SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NOVINKY V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ

WORKSHOP „OCHRANA OSOBNÍCH ÚDAJŮ“
Podnikatelské fórum Ústeckého kraje

6. 6. 2017, Ústí nad Labem

PROGRAM

11:00 – 10:10	**ZAHÁJENÍ A ÚVOD DO TÉMATU** ***MGR. MILENA JABŮRKOVÁ, MA**, VICEPREZIDENTKA SP ČR PRO DIGITÁLNÍ EKONOMIKU A VZDĚLÁVÁNÍ A PŘEDSEDKYNĚ PRACOVNÍ SKUPINY SP ČR PRO OCHRANU DAT*
10:10 – 11:30	**NOVINKY V NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ** MODEROVANÁ DISKUZE ***JUDR. JIŘÍ ŽŮREK**, ŘEDITEL ODBORU PRO STYK S VEŘEJNOSTÍ, ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ* ***ING. TOMÁŠ KNÍŽEK**, FOUNDER & CEO, DIGITAL CITY, A. S.* ***MGR. MILENA JABŮRKOVÁ, MA**, VICEPREZIDENTKA SP ČR*
11:30 – 12:30	**POVINNOSTI FIREM A PRÁVA SUBJEKTŮ ÚDAJŮ VYPLÝVAJÍCÍ Z NAŘÍZENÍ A JEJICH DOPAD V PRAXI** MODEROVANÁ DISKUZE (J. ŽŮREK, T. KNÍŽEK, M. JABŮRKOVÁ)

GENERAL DATA PROTECTION REGULATION

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 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/GDPR**)

Platnost: 25. 5. 2016 Účinnost: 25. 5. 2018

- Nařízení stanovuje sankce v případě porušení:
  - až 20 mil. EUR nebo
  - 4% ze světového obratu společnosti za předchozí fiskální rok (podle toho, co je vyšší)

Nový přístup k ochraně osobních údajů v EU

NAŘÍEZNÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ V EU

- **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 klientů (správci, zpracovatelé)
- Vysoké pokuty
  - Až 4 % celosvětového ročního obratu anebo 20 mil. €

LEGISLATIVNÍ RÁMEC

- Nařízení č. 2016/679 – Všeobecné nařízení o ochraně OÚ (GDPR)
  - Směrnice č. 2016/680 (směrnice GDPR)
  - Směrnice č. 2016/681 (směrnice PNRD)

- Výkladová praxe WP 29
  - Vodítko k právu na přenositelnost údajů (WP 242)
  - Vodítko k pověřenci pro ochranu osobních údajů (WP 243)
  - Vodítko k určení vedoucího dozorového úřadu (WP 244)
  - Vodítko k provádění DPIA (WP 248)
  - Průběžná aktualizace

- Zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ)
- Zákon č. 181/2014 Sb., o kybernetické bezpečností

- Výkladová praxe ÚOOÚ

PŘEDMĚT A CÍLE GDPR

- GDPR dopadne na všechny případy zpracování OÚ občanů EU a pohybů OÚ v rámci EU, kdy:
  - Správce/zpracovatel sídlí v zemích EU
  - Správce/zpracovatel nesídlí v zemích EU, ale zpracovává data občanů EU za účelem nabídky zboží, služeb anebo za účelem monitoringu jejich chování

- Všechny formy zpracování
  - Zcela/částečně automatizované i manuální (neautomatizované)

- Výluky
  - Anonymizované údaje
  - Statistické a výzkumné účely

Zásady pro práci s osobními údaji vyplývající z GDPR

OSOBNÍ ÚDAJE

- **Čl. 4 a 9 GDPR**

- **Osobní údaje × Identifikátory**
  - „veškeré informace o identifikované nebo identifikovatelné fyzické osobě“
  - „jméno, identifikační číslo, lokační údaje, síťový identifikátor anebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“

- **Zvláštní kategorie osobních údajů**
  - Osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod fyzických osob
  - Rasový či etnický původ
  - Genetické údaje
  - Biometrické údaje (za účelem jedinečné identifikace fyzické osoby)
  - Údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci
  - Politické názory, náboženské vyznání, filozofické přesvědčení
  - Členství v odborech

ZÁKONNOST ZPRACOVÁNÍ

- Nastává splněním a nejméně 1 z podmínek:
  - subjekt údajů udělil souhlas
  - zpracování je nezbytné pro:
    - → plnění smlouvy
    - → splnění právní povinnosti správce
    - → ochranu životně důležitých zájmů s.ú.
    - → splnění úkolu prováděného ve veřejném zájmu
    - → uskutečnění oprávněných zájmů správce

Hlavní práva subjektů údajů

PRÁVA SUBJEKTŮ ÚDAJŮ

- Čl. 13, 15, 17 GDPR
  - Rozšíření stávajícího katalogu práv subjektů OÚ odpovídající povinnosti správce
- Na informace o zpracování OÚ
- Na přístup subjektu k OÚ
- Získat od správce OÚ potvrzení o zpracování OÚ
- Poskytnout kopii zpracovávaných OÚ
- Na vyžádaný výmaz jeho OÚ („právo být zapomenut“)
  - již dříve dovozeno judikaturou, povinnost bez zbytečného odkladu vymazat OÚ subjektu a nesmí je dále zpracovávat
- Vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů
- Nebýt předmětem automatizovaného rozhodnutí

Povinnosti správců a zpracovatelů údajů

POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ

- **Vést záznamy o činnostech zpracování**
  - Písemné, dostupné na vyžádání dozorovému úřadu
  - Výjimka pro MSP
- **Zajistit odpovídající zabezpečení OÚ**
  - Přijmout vnitřní koncepce a opatření pro zabezpečené zpracování OÚ
  - Zásady záměrné a standardní ochrany osobních údajů
  - Neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb
  - Pravidelné testování, posuzování a hodnocení bezpečnosti opatření
- **Ohlašovat bezpečnostní incidenty (data breaches)**
  - Nejpozději do 72 hodin dozorovému orgánu
  - V případě závažného úniku i subjektům OÚ
- **Provést posouzení vlivu na ochranu OÚ (DPIA) a předchozí konzultace**
  - Posoudit vliv konkrétních operací při zpracování OÚ, které představují vysoké riziko pro práva a svobody FO před zahájením upracování
  - Předběžné konzultace s dozorovým orgánem

JMENOVAT POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

- **Čl. 37 a násl. GDPR**
- **Kdo musí jmenovat svého pověřence**
  - Každý orgán veřejné moci nebo veřejný subjekt s výjimkou soudů v rámci své soudní pravomoci
  - Subjekty provádějící v rámci svých hlavních činností
    → rozsáhlé pravidelné a systematické monitorování subjektů OÚ
    → rozsáhlé zpracování OÚ zvláštní kategorie a údajů týkajících se rozsudků ve věcech trestních
  - Ten, po němž to bude vyžadovat právo EU anebo právo členského státu
- **DPO v kontextu organizace**
  - Materiální zdroje
  - Časová disponibilita
  - Odpovídající kompetence
  - Přístup k informacím, databázím, procesům ad.

ÚKOLY POVĚŘENCE

- **Správce nebo zpracovatel svěří DPO tyto úkoly:**
  - poskytování informací a poradenství všem zaměstnancům zpracovávajícím osobní údaje (jejich povinností)
  - monitorování souladu s politikami správce nebo zpracovatele, zvyšování informovanosti a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů
  - poskytování poradenství o posouzení dopadu na ochranu údajů
  - spolupráce s orgánem dozoru
  - kontakt pro orgán dozoru

- **DPO bere při plnění svých úkolů ohled na riziko spojené s operacemi zpracování a přihlíží k povaze, rozsahu, kontextu a účelům zpracování**

POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DATA PROTECTION IMPACT ASSESSMENT)

Zpracování údajů může nést rizika z hlediska práv a svobod subjektů údajů, správce nebo zpracovatel posoudí dopad plánovaného zpracování DPIA

Kdy se musí posouzení provádět?

1. při návrhu legislativních opatření
2. při jakýchkoliv změnách zpracování osobních údajů
3. zpracování (nové technologie) může představovat vysoké riziko pro práva a svobody jedince, např.:
   - zavedení nových IT systémů pro zpracování údajů
   - před významnými změnami v systémech pro zpracování údajů, např.

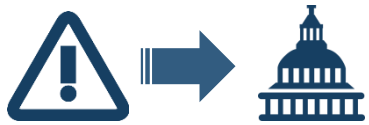
     →nový účel zpracování údajů

     →nový způsob či prostředky zpracování údajů

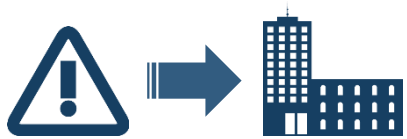
     →změna dosavadního modelu zpracování údajů

OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

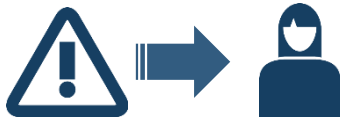
- Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.



- 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.



Ochrana a bezpečnost osobních údajů

BEZPEČNOST

- článek 32
  - Požadavky na šifrování a pseudonymizaci
  - Schopnost zajistit neustálou důvěrnost, dostupnost a odolnost systémů a služeb zpracování
  - Schopnost obnovit dostupnost údajů v případě incidentů
  - Proces pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření
  - Zajistit právo na přenositelnost, přístup a výmaz
  - Ohlašovací povinnost

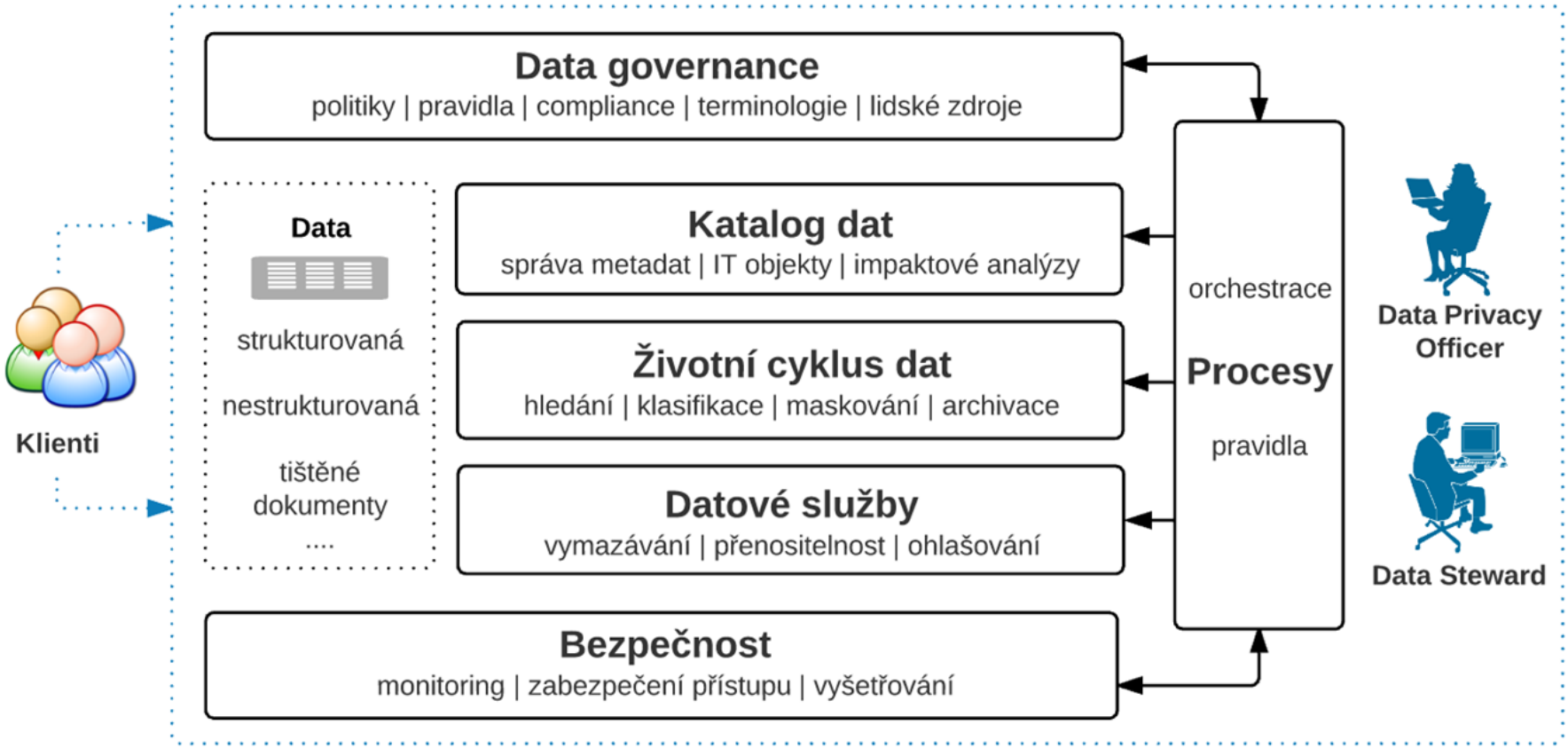
- GDPR zavádí přístup ke zpracování a ochraně osobních údajů založený na riziku

NASTAVENÍ OCHRANY ÚDAJŮ

- Správce a zpracovatel vyhodnotí rizika a přijmou opatření k ochraně o.ú.
  - před náhodným či nepovoleným zničením či ztrátou
  - před nepovolenými formami zpracování (sdělování či šíření o.ú., přístup, pozměnění)

- Správce:
  - standardně zpracovat pouze o.ú. nutné pro konkrétní účel zpracování
  - zajistí, že shromažďování či uchovávání nepřesáhne minimum pro účely nezbytné (množství, rozsahu, doba, dostupnost)
  - zaručí, že se o.ú. nebudou zpřístupňovat neomezenému počtu fyzických osob
  - nastaví ochranu údajů při vývoji a koncipování produktů, služeb a aplikací
  - zohlední právo na ochranu údajů
  - posoudí možnosti současného stavu techniky

LOGICKÝ POHLED NA ŘEŠENÍ POŽADAVKŮ GDPR



GDPR AKADEMIE

GDPR AKADEMIE

- **Vzdělávací program pro firmy zaměřený na implementaci nových evropských pravidel na ochranu osobních dat (GDPR)**
- Série seminářů: červen – prosinec 2016

- Organizátor: Svaz průmyslu a dopravy ČR
- Odborný garant: Úřad pro ochranu osobních údajů
- Odborní lektoři: experti ze společností IBM, KPMG, PRK Partners a Masarykovy univerzity v Brně

- POZVÁNKA: **PRVNÍ SEMINÁŘ 16. června 2017, Praha**
  - **Praktické shrnutí problematiky GDPR pro vrcholové manažery**
  - Registrace ZDE

- Více informací: www.gdprakademie.cz

DĚKUJEME ZA POZORNOST!

Mgr. Milena Jabůrková, MA, Viceprezidentka SP ČR
mjaburkova@spcr.cz

JUDr. Jiří Žůrek, Ředitel odboru pro styk s veřejností, Úřad pro ochranu osobních údajů
Jiri.Zurek@uoou.cz

Ing. Tomáš Knížek, Founder & CEO, Digital City, a. s.
tomas.knizek@digitalcity.cz