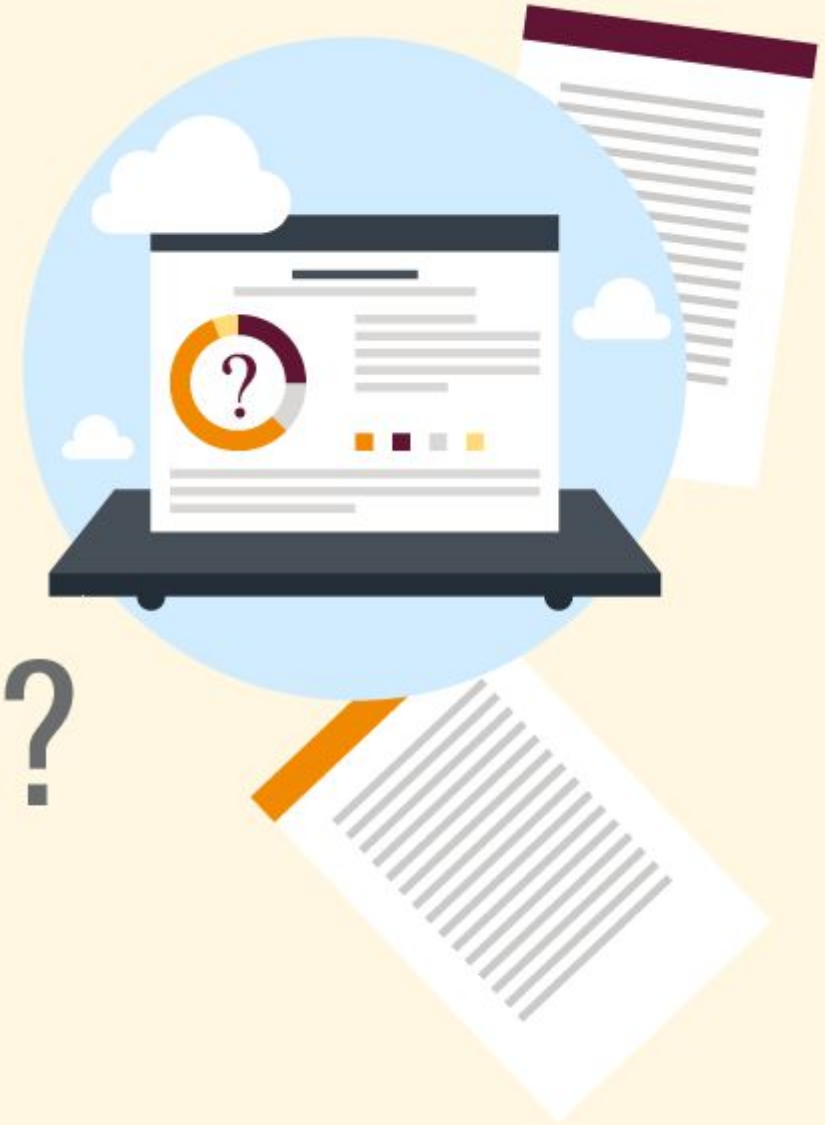
EVA ŠKORNIČKOVÁ

Obecné nařízení na ochranu osobních údajů

Úvod

Co je GDPR?



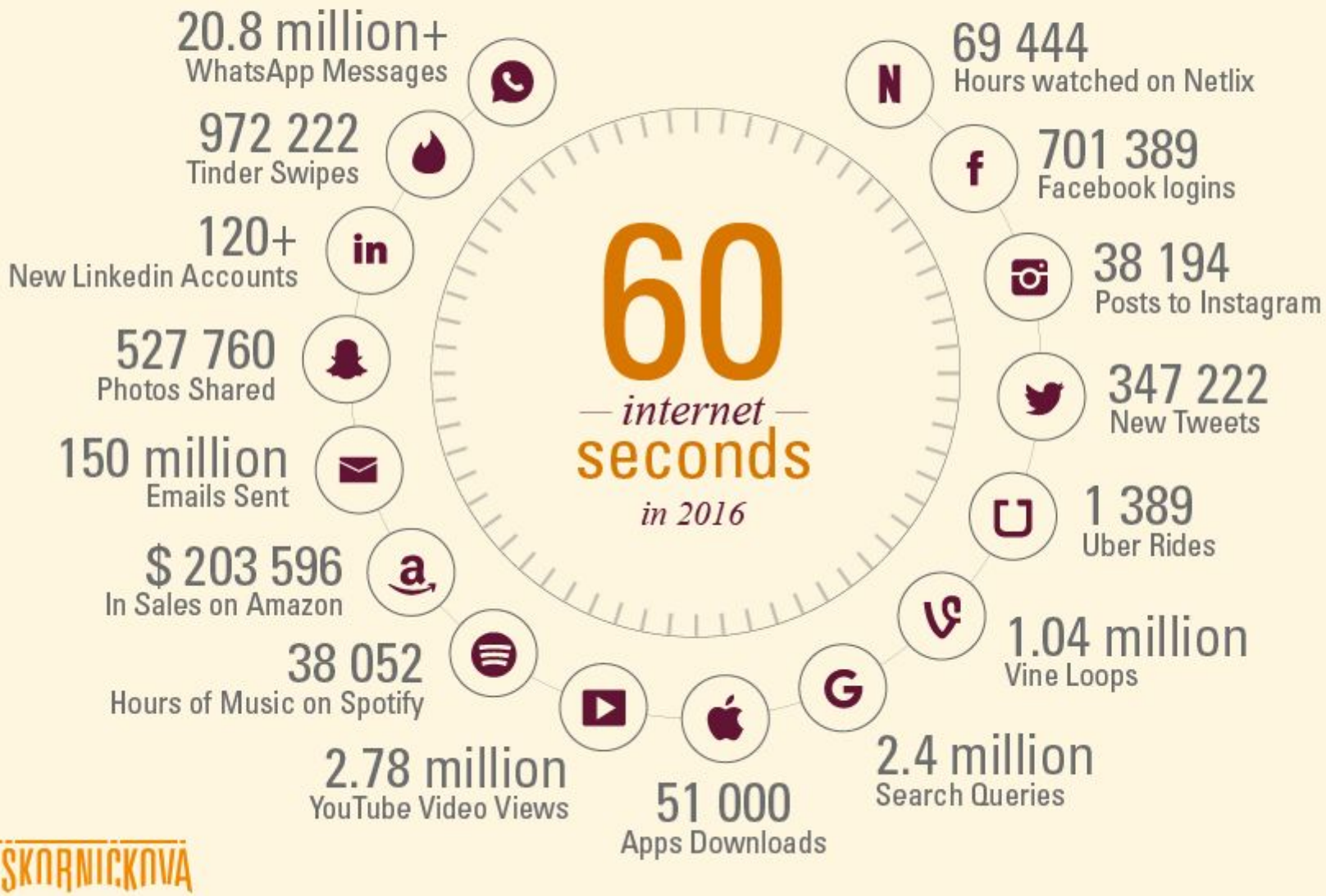
EVA ŠKORNIČKOVÁ

GDPR

- Nařízení bylo schváleno Evropským parlamentem 14. 4. 2016 po 4 letém vyjednávání
- Nahrazuje Směrnici 95/46 EC s účinností od 25.5. 2018 a v ČR zákon č. 101/2000 Sb. na ochranu osobních údajů
- Nejkomplexnější soubor pravidel na ochranu dat na světě
- Výrazným povýšením ochrany dat na úroveň evropského zákona se posiluje právo osob na lepší kontrolu nad jejich osobními údaji
- Harmonizace pravidel pro 28 států EU a EFTA zemí - Norsko, Island a Lichtenštejnsko = státy Evropského hospodářského prostoru - 31 národních zákonů bude zrušeno
- Rovnocenná vymahatelnost práva a stejné sankce pro všechny státy, konzistentní právní úprava, účinná spolupráce regulatorních orgánů
- Představuje rovnováhu mezi legitimními zájmy správců a zpracovatelů dat a právem osob na soukromí

EVA ŠKORNICKOVÁ

Proč potřebuje ochrana dat *reformu?*



EVA ŠKORNICKOVÁ

Správní *pokuty*

Výše závisí na řadě faktorů

- Povaha, závažnost a délka porušení s přihlédnutím k povaze, rozsahu či účelu zpracování
- Úmysl nebo nedbalost
- Počet dotčených subjektů a míra škody
- Kroky podniknuté správcem či zpracovatelem ke zmírnění škod
- Míra odpovědnosti s přihlédnutím na technické a organizační opatření
- Předchozí porušení
- Míra spolupráce s dozorovým úřadem za účelem nápravy
- Kategorie osobních údajů dotčené porušením
- Způsob, jakým se dozorový úřad dozvěděl o porušení

20 000 000 EUR

nebo *4 %* z celkového ročního obratu celosvětově za předchozí finanční rok

10 000 000 EUR

nebo *2 %*

EVA ŠKORNICKOVÁ

Článek 83

CO
se změní

EVA ŠKORNICKOVÁ

1. Směrnice *versus* nařízení

Směrnice

- Dokument přijatý na úrovni EU
- Národní implementace (“naklonování”)
- Místní variace (“genetické varianty”)

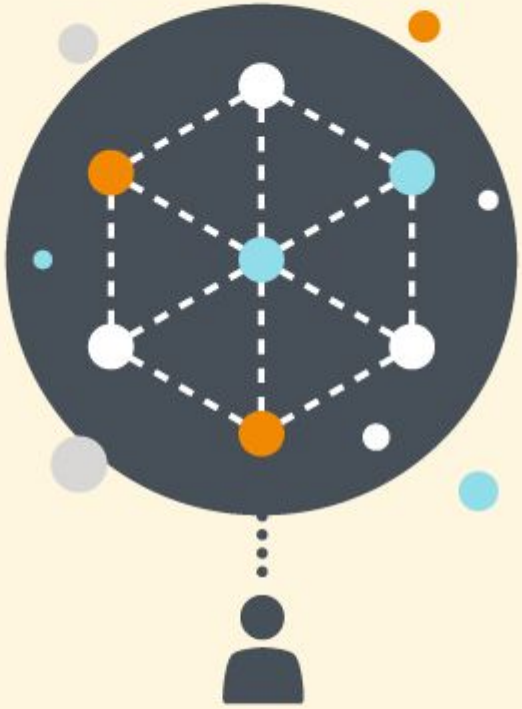
Nařízení

- Dokument přijatý na úrovni EU
- Není potřeba národní implementace
- “Jeden předpis řídí všechny”

EVA ŠKORNIČKOVÁ

Osobní *údaje*

- Veškeré informace vztahující se k identifikované nebo identifikovatelné fyzické osobě
- Nevztahuje se na osobní údaje zesnulých osob a anonymizované údaje
- Vztahuje se na šifrované osobní údaje, protože někdo zná šifrovací klíč



Fyzické osoby

Podnikatelé

- OSVČ
- Právnické osoby

EVA ŠKORNICKOVÁ

článek 4 (1)
vysvětlivky 26 - 27

Osobní údaje
- jednotlivé prvky

Obecné

- Jméno
- Pohlaví
- Věk a datum narození
- Osobní stav
- Občanství
- IP adresa
- Fotografický údaj

Organizační

- pracovní nebo osobní adresa
- pracovní nebo osobní telefonní číslo
- pracovní nebo osobní e-mail
- ověřovací identifikační údaje
- identifikační čísla vydaná státem

ČÍM VÍCE OSOBNÍCH ÚDAJŮ MÁTE, TÍM VĚTŠÍM RIZIKŮM SPOJENÝM S JEJICH OCHRANOU SE VYSTAVUJETE!

EVA ŠKORNICKOVÁ

Citlivé osobní údaje
- speciální kategorie

Vypovídají o:

- Rasovém či etnickém původu
- Politických názorech
- Náboženském nebo filozofickém vyznání
- Členství v odborech
- Zdravotním stavu
- Sexuální orientaci
- Trestních deliktech či pravomocném odsouzení

Genetické a biometrické údaje

Osobní údaje dětí

EVA ŠKORNICKOVÁ

3. Značně rozšířený *dosah*

Nový zákon platí pro:

- Podnik v EU
- Nabídku zboží a služeb rezidentům EU
- Monitorování chování rezidentů EU

EVA ŠKORNICKOVÁ

4. Přímé závazky *pro Zpracovatele dat*

- Současné právo = žádné povinnosti pro zpracovatele (poskytovatele služeb)
- Nový zákon = přímá odpovědnost zpracovatelů
- Velký dopad na cloudové služby
- Povinné smlouvy mezi správci a zpracovateli

Zpracovatel:

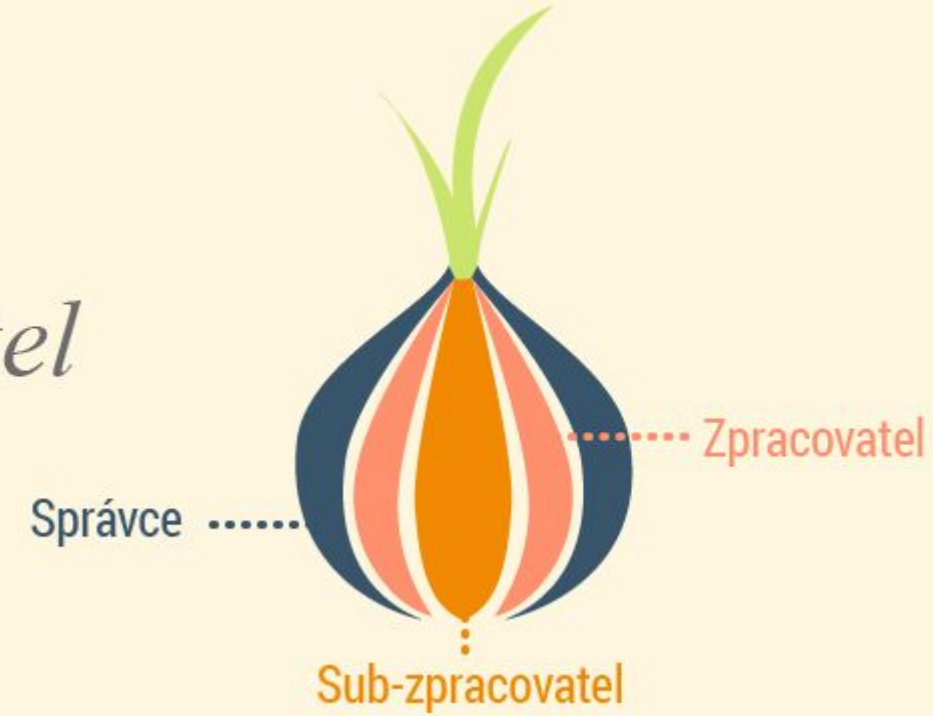
Fyzická nebo právnická osoba, která zpracovává data jménem správce

Správce:

Fyzická nebo právnická osoba, která sama nebo spolu s jinými určuje účel a způsoby zpracování

EVA ŠKORNICKOVÁ

Správce
a Zpracovatel



Zpracovatel:

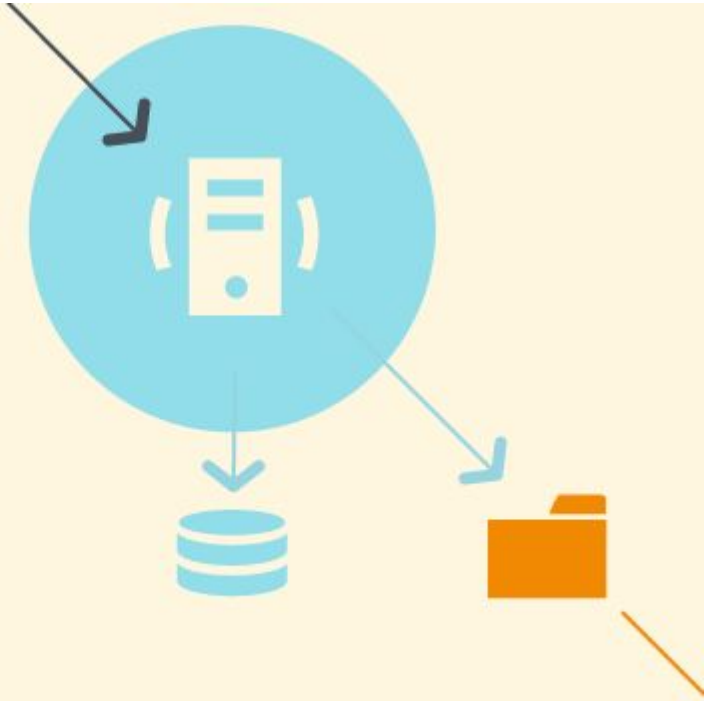
Fyzická nebo právnická osoba, která zpracovává data jménem správce

Správce:

Fyzická nebo právnická osoba, která sama nebo spolu s jinými určuje účel a způsoby zpracování

EVA ŠKORNICKOVÁ

Zpracování *osobních údajů*



Jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí nebo bez pomoci automatizovaných postupů spočívající v:

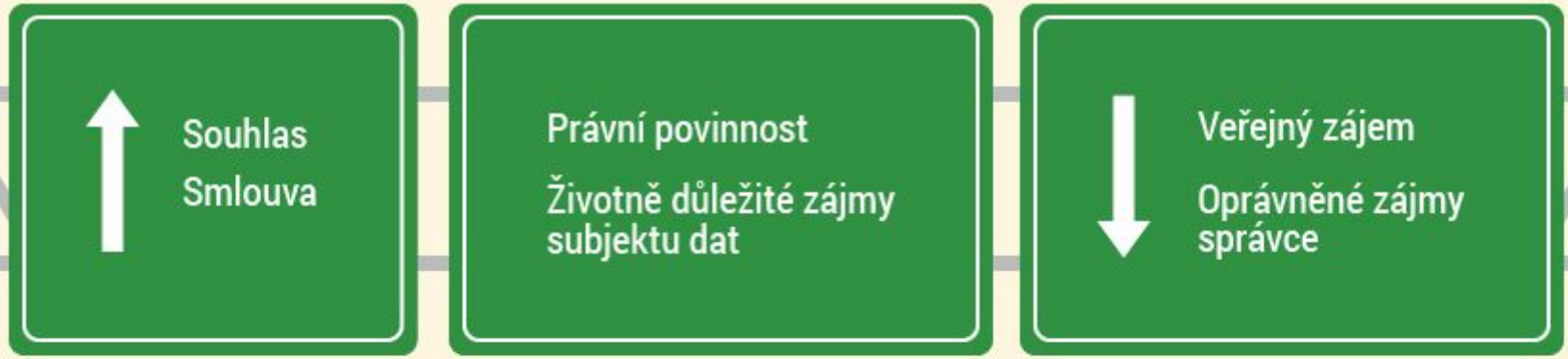
- Shromáždění
- Zaznamenání
- Uspořádání
- Strukturování
- Uložení
- Přizpůsobení nebo pozměnění
- Vyhledání
- Nahlédnutí
- Použití
- Zpřístupnění přenosem
- Šíření nebo jakékoliv jiné zpřístupnění
- Seřazení či zkombinování
- Omezení
- Výmaz nebo zničení

EVA ŠKORNICKOVÁ

článek 4 (2)

Zákonnost zpracování *osobních údajů*

- Musí být splněna aspoň 1 z podmínek



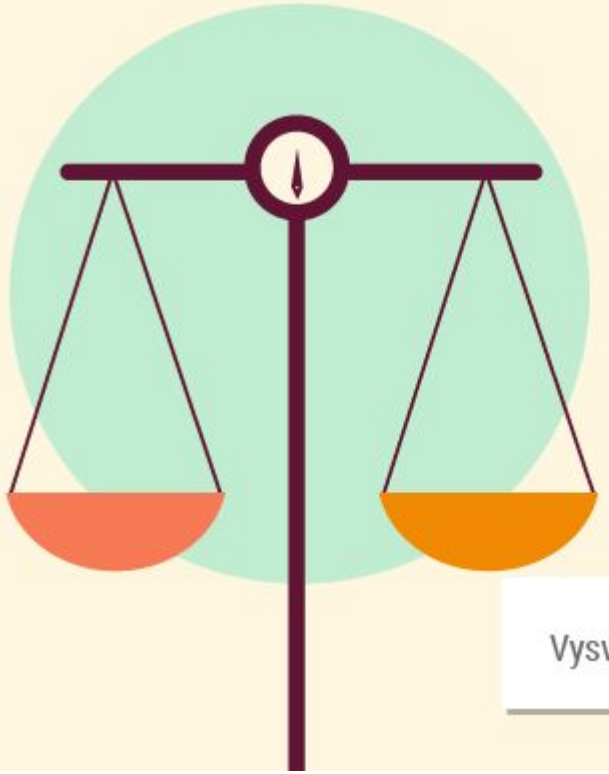
EVA SKORNICKOVÁ

Článek 6
vysvětlivka 40

Zpracování dat z důvodu oprávněného zájmu *správce nebo třetí strany*

- Oprávněné zájmy správce nesmí převažovat nad zájmy nebo právy a svobodami subjektu údajů = ROVNOVÁHA
- Např. předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely

Zpracování těchto údajů se doporučuje se souhlasem subjektu dat



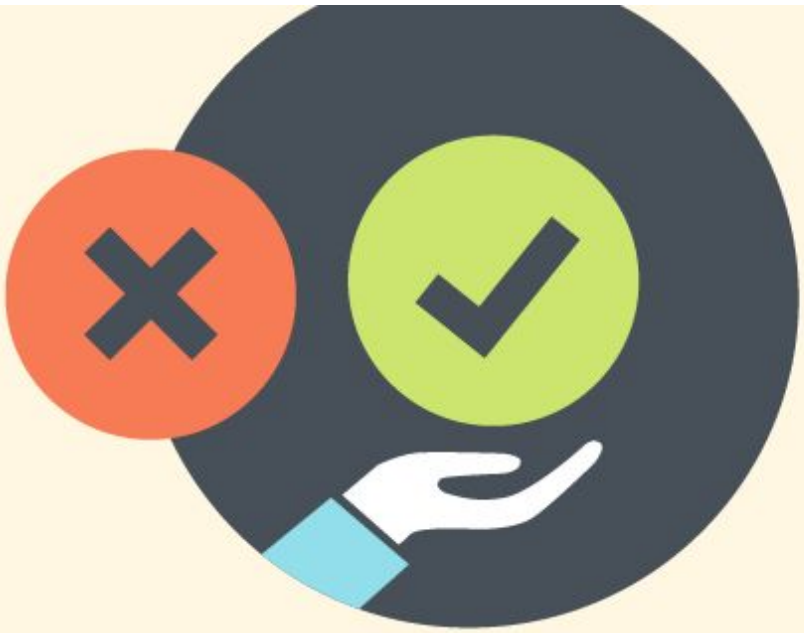
Vysvětlivky 47 - 49

Zákonnost zpracování *osobních údajů*

Souhlas subjektu údajů není nutný pro zpracování údajů na základě

- smlouvy - nikdy nedávat souhlas do smlouvy
- pro ochranu životně důležitých zájmů subjektu - např. subjekt dat je v bezvědomí a není schopen udělit souhlas
- pro splnění právní povinnosti správce nebo pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci - např. soukromé pojišťovny, zdravotnická zařízení - může být specifikováno národní legislativou

Státní úřady mohou zpracovávat osobní údaje jen ve veřejném zájmu nebo pro splnění právní povinnosti - např. daňový úřad, policie atd.



6. Souhlas

a

- Daný svobodně
- Konkrétní
- Informovaný
- Jednoznačný
- Vyjádření přání

Souhlas rodiče

- Do 16 let
- Nižší věk (podle práva členského státu)
- Minimálně 13 let

EVA ŠKORNIČKOVÁ

Zpracování *citlivých dat*

Je možné jen za těchto předpokladů:

- Výslovný souhlas subjektu údajů se zpracováním
- Zpracování je nezbytné v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany
- Zpracování je nutné pro ochranu životně důležitých zájmů subjektu, v případě, že subjekt není fyzicky nebo právně schopen udělit souhlas
- Zpracování sleduje politické, filozofické, náboženské nebo odborové cíle - nadace, sdružení, neziskové organizace
- Zpracování se týká údajů zjevně zveřejněných subjektem údajů
- Zpracování je nezbytné pro obhajobu právních nároků nebo v rámci soudního řízení
- Z důvodu veřejného zájmu na základě EU nebo národního práva
- Pro účely preventivního lékařství, posouzení pracovní schopnosti zaměstnance, veřejného zájmu v oblasti veřejného zdraví
- Zpracování pro účely vědeckého, historického výzkumu nebo statistické účely

Práva subjektů osobních údajů
- *výrazně posílena*

1. Přístup
2. Oprava
3. Výmaz a “právo být zapomenut”
4. Omezení zpracování
5. Přenositelnost údajů
6. Vznést námitku

Vztahuje se na všechny osobní údaje včetně tzv. nestrukturovaných, tj. uložených např. v přílohách k e-mailu, na různých úložištích

Toto právo může být ze strany nespokojených zákazníků nebo zaměstnanců zneužíváno!

OZNÁMENÍ (PRIVACY NOTICE) - měl by upravovat postup, jakým může subjekt osobních údaju uplatnit svoje práva

EVA ŠKORNICKOVÁ

5. *Nové požadavky* na zodpovědnost

- *Vhodná opatření k prokázání souladu (compliance)*
- *Mohou zahrnovat:*
  - Vyhodnocení dopadu na soukromí
  - Záměrná a nezbytná ochrana dat (Privacy by design/by Default)
  - Implementace procedur na ochranu dat
  - Jmenování DPO
  - Pseudonymizace osobních dat
  - Povinnost uchovávání záznamů u správců a zpracovatelů
  - Spolupráce správců a zpracovatelů s dozorovými orgány

6. Pseudonymizace

d

- Zpracování takovým způsobem
- Aby data již nemohla být přiřazena ke konkrétnímu subjektu dat
- Bez použití dalších informací
- Dokud jsou tyto informace uchovávány samostatně a podléhají opatřením

EVA ŠKORNIČKOVÁ

Zodpovědnost:

Povinný pověřenec pro ochranu osobních údajů (DPO)

Požadavek na správce a zpracovatele

Hranice pro jmenování:

- Povinný pro veřejné orgány
- Rozsáhlé systematické monitorování fyzických osob
- Rozsáhlé zpracování citlivých dat

Úkoly:

- Monitorování souladu
- Řízení činností interní ochrany dat
- Školení pracovníků ve zpracování dat
- Provádění interních auditů

EVA ŠKORNICKOVÁ

Článek 37 - 39

Kam až může GDPR dosáhnout

v rámci organizace

Osobní informace

- Elektronické
- Listinné

Souhlasy

CRM

ERP

COM

HRM

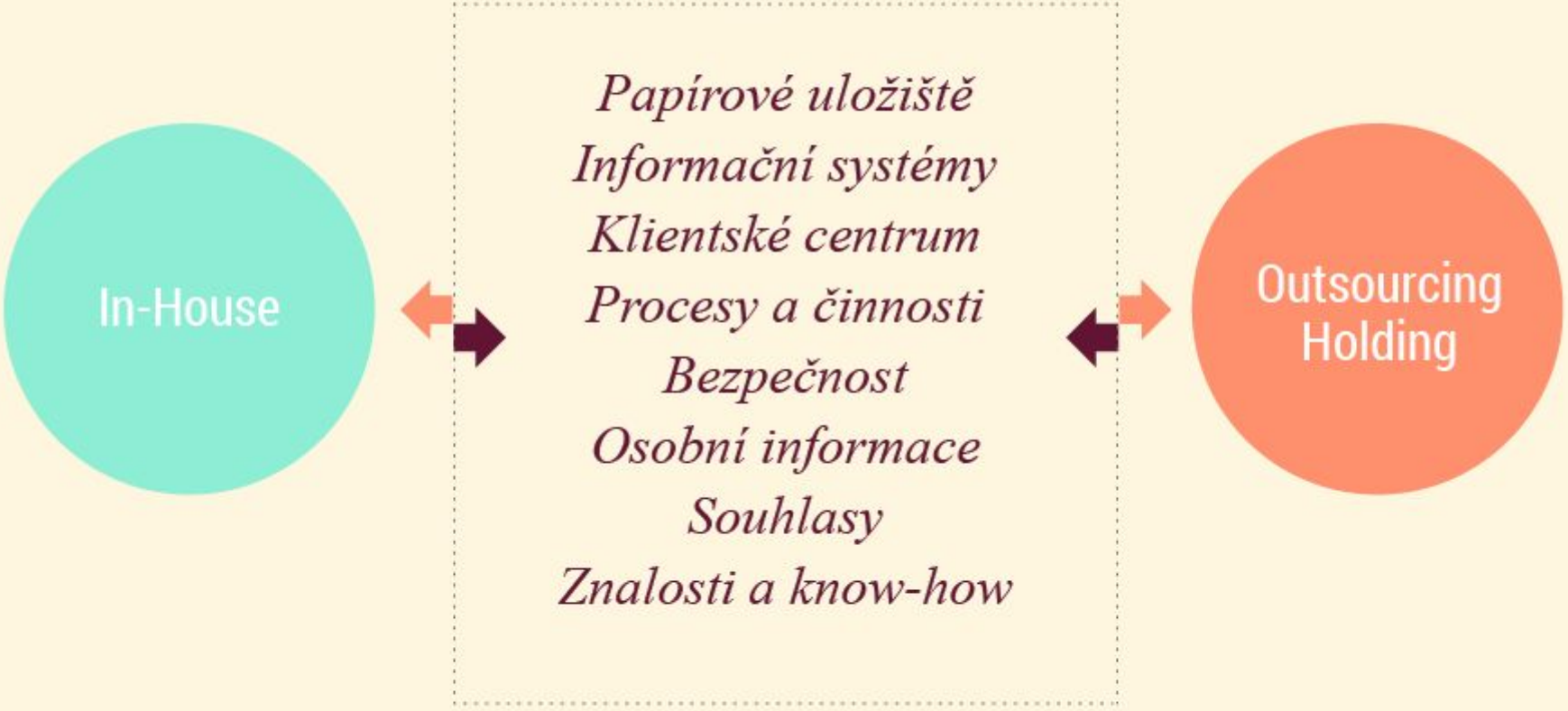
ZIS

...

- Bezpečnostní odd.
- Finanční odd.
- IT a Technické odd.
- Klientské odd.
- Legislativní a právní odd.
- Logistické a výrobní odd.
- Marketingové odd.
- Obchodní odd.
- Personální odd.

EVA ŠKORNICKOVÁ

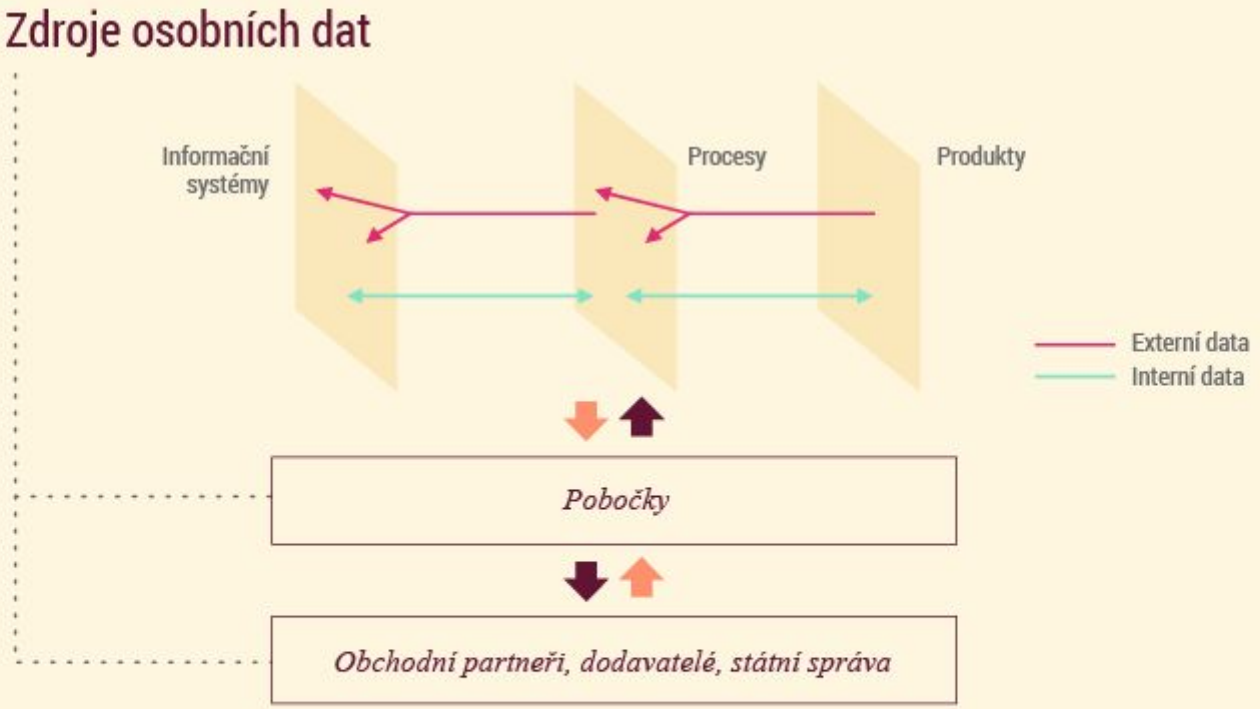
Rozsah oblastí
s možným dopadem GDPR



EVA ŠKORNICKOVÁ

Doporučený přístup
k zajištění shody s GDPR

Dopady GDPR se prolínají celou organizací a všemi úrovněmi její činnosti. Změny je vždy nutné vnímat v kontextu produktů, procesů a informačních systémů. GDPR ovlivňuje jak toky informací v podobě afilací (informací sdílených s pobočkami či dceřinými společnostmi), tak i externí toky (např. dodavatelé ICT).



EVA ŠKORNICKOVÁ

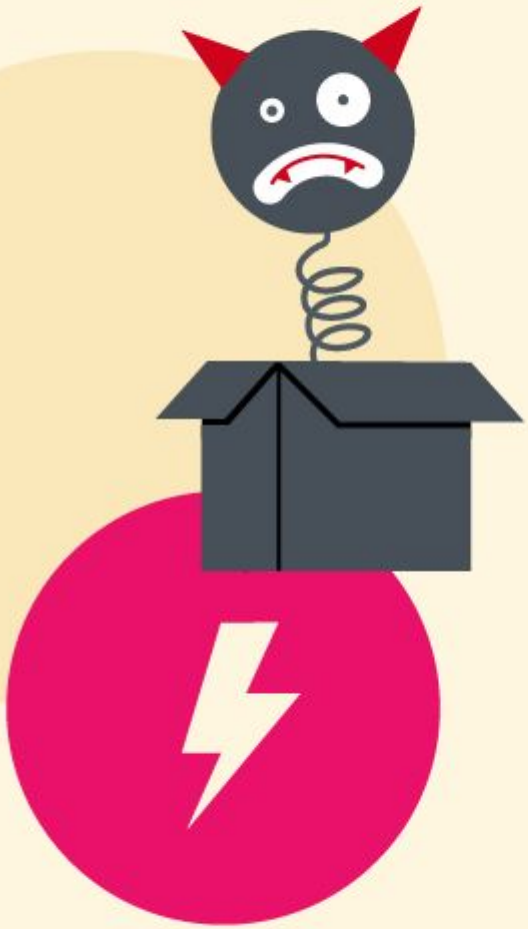
Doporučený přístup
k zajištění shody s GDPR

- Zajištění shody s GDPR proto vyžaduje komplexní přístup. Nabídka služeb v rámci implementace GDPR pravidel se skládá z jednotlivých na sebe navazujících fází. S ohledem na skutečnost, že se aplikace GDPR pravidel dotkne celé organizace jako celku s výrazným dopadem na řadu interních činností a procesů, tak i tato nabídka vychází z nutnosti zapojení týmu expertů, kteří budou aplikaci pravidel nařízení řídit ve spolupráci s vrcholným managementem dané společnosti.

1. Definice rozsahu posuzování
2. Analýza stávajícího stavu zpracování osobních údajů
3. Příprava projektových záměrů a harmonogramu implementace
4. Realizace projektových záměrů

EVA ŠKORNICKOVÁ

Je GDPR strašák
v podobě black boxu?



- V současnosti lze získat informace o dané problematice. Probíhají různé konference a prezentace. Obvykle se jedná o informace, které byly získány z veřejných zdrojů a které teoreticky popisují možná rizika a dopady plynoucí z daného nařízení.

  Vzniká tudíž jakýsi démonizovaný Black Box.

- Díky skutečnosti, že subjekty, které poskytují tyto informace jsou obyvkle jen jednostranně odborně zaměřené, nedokáží poskytnout komplexní informace o skutečném dopadu dané problematiky. Dochází tudíž k podcenění problematiky jako celku.

EVA ŠKORNICKOVÁ

Kdo s problematikou *může pomoci*

Varianta č.1

GDPR SuperExpert

Varianta č.2

Tým expertů GDPR

- Právo
- IT
- Procesy
- Bezpečnost
- Management

Minimální počet oblastí

Ideálním týmem jsou experti disponující průřezově znalostmi a dovednostmi z více než jedné oblasti. Pro jednotlivé oblasti následně zajistit specialisty s kombinací znalostí know-how GDPR.

EVA ŠKORNIČKOVÁ

EVA ŠKORNIČKOVÁ

Nejste v tom sami,
dejte mi vědět!

WWW.GDPR.CZ

+420 602 655 008 | eva@skornickova.eu | www.skornickova.eu