

Zvyšování připravenosti na požadavky GDPR - doporučení a návrh opatření k rozpracování

Asociace komunitních služeb v oblasti péče o duševní zdraví
Fokus Praha, z. ú.



IBM Česká republika, spol. s r.o. – Security and Global Business Services

Daniel Joksch, Peter Gardlík, Michal Meliška





Agenda

- Přístup k analýze a hodnocení připravenosti na požadavky GDPR
- Shrnutí výsledků hodnocení připravenosti
- Identifikovaná rizika s vysokou úrovní
- Doporučení a návrh opatření k dalšímu rozpracování
- Diskuse - otázky a odpovědi

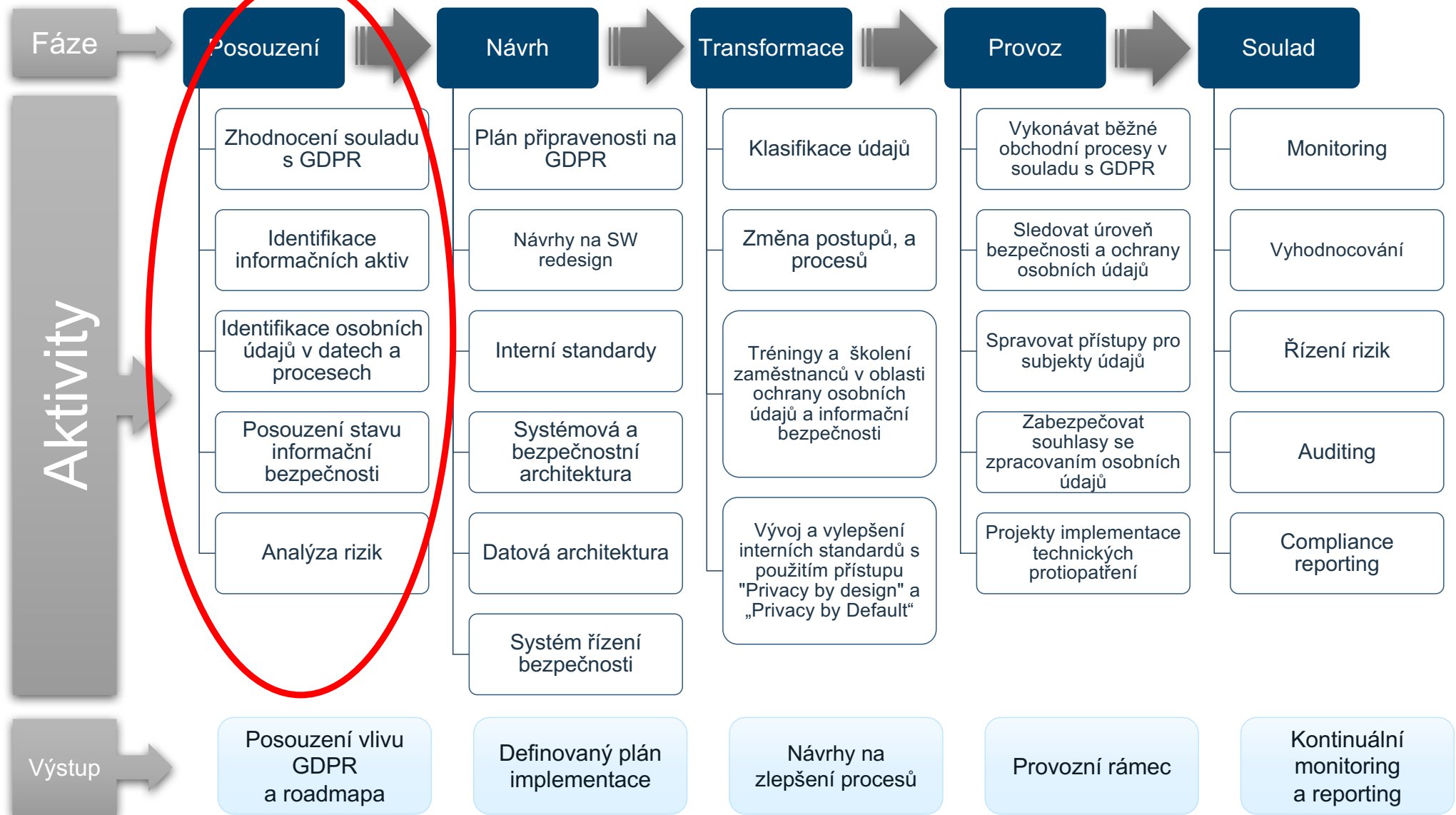
Průběžný stav projektu

- ✓ **1. Kick-off workshop a edukace organizace**
- ✓ **2. Shromáždění informací relevantních k projektu**
 - Dokumentace (bezpečnostní, procesní dokumentace, organizační struktura)
 - Identifikace klíčových vlastníků problematiky
 - V případě, že některé oblasti nebudou dosud zpracovány v dokumentacích, v průběhu projektu se potřebné informace nasbírají v rámci on-site části od účastníků projektu
- ✓ **3. Vyplnění dotazníků a interview**
 - S organizací budou nasdíleny dotazníky k vyplnění, otázky, které nedokáže organizace vyplnit budou doplněny v průběhu interview
 - Interview budou probíha pro ucelení kompletního obrazu fungování organizace a pomohou v následujících částech projektu
- ✓ **4. Off-site příprava srovnávací analýzy**
 - Identifikace oblastí, kde organizace není v souladu s GDPR a vytvoření grafického znázornění úrovně souladu organizace
- ✓ **5. Prezentace výsledků srovnávací analýzy**

Plán dalších aktivit projektu

- ✓ **6. Identifikace informačních aktiv**
 - Popsání výskytů osobních údajů v aktivech a procesech organizace a zjištění účelu jejich používání
- ✓ **7. Revize stavu informační bezpečnosti**
 - Zhodnocení stavu kybernetické bezpečnosti, předávání osobních údajů třetím stranám, stručná revize fyzické bezpečnosti u údajů vyskytujících se pouze ve fyzické podobě
- ✓ **8. Analýza rizik**
 - Vytvoření matice řízení rizik a identifikace nejrizikovějších oblastí zpracování osobních údajů
- ✓ **9. Doporučení a návrh opatření k dalšímu rozpracování s ohledem na připravenost a požadavky GDPR**
 - Série doporučení vycházející z předchozích bodů analýzy. Tato doporučení by měla být konkrétní a poskytnout organizaci prioritizovaný seznam projektů a doporučení s ohledem na požadavky Nařízení
- 10. Prezentace výstupů projektu a doporučení**

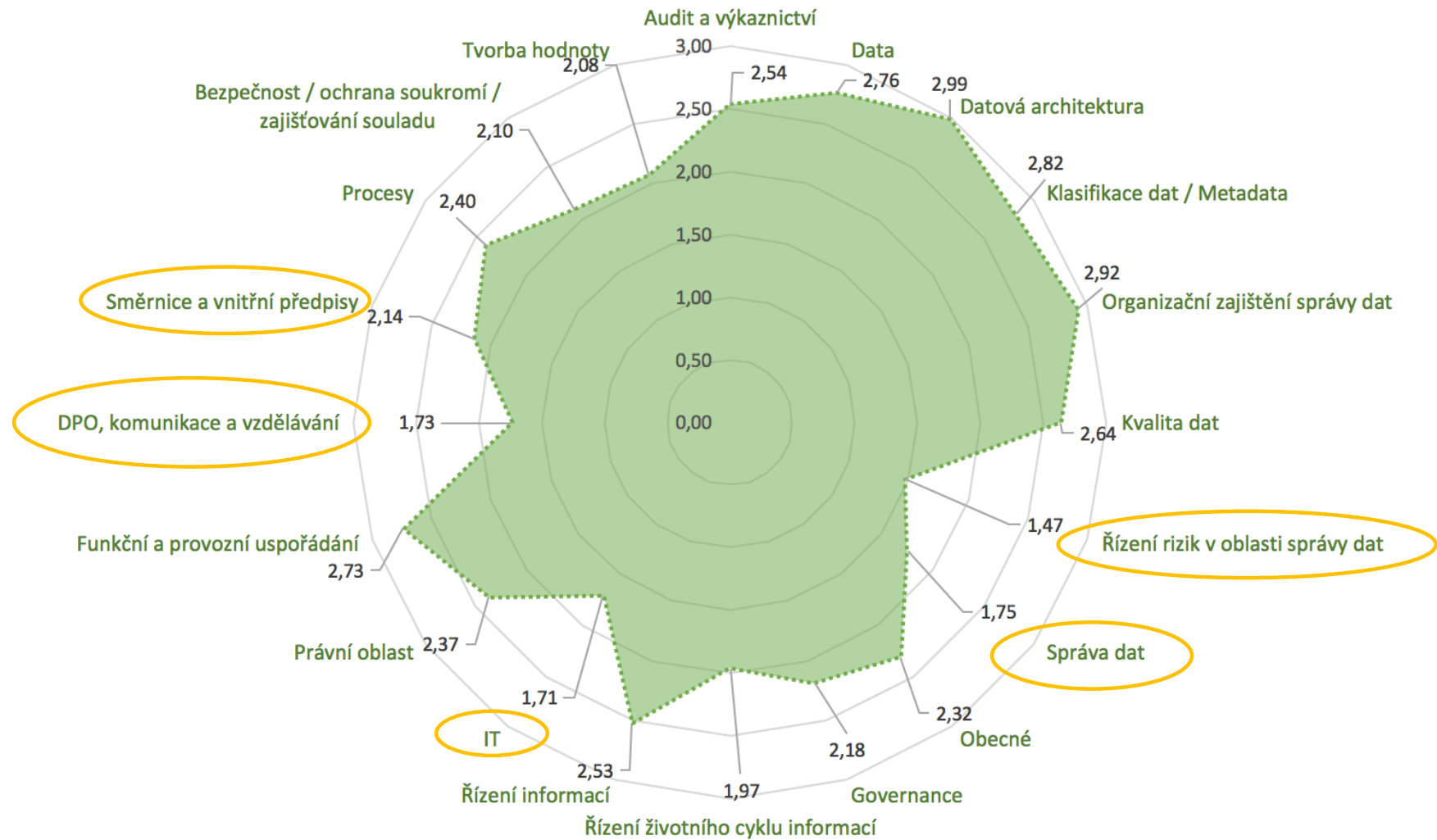
Přístup k hodnocení připravenosti na požadavky GDPR



Dimenze hodnocení připravenosti na požadavky GDPR



Výsledky hodnocení připravenosti na GDPR a oblasti dopadů



"DŮVĚRNÉ"


Komentář k výsledkům 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

Doporučení a návrhy opatření ve vazbě na analýzu rizik

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. System 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



Identifikovaná rizika s vysokou úrovní – přehled v tabulce (viz Excel)

Metodiky použité pro úvodní hodnocení rizik

- LINDDUN – privacy threat modeling
- ISO27001/2013



Doporučená opatření k vybraným rizikům - Excel



Otázky & Odpovědi





IBM's commitment to GDPR readiness

- IBM is committed to providing our clients and partners with innovative data privacy, security and governance solutions to assist them on their journey to GDPR compliance.
- Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey at ibm.com/gdpr



Děkujeme

FOLLOW US ON:



ibm.com/security



securityintelligence.com



xforce.ibmcloud.com



[@ibmsecurity](https://twitter.com/ibmsecurity)



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

