IBM Security

Analýza a hodnocení připravenosti na požadavky GDPR

ASOCIACE KOMUNITNÍCH SLUŽEB V OBLASTI PÉČE O DUŠEVNÍ ZDRAVÍ
FOKUS – PRAHA, O. S.

IBM Česká republika, spol. s r.o. – Security and Global Business Services
Kristina Kosatíková, Daniel Joksch, Michal Meliška

IBM

AGENDA

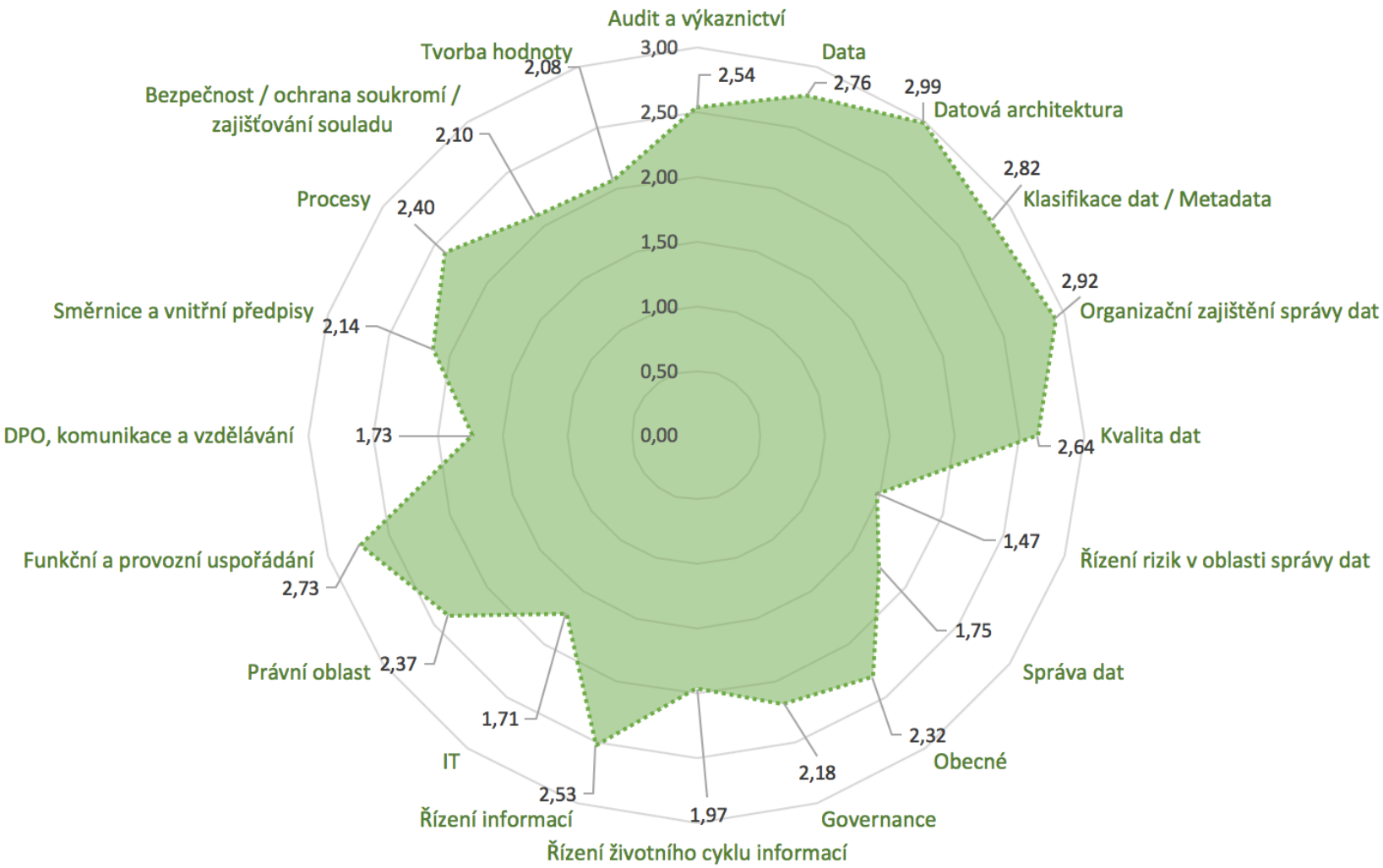
- Shrnutí hodnocení připravenosti na požadavky GDPR
- Zpráva o průběhu projektu a plán aktivit na další období
- Otázky a odpovědi

Analýza dotazníků a hodnocení připravenosti na GDPR

Doména	Externí 1	Externí 2	Klient 1	Klient 2	Klient 3	Klient 4	Klient 5	Klient 6	Průměrné hodnocení
Typ	Tech	Tech	Bus	Bus	Bus	Bus	Bus	Tech	
Audit a výkaznictví	2,60	2,20	2,60	2,40	2,40	2,75	2,80	0,00	2,54
Data	2,29	2,38	3,17	3,00	2,81	2,91	2,79	0,00	2,76
Datová architektura	2,20	2,40	0,00	2,60	3,75	3,00	4,00	0,00	2,99
Klasifikace dat / Metadata	1,67	2,17	0,00	2,40	3,00	3,20	4,50	0,00	2,82
Organizační zajištění správy dat	2,20	2,80	0,00	3,50	3,25	2,50	3,25	0,00	2,92
Kvalita dat	2,17	2,33	0,00	2,67	2,67	3,00	3,42	2,25	2,64
Řízení rizik v oblasti správy dat	1,60	1,40	0,00	1,60	1,20	0,00	1,80	1,20	1,47
Správa dat	1,33	1,83	0,00	2,17	2,10	0,00	1,67	1,42	1,75
Obecné	2,40	2,40	0,00	2,50	3,00	0,00	2,00	1,60	2,32
Governance	1,67	2,15	0,00	2,62	2,08	0,00	2,50	2,08	2,18
Řízení životního cyklu informací	1,80	1,80	0,00	3,00	2,00	0,00	2,20	1,00	1,97
Řízení informací	1,25	3,00	0,00	2,33	2,75	0,00	3,50	2,33	2,53
IT	1,00	2,00	0,00	0,00	2,33	0,00	0,00	1,50	1,71
Právní oblast	1,75	2,50	0,00	0,00	2,00	0,00	4,25	1,33	2,37
Funkční a provozní uspořádání	1,00	2,75	0,00	0,00	3,67	0,00	3,50	2,75	2,73
DPO, komunikace a vzdělávání	1,33	1,67	0,00	0,00	1,33	0,00	2,33	2,00	1,73
Směrnice a vnitřní předpisy	1,60	1,80	0,00	0,00	2,40	0,00	2,70	2,20	2,14
Procesy	2,00	2,50	0,00	0,00	2,50	0,00	2,50	2,50	2,40
Bezpečnost / ochrana soukromí / zajišťování souladu	1,58	1,89	0,00	0,00	2,28	0,00	2,90	1,84	2,10
Tvorba hodnoty	1,6	2,3	0,0	0,0	2,7	0,0	1,9	2,0	2,08
								Celkem	**2,31**

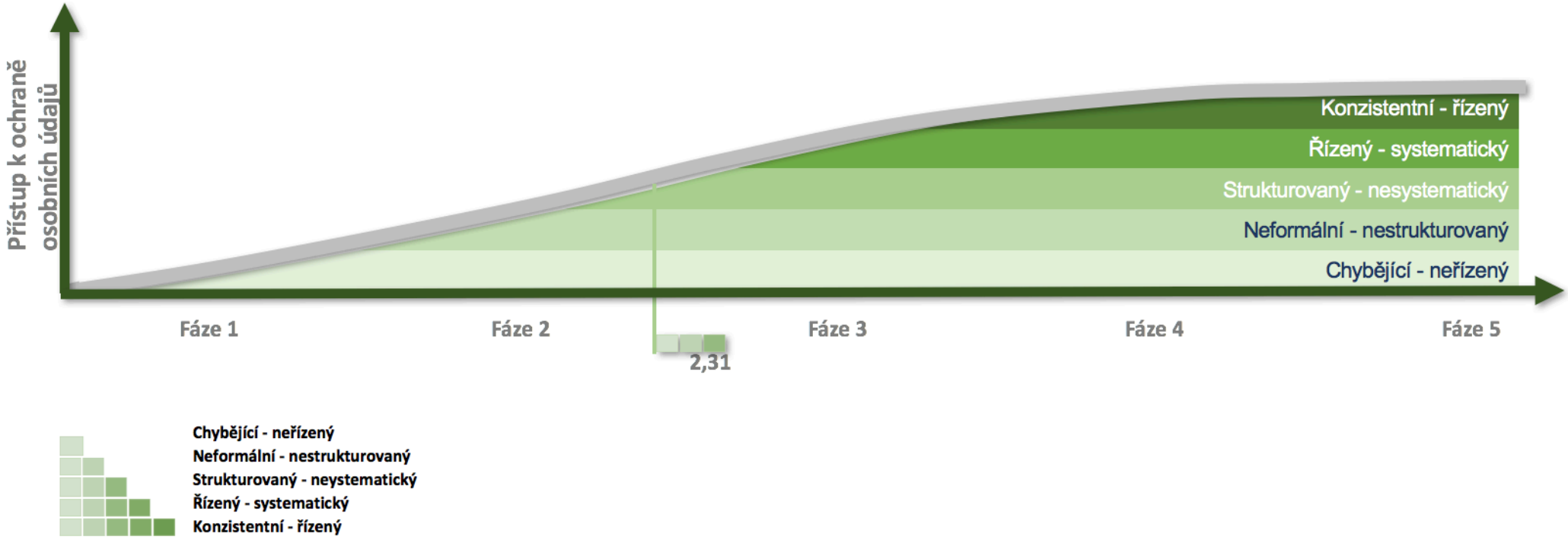
"DŮVĚRNÉ"

Shrnutí hodnocení připravenosti na GDPR



"DŮVĚRNÉ"

Hodnocení přístupu k ochraně osobních údajů



"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

Zpráva o průběhu projektu plán dalších aktivit

- **Cíle projektu**

a) Provedení analýzy připravenosti na požadavky GDPR ve vybrané organizaci Asociace a zhodocení dopadů na stávající postupy a způsob nakládání s osobními údaji a daty;
b) Identifikace rizik a posouzení stavu informační bezpečnosti;
c) Doporučení a návrh opatření k dalšímu rozpracování s ohledem na připravenost a požadavky GDPR.

- **Zpětná vazba**
  a) Dotazníky;
  b) Interviews;
  c) Organizace.

Realizované aktivity projektu

1. **Kick-off workshop a edukace organizace**

2. **Shromáždění informací relevatních 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

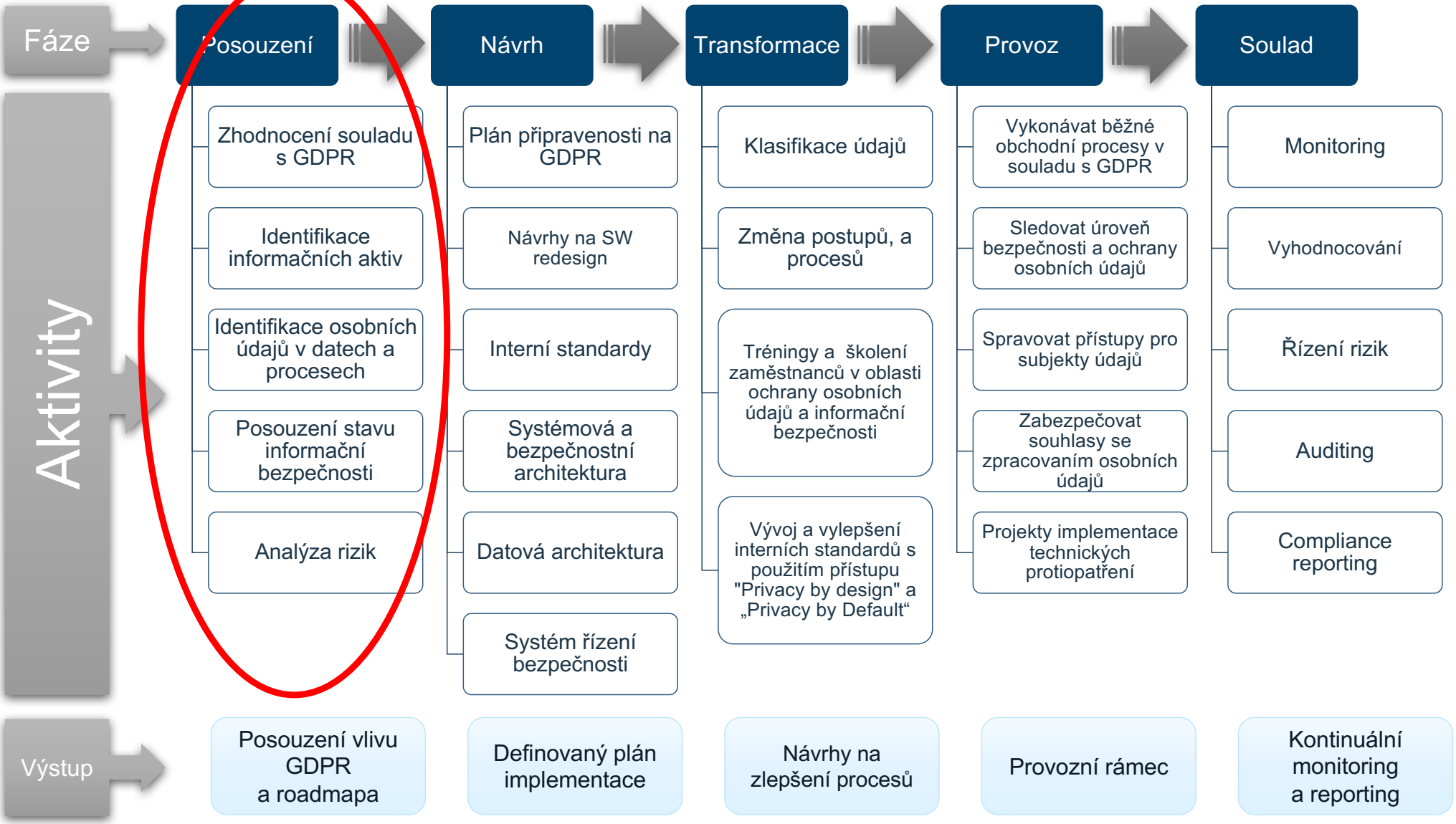
4. **Off-site příprava srovnávací analýzy**
   - Identifikace oblastí, kde organizace není v souladu s GDPR a vytvoření grafického znázornění úrovně souladu organizace

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 vysktytujících 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**

GDPR Framework: 5 fází připravenosti



Další očekávaná součinnost

- **Identifikace informačních aktiv a analýza bezečnosti**
  - Vedení Focus
  - Provoz, ekonomika a personální agendy
  - IT
  - CDZ
- **Forma**
  - Strukturované interview (v návaznosti na doporučení ISO27001)
- **Časový odhad**
  - **CDZ** – cca 5 - 6 hodin (včetně Analýzy připravenosti)
  - Ostatní - 3 hodiny

otázky
&
odpovědi

Děkujeme a těšíme se na

další spolupráci

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**