IBM Security

Nařízení (EU) 2016/679 – Obecné Nařízení o ochraně údajů (GDPR)

Daniel Joksch, Michal Meliška

IBM

Agenda

- Stručný úvod problematiky nařízení
- Práva a povinnosti podle GDPR
- Přístup k projektu splnění požadavků GDPR
- Praktická ukázka projektu z oblasti neziskových organizací

GDPR STRUČNĚ

- Vrátit osobní údaje (OÚ) těm, kterým patří!

- Účinné od 25. 5. 2018 (platné od 24. 5. 2016)
  - Přímo závazné × cca 50 oblastí pro národní úpravu
  - Derogace dosavadní právní úpravy (směrnice č. 95/46/ES – DPD)

- Další posilování a precizace práv subjektů OÚ
- Podstatně náročnější administrace zpracování OÚ pro většinu osob a institucí (správci, zpracovatelé)
- Vysoké pokuty
  - Až 2 % celosvětového ročního obratu anebo 10 mil. €
  - Až 4 % celosvětového ročního obratu anebo 20 mil. €

  (při zvlášť závažném porušení povinností)

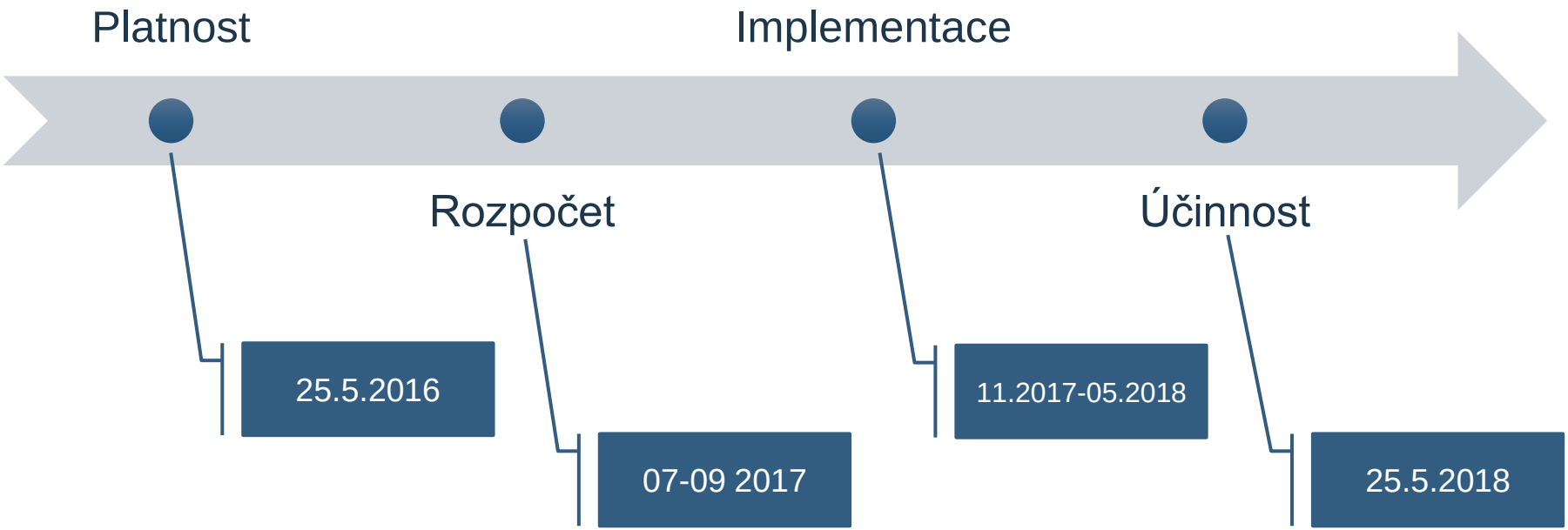
Věcná a místní působnost GDPR

- Všechny formy zpracování
  - Zcela/částečně automatizované
  - Manuální, jsou-li anebo mají-li OÚ být součástí evidence

- Veškeré zpracování OÚ na území EU/EHP, občanů EU a pohyby OÚ v rámci EU/EHP, když:
  - Správce / zpracovatel OÚ sídlí v zemích EU
  - Správce / zpracovatel OÚ nesídlí v zemích EU, ale zpracovává data občanů EU za účelem nabídky zboží, služeb anebo za účelem monitoringu jejich chování na území EU

- Výluky působnosti GDPR
  - Osoby bez ochrany + Právnické osoby × ochrana OÚ zaměstnanců
  - Zpracování OÚ v oblasti ochrany zákonnosti a bezpečnosti
  - Anonymní a anonymizované údaje, (neidentifikující) údaje pro statistické a výzkumné účely

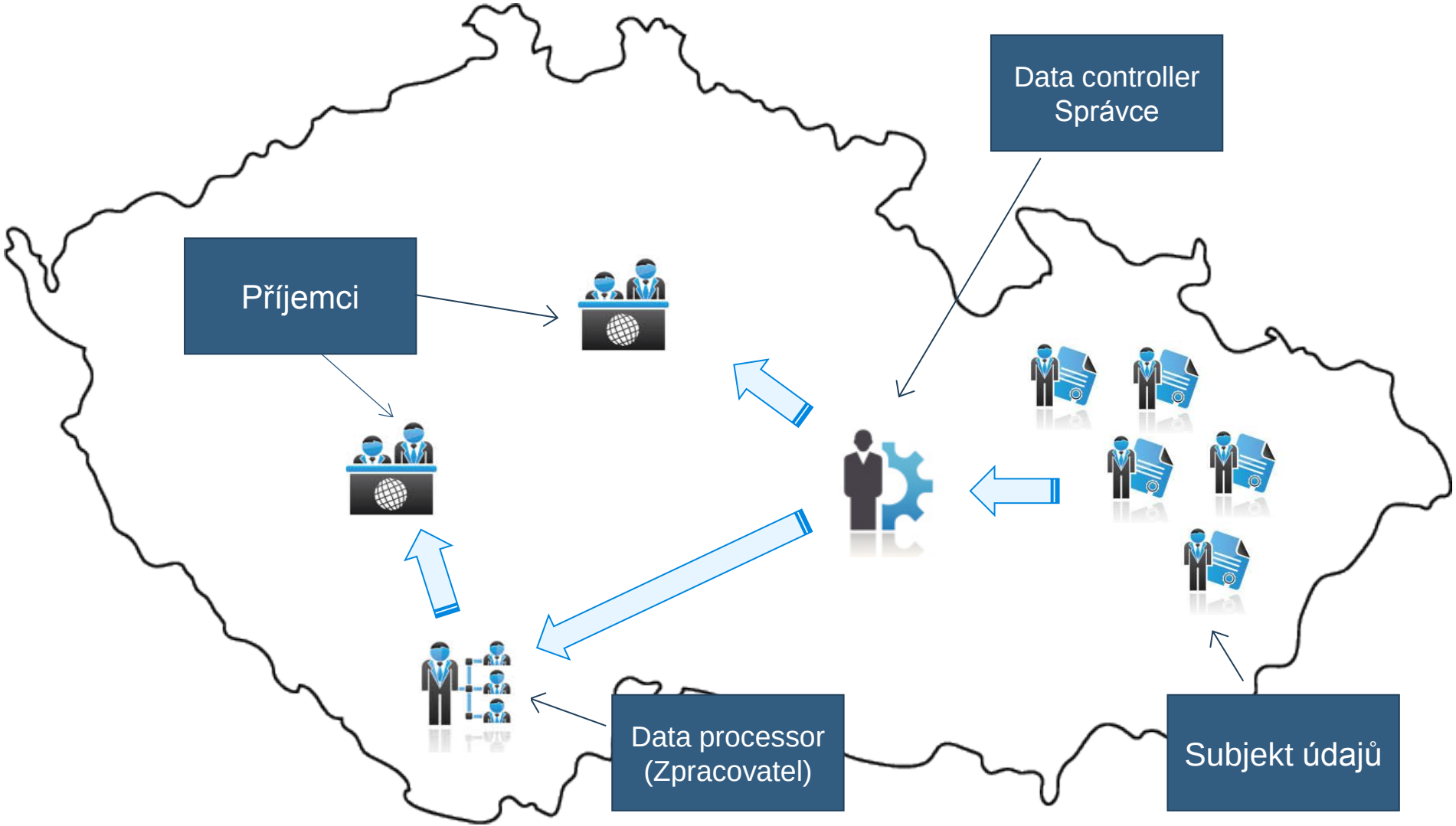
General Data Protection Regulation



- Povinnosti plynoucí z Nařízení
  - analyzovat dopady na současné zpracování údajů
  - stanovit postupy pro jejich realizaci
  - docílit souladu v roce 2018

Požadavky na ochranu informačných aktív v európskej legislatíve

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze 6. července 2016 o opatřeních na zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (The Network and Information Security Directive , dále jen „**NIS“**)
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
  (The General Data Protection Regulation, dále jen „**GDPR“**)
- Směrnice Evropského parlamentu a Rady (EU) 2015/2366 z 25. listopadu 2015 o platebních službách na vnitřním trhu Unie
  (Payment Services Directive 2, dále jen „**PSD2“**)
- Nařízení Evropského parlamentu a Rady (EU) 910/2014 z 23. července 2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu
  (Regulation on Electronic identification and trust services for electronic transactions dále jen „**eIDAS“**)


Data controller
Správce
Příjemci
Data processor
(Zpracovatel)
Subjekt údajů

Nové zásady při ochraně údajů

- **Zásada zákonnosti, korektnosti a transparentnosti**: Osobní údaje musí být zpracovávány korektně a zákonným a transparentním způsobem
- **Zásada omezení účelem**: Osobní údaje musí být shromážděny pro určité, výslovně vyjádřené a legitimní účely
- **Zásada minimalizace údajů**: Osobní údaje nesmí být dále zpracovávány pro účely neslučitelné s původním účelem přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování
- **Zásada přesnosti:** Osobní údaje musí být přesné a v případě potřeby aktualizované; nepřesné údaje opravit nebo vymazat
- **Zásada omezení uložení:** Osobní údaje musí být uloženy ve formě umožňující identifikaci po dobu nezbytnou pro naplnění účelu
- **Zásada zabezpečení zpracování**: Osobní údaje musí být zpracovány způsobem, který zajistí náležité zabezpečení údajů, jejich ochranu pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním, před náhodnou ztrátou, zničením nebo poškozením
- **Zásada odpovědnosti**: Správce odpovídá za dodržení zásad a musí být schopen to doložit

Práva pro subjekty údajů

- **Právo na informace** a přístup k osobním údajům
- **Právo na omezení zpracování**
- **Právo na zapomenutí** (t. j. úplný výmaz osobních údajů)
- **Právo vznést námitku** a právo na opravu nepřesných o.ú., které se subjektu údajů týkají
- Mění se **podmínky vyjádření souhlasu** se zpracováním osobních údajů, který musí být:
  - dotknutou osobou jasně a jednoznačně potvrzený
  - odvolatelný
- **Právo přenášet údaje** k jinému poskytovateli služeb v standardním elektronickém formátu
- Právo dotknuté osoby **dozvědět se o porušení práva** na ochranu osobních údajů
- Nové specifické politiky ochrany osobních údajů - například **ochrana osobních údajů dětí**
- **Omezení profilování -** Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování
- **Posílení práv orgánu dozoru**

Odpovědnosti pro správce (1/2)

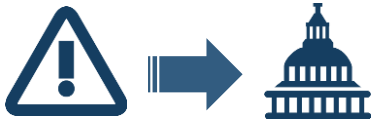
- **Odpovědnost za jakékoliv zpracování osobních údajů** prováděné správcem nebo jeho jménem
- Povinnost doložit, že **zpracování je prováděno v souladu s Nařízením**
- **Přímá odpovědnost správce** (změna důkazného břemena)
- **Výrazné zvýšení horných hraníc pokut** (až 4 % z celkového celosvětového ročného obratu společnosti za předcházející účetní rok, resp. do 20 milionů EUR)
- Povinné zohlednění různě pravděpodobných a různě závažných rizik pro práva a svobody fyzických osob (**risk-based přístup**)
- Povinné **posuzování dopadu na ochranu údajů** (tzv. Data Protection Impact Assessment)
- Povinnost některých správců **vyjmenovat Pověřence pro ochranu osobních** údajů (tzv. Data Protection Officer-a)

Odpovědnosti pro správce (2/2)

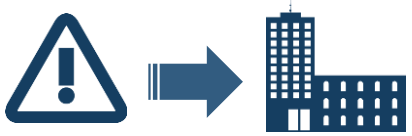
- Povinnost přijmout **vhodná a účinná vhodná technická a organizační opatření** k ochraně údajů
- Povinnost doložit, že:
  - **opatření jsou aplikována v souladu s Nařízením**
  - **opatření jsou podle potřeby revidována a aktualizována**
- Povinná **záměrná ochrana údajů** již ve fázi návrhu (tzv. „Privacy by Design“)
- Povinné **standardní nastavení ochrany údajů** (tzv. „Privacy By Default“)
- Povinné ohlašování případů narušení bezpečnosti (**notifikační povinnost**)
- Nové **pravidla přeshraničního přenosu** osobních údajů
- Dodržování schválených **Kodexů chování** (Code of Conduct)

Ohlašování případů porušení zabezpečení osobních údajů

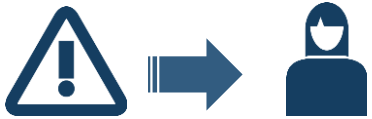
- Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí **dozorovému úřadu** příslušnému, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.



- **Zpracovatel** je povinen informovat **správce** o porušení zabezpečení osobních údajů okamžitě poté, co bylo porušení zjištěno, a na tuto skutečnost jej upozornit



- Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu **subjektu údajů**.



Podrobnosti nových zásad při ochraně údajů

CO JSOU „vhodná technická a organizační opatření“…?

- Ochranná (bezpečnostní) opatření:
  - Jsou **praktiky, procedury a mechanismy,** které mohou pomoci chránit před nějakou hrozbou, snížit zranitelnost, omezit vliv nechtěné události, odhalit nechtěnou událost a umožnit zotavení nebo odškodnění.
  - Jejich přijetím je:
    - **neoprávněným osobám** znemožněn nedovolený přístup k osobním údajům, manipulace s technickými zařízeními určenými pro zpracování osobních údajů a manipulace s nosiči osobních údajů
    - **oprávněným osobám** zajištěn přístup k osobním údajům v rozsahu nezbytném pro plnění jejich povinností
  - Generické dělení opatření:
    - **Technická** – opatření na snížení bezpečnostních rizik pomocí prostředků fyzické a technologické povahy
    - **Organizační** - opatření na snížení bezpečnostních rizik pomocí změn procesů a úpravou dokumentace
  - Dosažení efektivní bezpečnosti obvykle vyžaduje **kombinaci** různých opatření

Přístup k hodnocení identifikovaných rizik

Metodiky použité pro úvodní hodnocení rizik

- LINDDUN – privacy threat modeling
- ISO27001/2013

Matice pro stanovení úrovně rizika

Pravděpodobnost hrozby	**Dopad**				
	Zanedbatelný (20)	Malý (40)	Střední (60)	Značný (80)	Katastrofický (100)
Vysoká (1)	20*1,0=20	40*1,0=40	60*1,0=60	80*1,0=80	100*1,0=100
Střední (0,7)	20*0,7=14	40*0,7=28	60*0,7=42	80*0,7=56	100*0,7=70
Malá (0,4)	20*0,4=8	40*0,4=16	60*0,4=24	80*0,4=32	100*0,4=40
Velmi malá (0,2)	20*0,2=4	40*0,2=8	60*0,2=12	80*0,2=16	100*0,2=20

Návrh opatření v závislosti na stanovené úrovni rizika

Úroveň rizika	Opatření
Extrémně vysoké	Nápravná opatření jsou bezpodmínečně nutná a je nutné přijmout je bezodkladně. Je vhodné zvážit i možnost odstavení systému.
Velmi vysoké	
Vysoké	
Střední	Nápravná opatření jsou potřebná a měla by být přijata v dohledné době. Systém nemusí být odstaven a může být i nadále provozován.
Malé	Vlastník aktiva musí stanovit, zda je nutné přijímat nápravná opatření, anebo v minulosti přijatá protiopatření jsou nadále potřebná. Případně je možné akceptovat riziko jako inherentní.
Zanedbatelné	Není nutné přijímat nápravná opatření

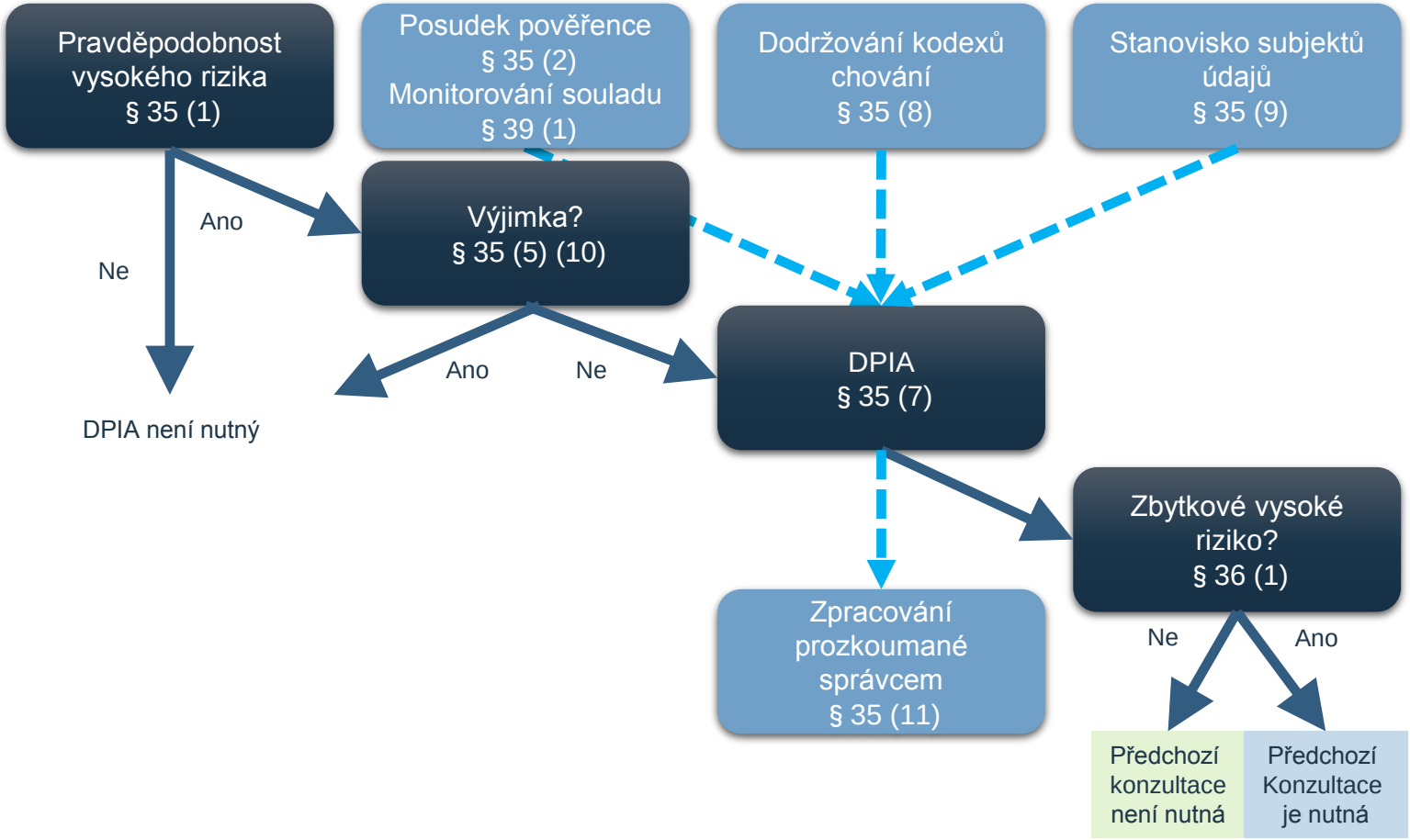
Zbytkové riziko

- **Zbytkové riziko** je takové riziko, jehož hodnota po komplexním ošetření rizik implementací původních, dodatečných a vylepšených opatření na ošetření rizika je tak nízká (tj. **nepřekračuje referenční úroveň**), že je pro organizaci přijatelné a **není nutné uplatnit další opatření** k jeho snížení.
- Referenční hodnota zbytkového rizika by měla být stanovena na takové úrovni, aby **dopad hrozby byl tak nízký, že ho bude možné zanedbat**.
- GDPR (Článek 36) vyžaduje tzv. předchozí konzultaci rizik (zatím není známo, jaká bude kompetence ÚOOÚ v řízení rizik…)
- Zbytkové riziko musí být vždy zásadně akceptováno vedením organizace

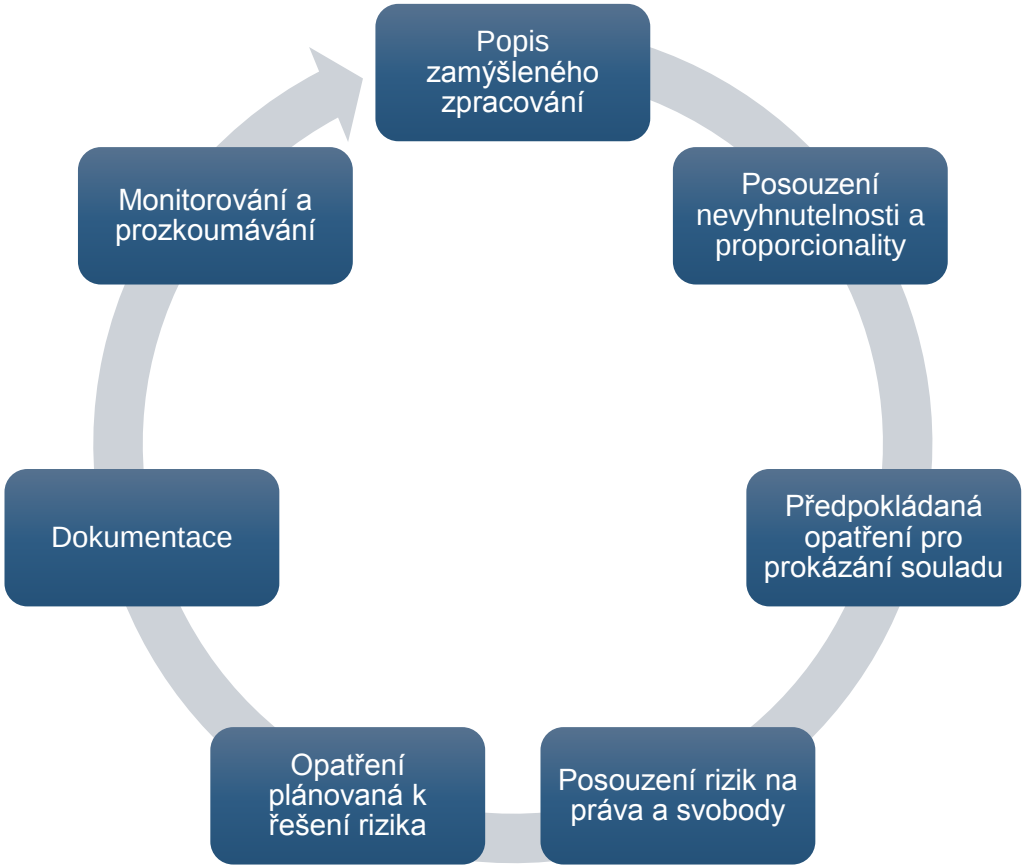
Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)

- Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.
  - Kdy se musí DPIA provádět?
    - při změnách legislativních opatření
    - při jakýchkoliv změnách v zpracování osobních dat
    - pokud je pravděpodobné, že zpracování (zejména využitím nových technologií), bude představovat vysoké riziko pro práva a svobody jedince
  - Např.:
    - před zavedením nových IT systémů na zpracování dat
    - před významnými změnami ve zpracování údajů:
      - při stanovení nového účelu zpracování údajů
      - při novém způsobu či prostředcích zpracování údajů
      - při jakýchkoliv změnách dosavadního modelu zpracování údajů

PRINCIPY výkonu DPIA PODLE WP29

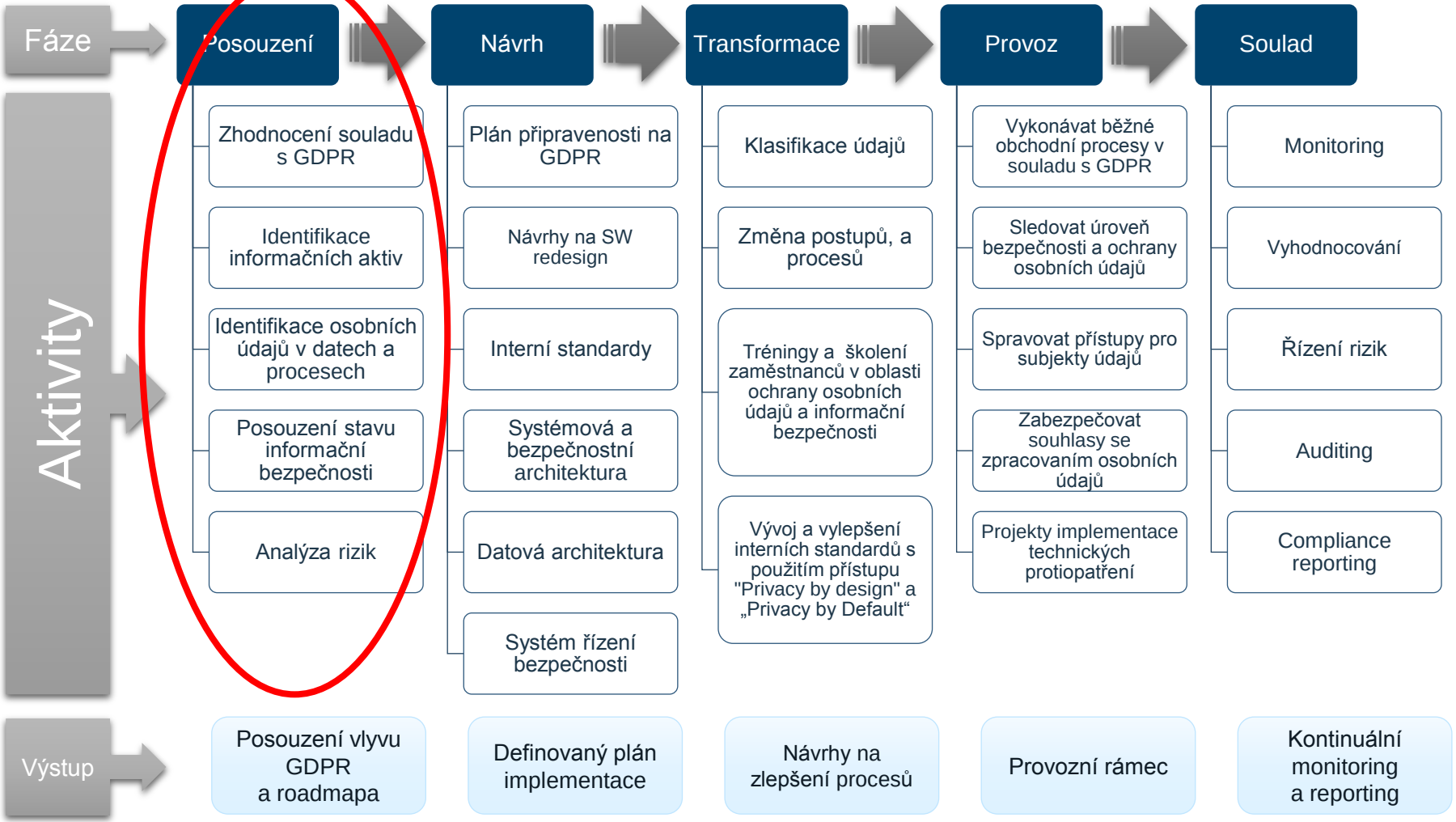


Generický PROCES DPIA PODLE WP29



Implementace požadavků GDPR

GDPR Framework: 5 fáz připravenosti



Dimenze hodnocení připravenosti na požadavky GDPR

Náš přístup

Analýza souladu

- Porovnání současného stavu prostředí společnosti a vyhodnocení souladu s GDPR
- Rozdílová analýza souladu s požadavky GDPR

Identifikace informačních aktiv

- Identifikace současných procesů, které se mohou vázat na GDPR
- Seznam informačních aktiv souvisejících se zpracovatelskými operacemi
- Přehled identifikovaných informačních systémů v kontextu zpracování osobních údajů
- Zhodnocení vyspělosti procesů

Identifikace osobních údajů

- Identifikace datových toků
- Seznam osobních údajů a klasifikovatelných atributů v datech a procesech
- Přehled identifikovaných kategorií subjektů osobních údajů

Posouzení stavu ISMS

- Posouzení úrovně řízení bezpečnosti
- Posouzení stávajících bezpečnostních opatření

Analýza hrozeb a rizik

- Identifikace zranitelností
- Posouzení hrozeb
- Kvantifikace rizik

Příklad interpretace analýzy připravenosti na požadavky GDPR

Klíčové domény pro zajištění vyšší míry připravenosti na požadavky GDPR

a) DPO, komunikace a vzdělávání
   - Potřeba zavedení pozice DPO
   - Pravidelná školení zaměstnanců
   - Vytvoření jednotného komunikačního místa (včetně směrem k dozorovému orgánu)

b) IT, bezpečnost a ochrana dat
   - Bezpečnostní politiky / směrnice
   - Procesy a nástroje pro řešení bezpečnostních incidentů
   - Centralizace správy toku dat (včetně třetích stran a správy aplikací)

c) Řízení rizik v oblasti správy dat

d) Směrnice, správa dat a řízení životního cyklu informací
   - Formalizace / standardizace komunikačních postupů včetně třetích stran
   - Katalogizace dat a ucelené postupy pro nakládání s osobními údaji (včetně vykonatelnosti opatření, např. výmazy)
   - Nastavení rolí a odpovědností v oblasti správy dat / osobních údajů

IBM Security

THANK YOU

FOLLOW US ON:

 ibm.com/security

 securityintelligence.com

 xforce.ibmcloud.com

 @ibmsecurity

 youtube/user/ibmsecuritysolutions

 ivan.makatura@sk.ibm.com

IBM