co se vlastně zpracovává
  - export dat v běžném strojově zpracovatelném formátu (68)
- Oprava údajů
  - pokud mám podezření ze subjektivních nebo objektivních důvodů
- Odmítnout zpracování
  - pokud neexistuje jiný prokázaný důvod proč nelze zpracování ukončit (faktury, zálohy, ...)
- Právo nebýt profilován (4.3) (22.1)
- Být smazán a zapomenut
  - pokud to nenarušuje "historii" (4)
- Data mohou být uchovávána ne déle než je nutné (5.1e)

GOPAS

8

Relativnost práva na ochranu osobních údajů (4)

- Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy. Toto nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou, jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost.

GOPAS

9

Zajímavé ochranné mechanismy a opatření

Přehled GDPR

GOPAS

10

Anonymizace

kamil	zlomená noha	zlomena ruka	infarkt	nateklé oko
ondrej	infarkt	zlomená ruka	ledvina	
jitka	chřipka	chřipka	bolest hlavy	transplantace mozku

zdravotní dokumentace

export

chřipka, chřipka, ledvina, bolest hlavy, transplantace mozku, infarkt, zlomená ruka, infarkt, zlomená ruka, nateklé oko, zlomená noha

GOPAS

11

Anonymizace

kamil	35	zlomená noha	zlomena ruka	infarkt	nateklé oko
ondrej	19	infarkt	zlomená ruka	ledvina	
jitka	67	chřipka	chřipka	bolest hlavy	transplantace mozku

zdravotní dokumentace

export

chřipka 67, chřipka 67, ledvina 19, bolest hlavy 67, transplantace mozku 67, infarkt 35, zlomená ruka 19, infarkt 19, zlomená ruka 35, nateklé oko 35, zlomená noha 35

GOPAS

12

Pseudonymizace (28) (25.1) (32.1) (89.1)

#1	kamil
#2	ondrej
#3	jitka

#1	zlomená noha	zlomená ruka	infarkt	nateklé oko
#2	infarkt	zlomená ruka	ledvina	
#3	sifilis	aids	bolest hlavy	transplantace mozku

zdravotní dokumentace

kamil	otisk prstu hash#1
ondrej	otisk prstu hash#2
jitka	otisk prstu hash#3

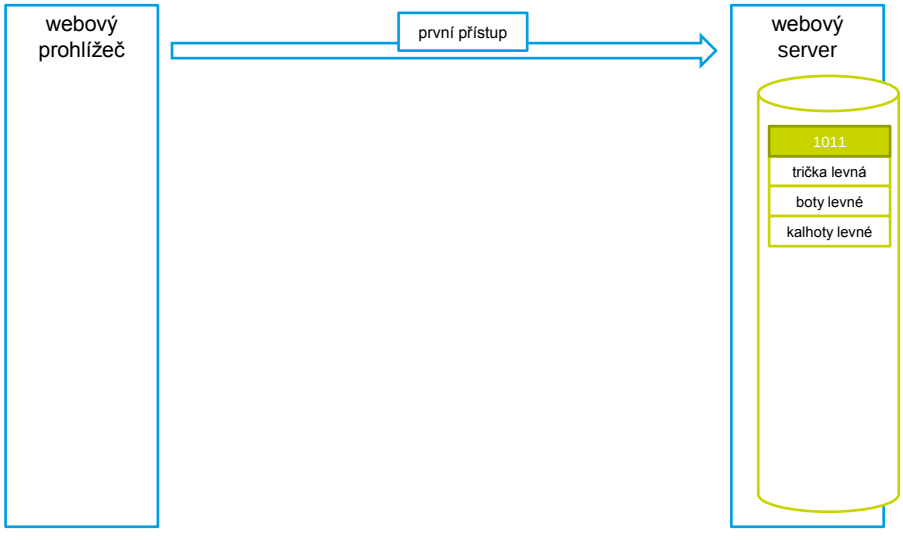
databáze přihlašovacích údajů

- jednoduché rušení souhlasu a mazání
- zpětná identifikovatelnost není problém

GOPAS

13

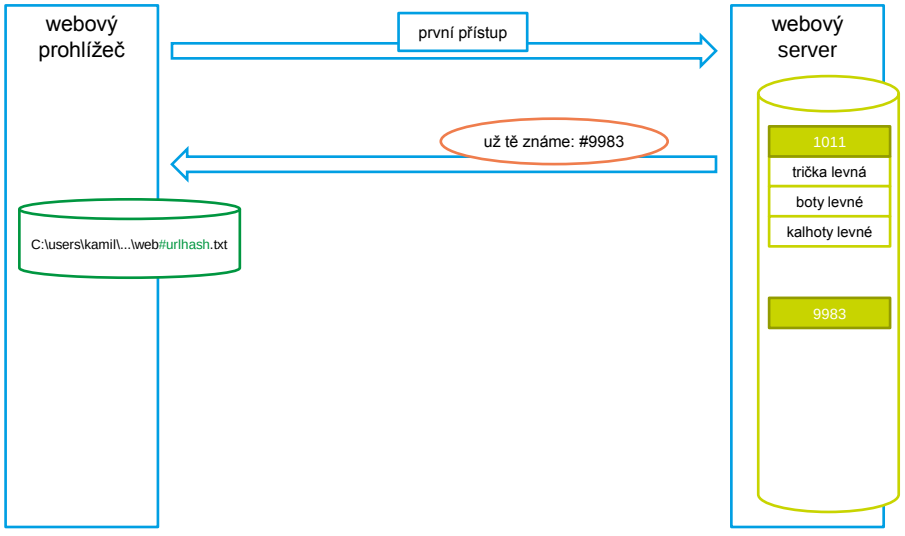
Cookies hlavní stránky nemusí být osobním údajem



GOPAS

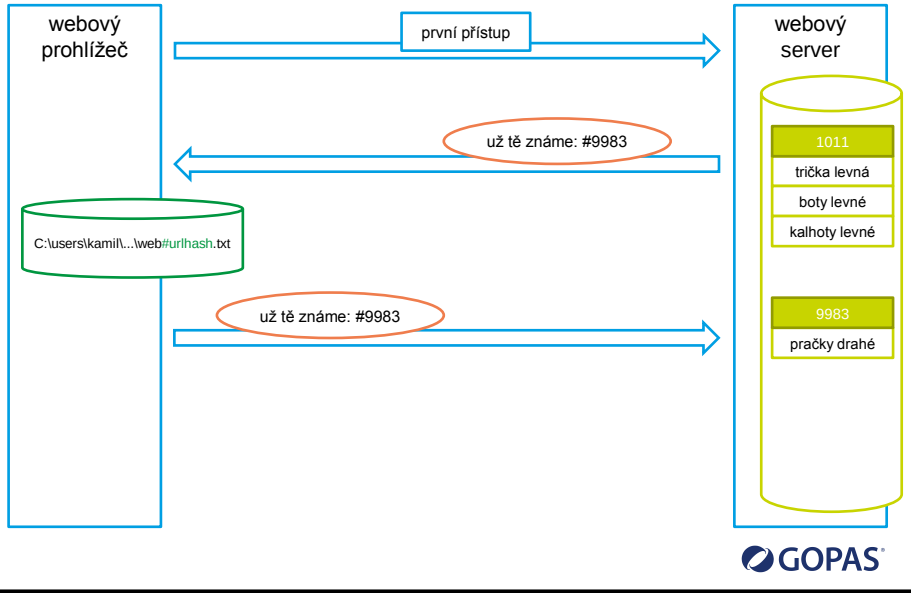
14

Cookies hlavní stránky nemusí být osobním údajem



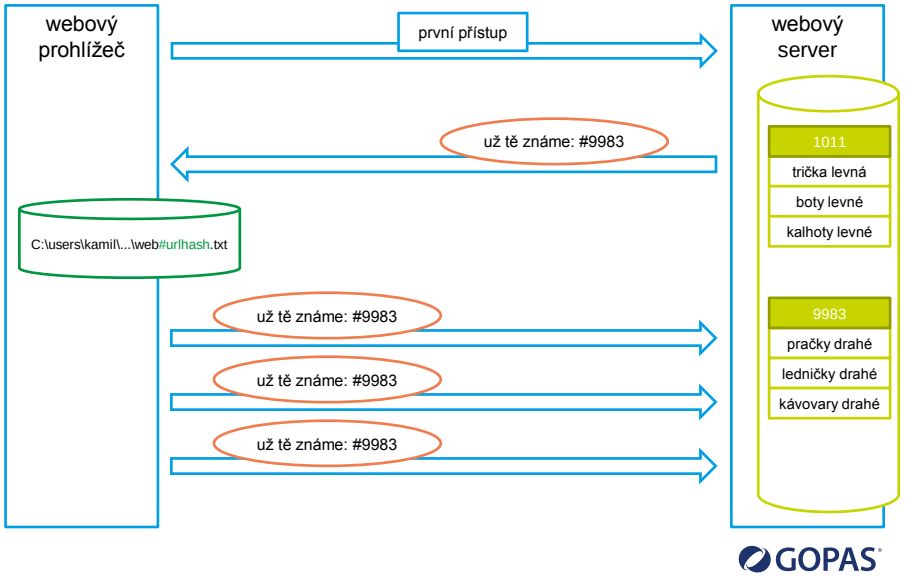
15

Cookies hlavní stránky nemusí být osobním údajem



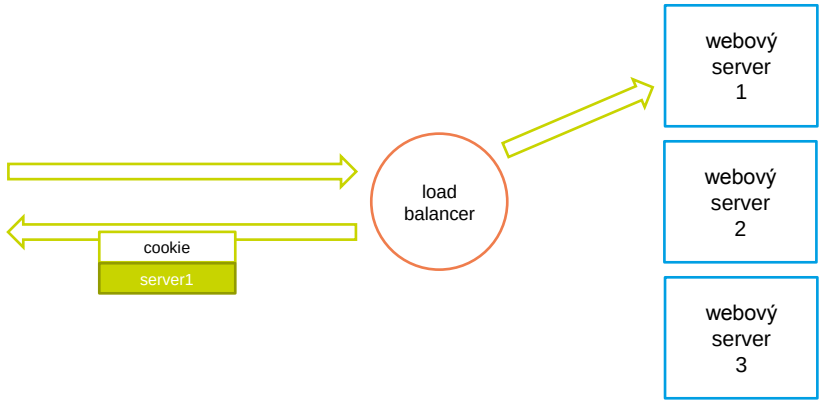
16

Cookies hlavní stránky nemusí být osobním údajem



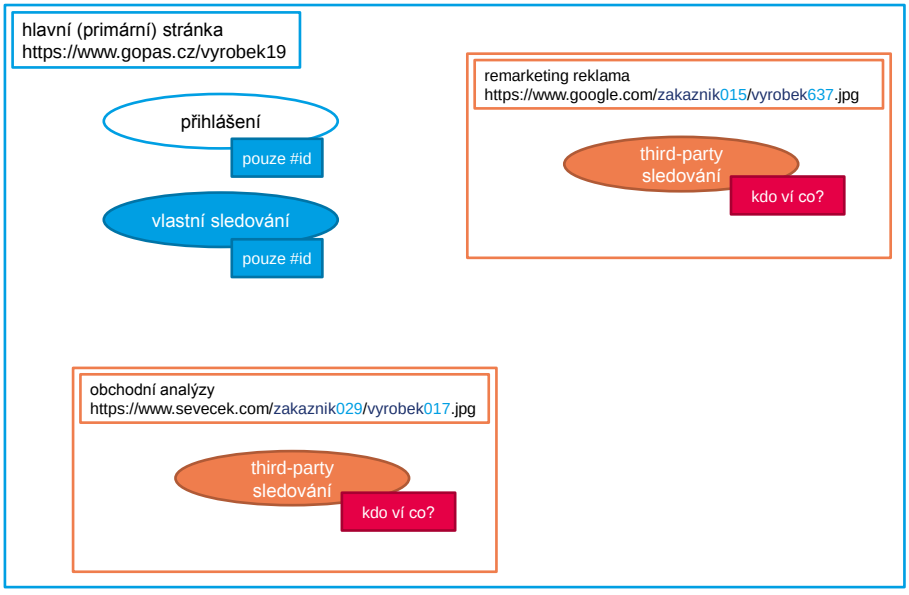
17

Technické cookies (load balancing)



18

Cookies primární a třetí strany a jejich sdílení



19

Názor na cookies

- Vyžaduje se opt-in, nikoliv opt-out, určitě ne „nechci vidět panel = souhlasím“
  - podle zákona č. 468/2011 Sb.
- "Souhlas není potřeba, pokud jsou cookies využívány pouze za účelem provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo nezbytné k tomu, aby mohl poskytovatel služeb informační společnosti zajistit služby, které si účastník nebo uživatel výslovně vyžádal."
- další výjimky ze souhlasu podle Article 29 DPWP (cookie consent exemption)
  - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
- typy cookies
  - session/persistent
  - first-party/third-party
  - sliding expiration
- druhy podle použití
  - user-input cookies (nepotřebuje souhlas)
  - authentication cookies (session nepotřebuje, persistent musí mít zaškrtávátko)
  - multimedia (flash) session cookies (nepotřebuje souhlas)
  - load-balancing cookies (nepotřebuje souhlas)
  - UI customizations (session/krátkodobé nepotřebují souhlas)

GOPAS

20

Příklady na cookie

- https://www.gopas.cz
- https://www.uoou.cz/cookies-prechod-z-principu-opt-out-na-opt-in/ds-1853/p1=1853
- http://www.iwc.com
- http://mirror.co.uk
- http://cyclingnews.com
- https://www.bbc.com

- https://cookie-bar.eu

GOPAS

21

Device fingerprinting?

- +/- náhrada cookies
- IP adresa, jazyk prohlížeče, verze prohlížeče, některá instalovaná rozšíření prohlížeče, ...

- nelze jen smazat cookies
  - a možná ani historii a mezipaměť prohlížeče
- jiný prohlížeč, jiný OS, ...

- riziko špatné identifikace jiného uživatele

GOPAS

22

Kombinovaná DAC/MAC a logická ochrana přístupu

- Discretionary access control - DAC (nebo mandatory access control - MAC)
  - řídí a omezuje přístup pomocí uživatelských účtů
  - každý může kdykoliv na všechna svoje data
  - z pohledu bezpečnostního auditu definuje maximální rozsah přístupu
- Logická vrstva ochrany na aplikační úrovni
  - přístup podle daného údaje
  - musím vědět koho chci zpracovávat
  - nelze považovat za definitivní omezení přístupu
    - náhoda a štěstí, iterativní zkoušení

GOPAS

23

Omezení dat na koncových bodech

- Notebooky, stanice, mobilní zařízení
- Všechna data trvale pouze na serverech
  - bez internetu nelze pracovat
- Technologie remote-wipe

GOPAS

24

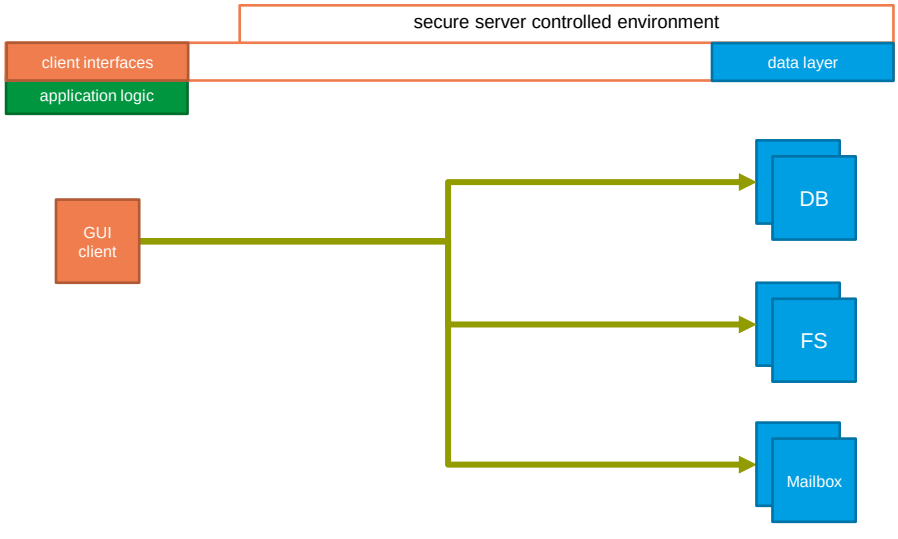
Omezení doby přístupnosti dat

- Maximální stáří položek v emailové složce
  - všechno starší se automaticky maže
  - compliance?
- Maximální stáří souborů na souborovém serveru
  - všechno starší se přesouvá do archivu nebo maže

GOPAS

25

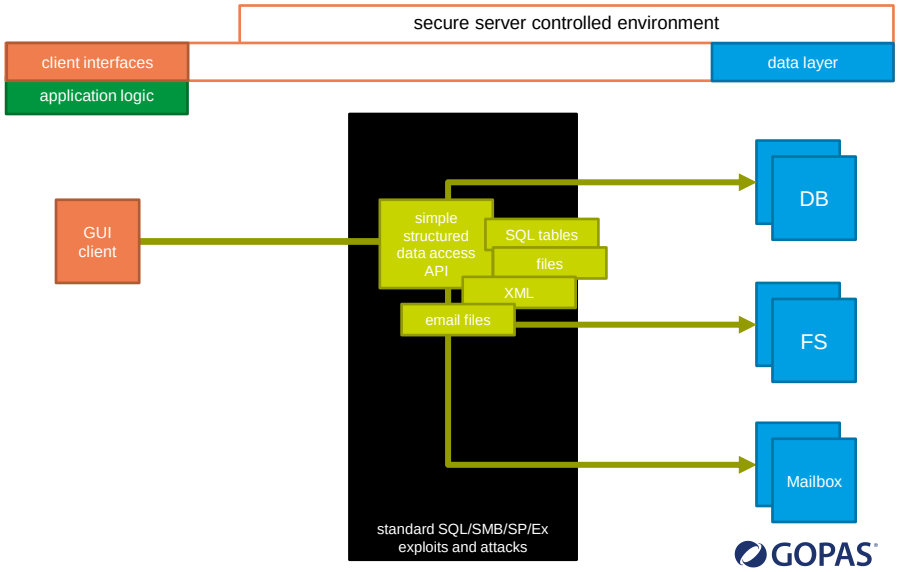
Aplikační vrstvy a jejich rizika



GOPAS

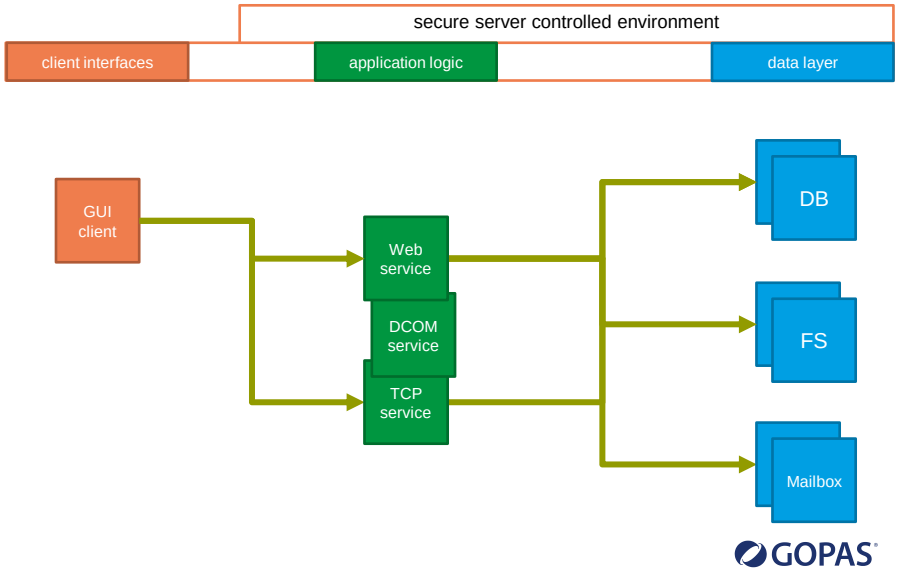
26

Aplikační vrstvy a jejich rizika



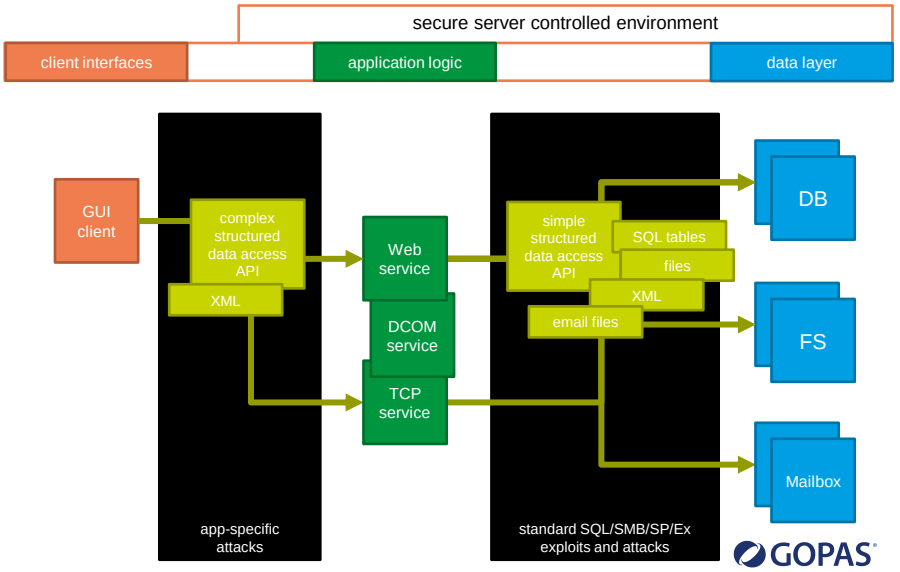
27

Aplikační vrstvy a jejich rizika



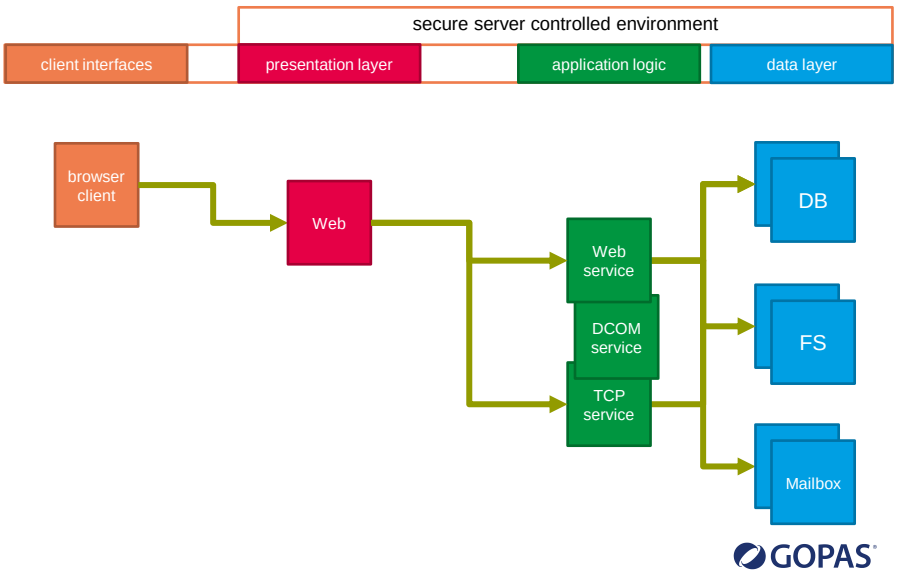
28

Aplikační vrstvy a jejich rizika



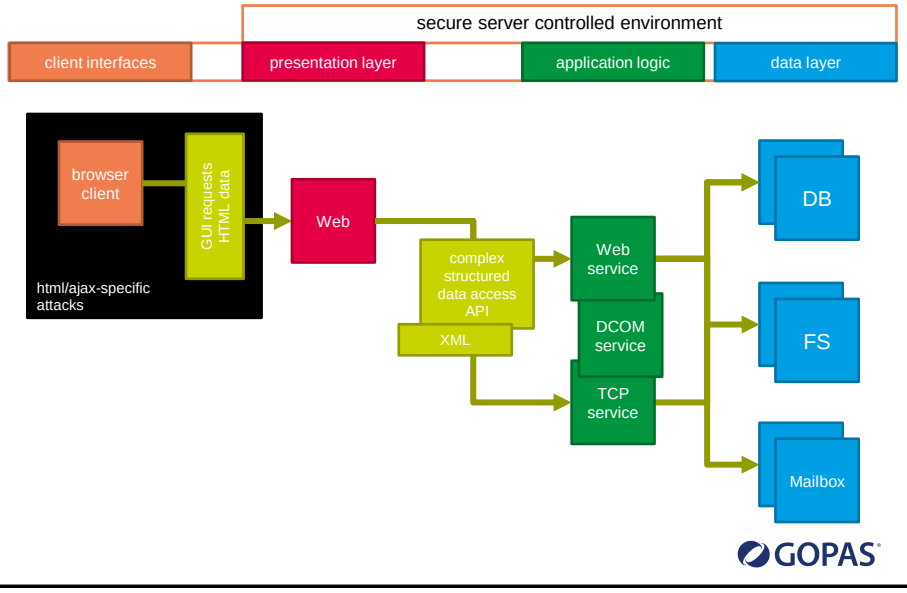
29

Aplikační vrstvy a jejich rizika



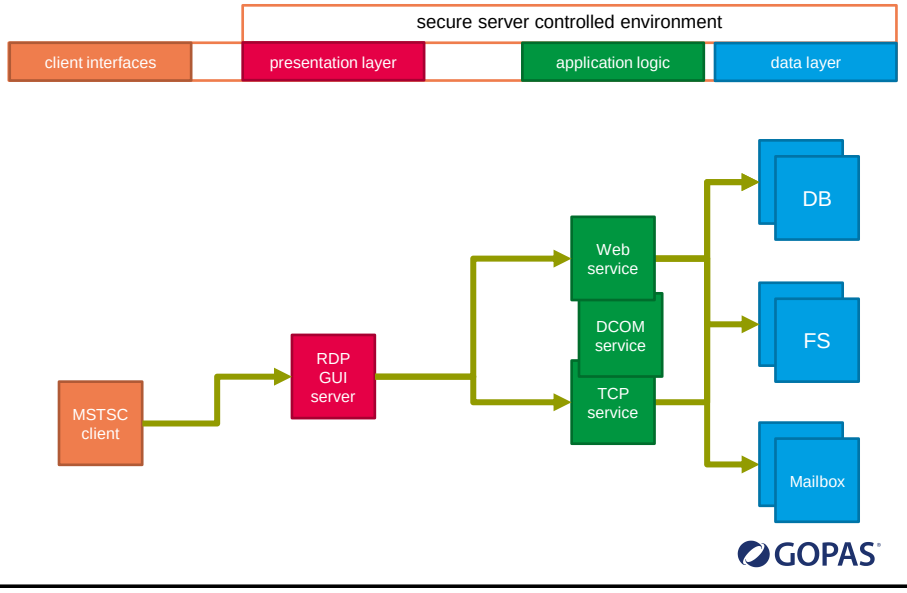
30

Aplikační vrstvy a jejich rizika



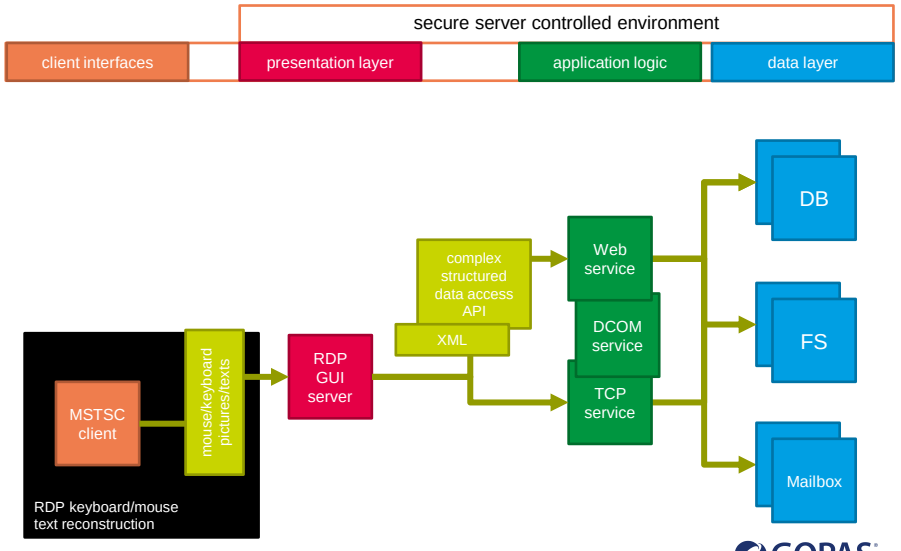
31

Aplikační vrstvy a jejich rizika



32

Aplikační vrstvy a jejich rizika



33

VPN není "absolutní bezpečnost"

- šifruje přenos
- řídí přístup oprávněných
- otevírá kompletní přístup do sítě

- co vyžadovat
  - MFA - multifactor authentication
  - pouze vynutit firemní zařízení

GOPAS

34

Více-faktorové ověření (MFA)

- login
  - nelze utajit v principu
- heslo + další faktor
  - mobil s aplikací
  - mobil a SMS
- čipová karta + PIN
- útoky na rozběhnuté sešny

GOPAS

35

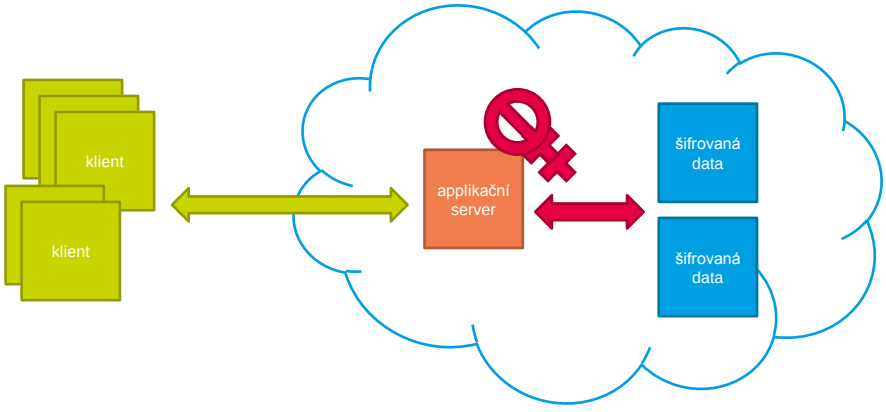
Šifrování dat

- Pouze doporučeno v GDPR (32.1a)
- Fyzická ochrana proti krádeži "cizincem"
- Nechrání nijak proti přístupu skutečně autorizovaných uživatelů
  - + privilegovaný správce s přístupem k OS s dešifrovacím klíčem
- Oddělení správců dat od uživatelů dat

GOPAS

36

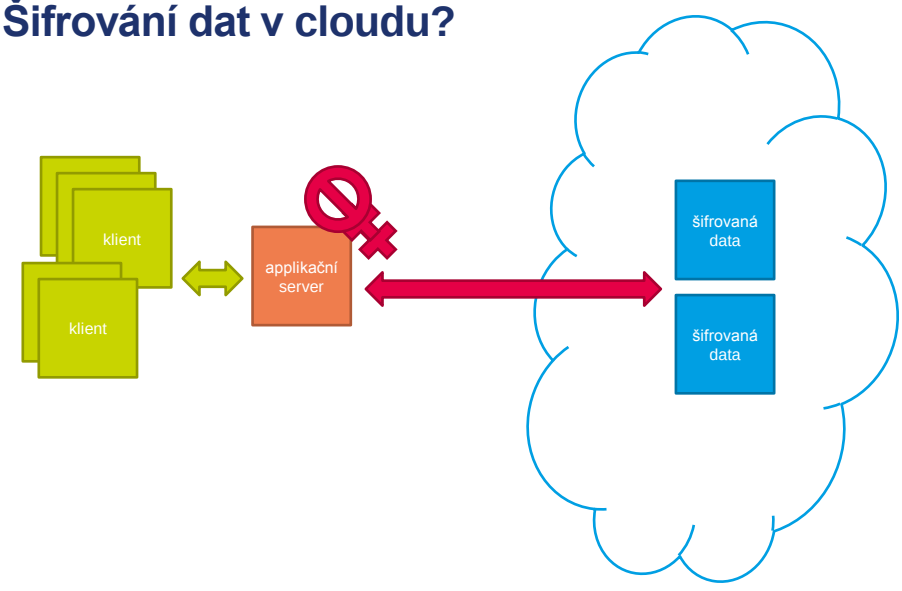
Šifrování dat v cloudu?



GOPAS

37

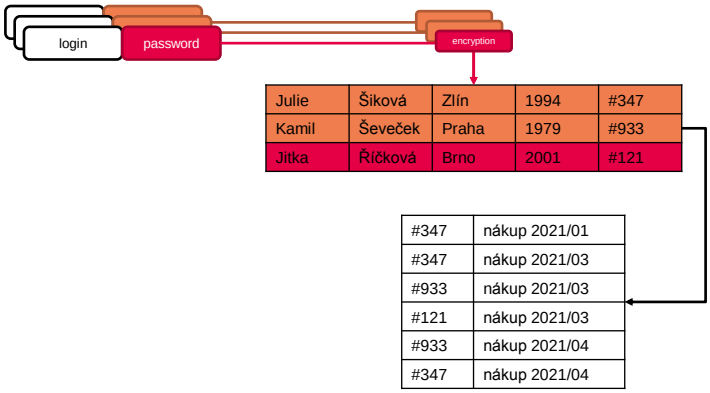
Šifrování dat v cloudu?



GOPAS

38

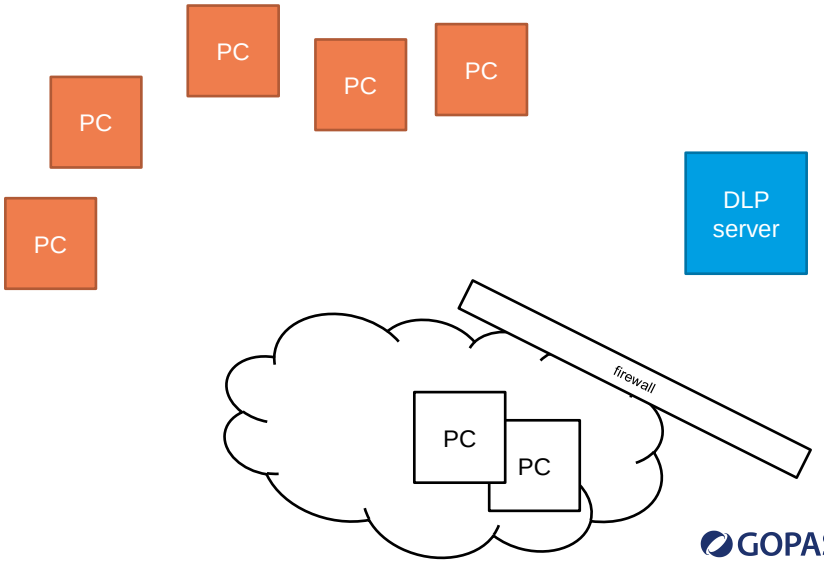
Per-uživatel šifrování (pseudonymizace)



GOPAS

39

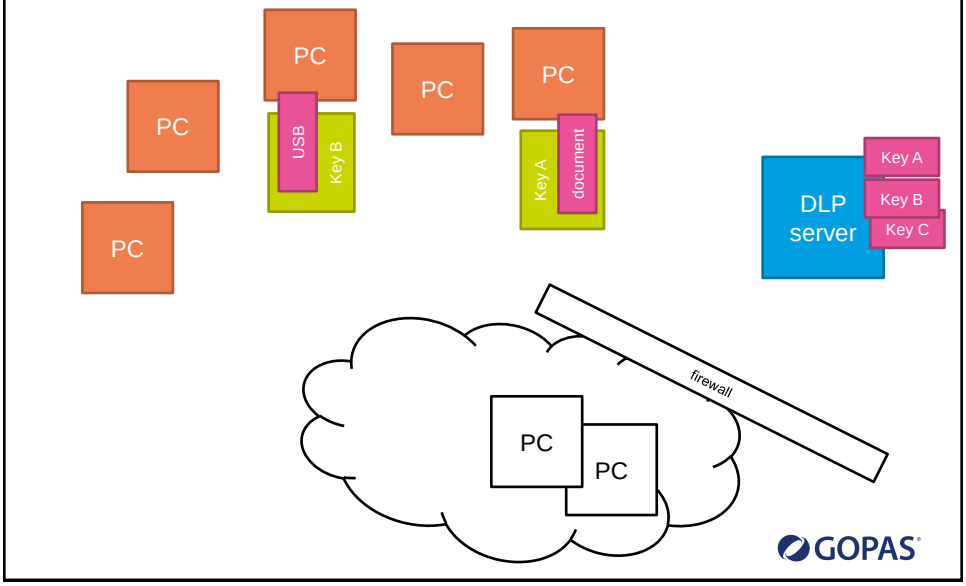
Data Leakage Prevention (DLP)



GOPAS

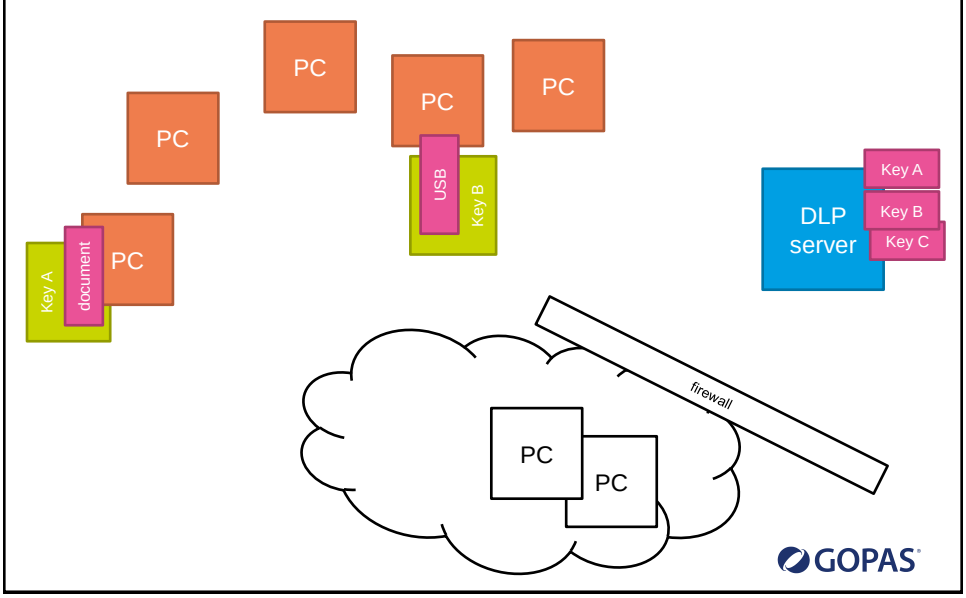
40

Data Leakage Prevention (DLP)



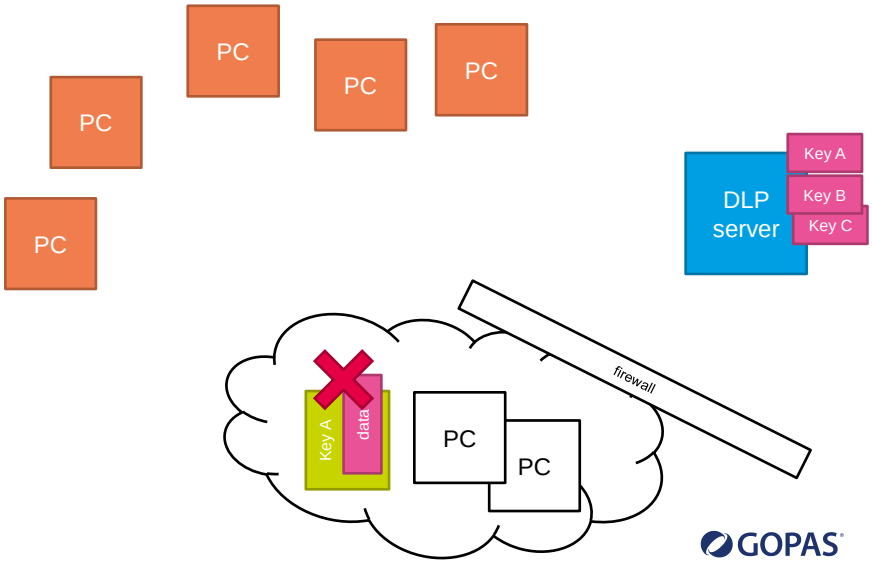
41

Data Leakage Prevention (DLP)



42

Data Leakage Prevention (DLP)



43

Co dalšího si uvědomit

Přehled GDPR

GOPAS

44

Data která musíme mít na paměti

- emaily a jejich přílohy, soubory a dokumenty, CSV a XML soubory
- DB tabulky a datové soubory
- úložiště v cloudu
- přenosná média, USB flash, DVD se zálohami
- papíry popsané, potisknuté, naskenované a zkopírované (2.1)
- zálohy a archivy
- mobilní zařízení, BYOD

- odvozená data
  - protokoly událostí, záznamy z vrátnice, přístupové systémy, odpovědi na emaily, firewall/proxy logy, GDPR zpracovatelské a ne/souhlasové logy
  - tempy

- osobní data a činnosti zaměstnanců na firemních počítačích
  - kontrola autorizovanou osobou vs. široké zveřejnění
  - důvodné očekávání (reasonable expectation)
  - šikana jednotlivců vs. sledování větších skupin

GOPAS

45

Životní cyklus dat

- operační online data
- provozní zálohy
  - nejnovější záloha kvůli uvedení do chodu po výpadku
  - krátkodobá záloha kvůli obnově smazaných a poškozených datových položek
- provozní „předchozí verze“
  - Exchange smazané položky
  - Předchozí verze dokumentů
- dlouhodobé zálohy (compliance) (archivace)
  - obnova kvůli vyhovění "zákonnému" požadavku
  - obnova kvůli vyšetřování starších incidentů

- mazání dat
  - celá data vs. jednotlivé záznamy
  - zpětné odmazání po obnově

- logy

GOPAS

46

Zálohování a obnova

- nainstalované operační systémy a aplikace
  - binární soubory, OS image, ...
  - postup nové instalace "na čisto"
- konfigurační soubory a nastavení
  - soubory, registrové hodnoty, ...
  - dokumentace nastavení po instalaci "na čisto"
- data
  - RPO - recovery point objective
  - RTO - recovery time objective

GOPAS

47

Hrozby osobním údajům (4.12)

- Ztráta
  - nezáměrná ztráta
  - záměrná krádež "cizincem"
  - záměrná krádež "internistou" (inside-job)
- Modifikace
  - nezáměrná (šum)
  - cílená modifikace k vlastní výhodě nebo poškození subjektu
    - ransomware
  - krádež identity (identity theft)

GOPAS

48

IAA terminologie

- Identification = identifikace
  - kdo ten člověk tvrdí že je
- Authentication = autentizace / autentifikácia (autentikace ne)
- Authorization = autorizace

- Autentizace v případě souhlasů se zpracování osobních údajů dětí (8.1)
  - děti 16+ mohou dávat vlastní souhlas
  - děti 16- potřebujeme souhlas zákonného zástupce
  - (CZ úprava údajně 13let)

GOPAS

49

Řešení rizik

- Minimalizace/zmírnění
  - plus akceptace zbytkového rizika
- Ukončení
  - prostě přestaneme dané údaje zpracovávat
- Přenos
  - pojištění, zpracovatelská smlouva se sankcí

GOPAS

50

Privilegované činnosti správců

- IT admin
- ostraha
- servis elektro, komunikace, ...

- oddělení rolí (zodpovědností)
- oddělení účtů
  - při nedostatečné separaci zodpovědností

GOPAS

51

Postup implementace

Přehled GDPR

GOPAS

52

Zaveďte si alespoň "jako" DPO

- DPO vyžadována podle (37.1)
  - bezpečnost musí být vždy řízena
- Může být sdílen (37.2)
- Může být zaměstnanec (37.6)
- Může pracovat na více věcech (38.6)
- Vybrána na základě profesních kvalit (37.5)

- Komunikace se subjekty údajů a řešení jejich požadavků
- Komunikace s úřadem a hlášení incidentů (39.1d, 39.1e)
- Komunikace IT/právníci/vedení
- Dohled (39.1b), nápady na vylepšení (39.1a), řešení incidentů, účast na výběrových řízeních, dokumentace
- Školení zaměstnanců (39.1b)
- Udržování povědomí vedení (83.2b)
  - Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti ... zda k porušení došlo úmyslně nebo z nedbalosti ...

- Auditor znamená nezávislost
  - nemůžu si auditovat co jsem si sám vymyslel, rozhodl, nebo implementoval, nebo co dělám
  - můžu (pomoci) vytvářet dokumentaci
- DPO
  - nesmí jen „definovat účely zpracování“, nesmí „rozhodovat o opatřeních“ a nesmí „implementovat/dodržovat opatření“

GOPAS

53

Zajistěte si podporu nejvyššího vedení

- Jen oni jsou ve výsledku zodpovědní
- Jen oni rozhodují o "útratách"
- Jen oni přijímají zbytková rizika

- DPO není v podstatě za nic zodpovědný
  - koná podle nejlepšího vědomí a svědomí

GOPAS

54

Analýza a dokumentace PII prostředí

- Proaktivní zabezpečení (5.1f)
  - S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům ... (25.1)
- Dokumentace a povinnost doložit proaktivní ochranu (5.2)

GOPAS

55

Redukční analýza a dokumentace PII prostředí (řízení aktiv)

- Obláčky osobních údajů
  - bez průniků
  - které údaje, účel a souhlasy, systémy, úložiště
- Vstupní a výstupní rozhraní
  - email, webové stránky, šnečí pošta, GUI
  - aktualizace/souhlasy/mazání subjektem
  - přenos od jiných a k dalším správcům
  - doba zpracování
- Politika řízení přístupu (access control policy) (32.4)
  - čtení, změny, mazání, použití (internet, kalkulačka), udělování přístupu
- Kompozice vnitřního rozložení dat
  - mailové schránky, soubory, DMS, CRM, zálohy, výtisky, ...
  - HDD, off-site, cloud
  - Backup, archivy
- Logování operací zpracování a provozní
  - plus kamery
- Technické vnitřní toky údajů mezi úložišti
  - technické, procedurální, audit přístupu
- Fyzická bezpečnost a přístup

GOPAS

56

Nezpracovávat a neukládat údaje déle než je nutné

- A znát přesné doby a důvody (5.1e)

GOPAS

57

Souhlasy

- Konkrétní a informované (32)
- Zvláštní souhlas na citlivé (zvláštní) údaje (9.2a)
- Zvláštní souhlas a poučení o profilování (13.2f)
- Super zvláštní souhlas a poučení o rizicích v případě předávání do neGDPR prostředí (49.1)

- Kontaktní informace na správce a DPO (13.1)
- Informace o době zpracování a uložení (13.2a)

GOPAS

58

Informační povinnost k subjektu údajů

- Jestli vůbec zpracováváme (14.x)
- Co, proč, jak dlouho, jestli jsme předali dalšímu správci
- Zdroj údajů, pakliže přišly přenosem od jiného správce (15.1g)
- Reakce do 1 měsíce (12.3)
- Export v běžně používaném strojově zpracovatelném formátu (15.3)
  - email? https?

GOPAS

59

Možnost odebrání souhlasu a žádost o smazání

- Stejnou cestou jako se souhlas vydával (7.3)
- Aktualizace údajů (16.x)
- Smazání (right to be forgotten) (17.1)
- Ideálně automatickou cestou
- Pokud byly údaje zveřejněny, měli bychom ostatní správce přiměřenou cestou informovat (17.2)

GOPAS

60

Zpracovatelské protokoly

- Kdo, proč, co (30.1) + mezinárodní předání
- Nad 250 zaměstnanců se vyžaduje (30.5)
- DPA si je může vyžádat do 72 hodin (30.4)

GOPAS

61

Sledování a hlášení incidentů

- Povinné hlášení incidentů do 72 hodin (33.x) (34.x)
- Úřadu i zasaženým subjektům údajů
  - fázovatelné bez zbytečného odkladu (33.4)

GOPAS

62

Posouzení vlivu na zpracování osobních údajů (35.x)

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad
- 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

- Co, účely, nezbytnost, rizika pro subjekty, opatření (35.7)

GOPAS

63

Dobrovolná certifikace

- Osvědčení od úřadu (42.x)
- Nezávislá oborová certifikace bezpečnosti informací
  - ISO 2700x

- Kodexy chování asociací (40.x)
  - schvaluje úřad

GOPAS

64