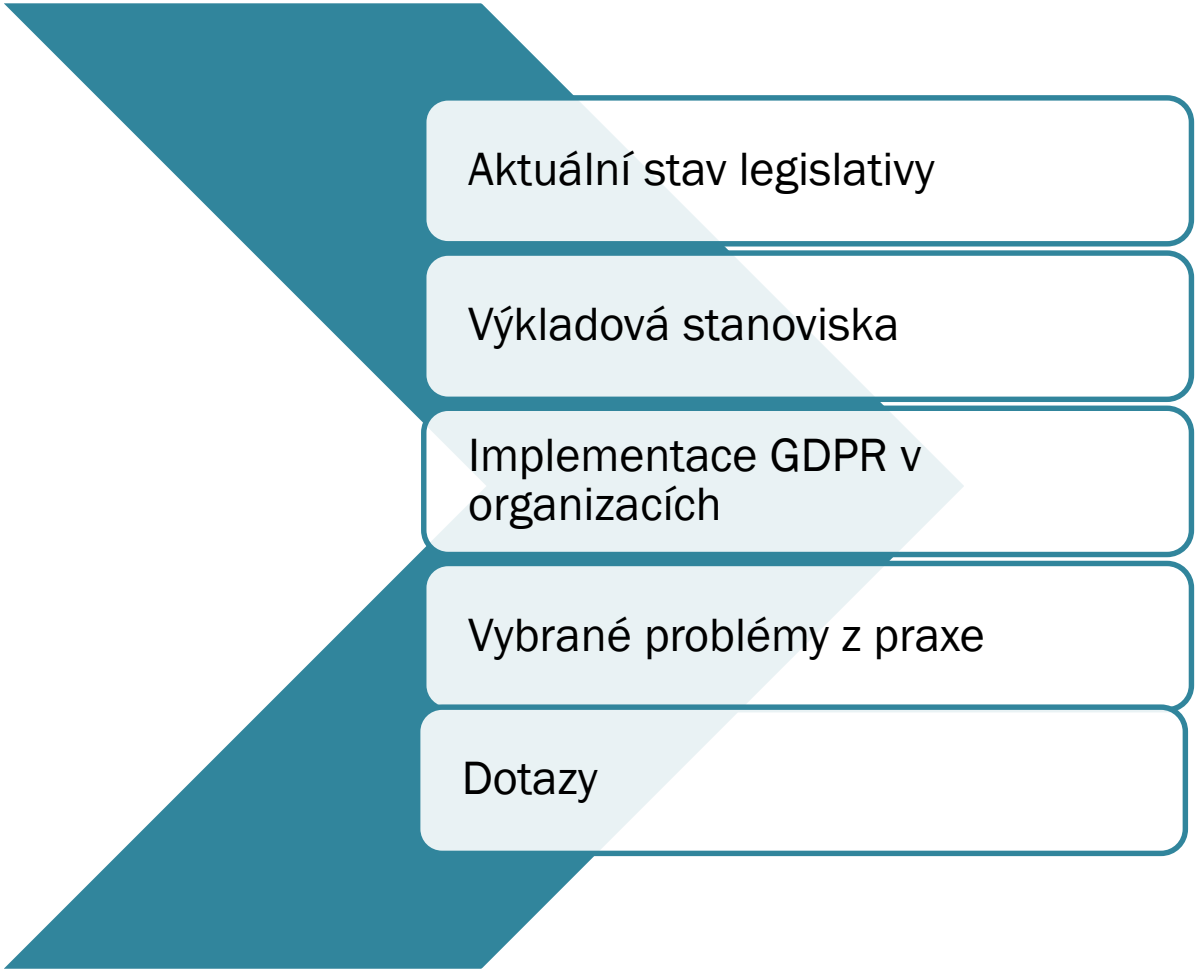
Implementace GDPR – vybrané problémy z praxe

12.4.2018

Mgr. Lenka Suchánková, LL.M.

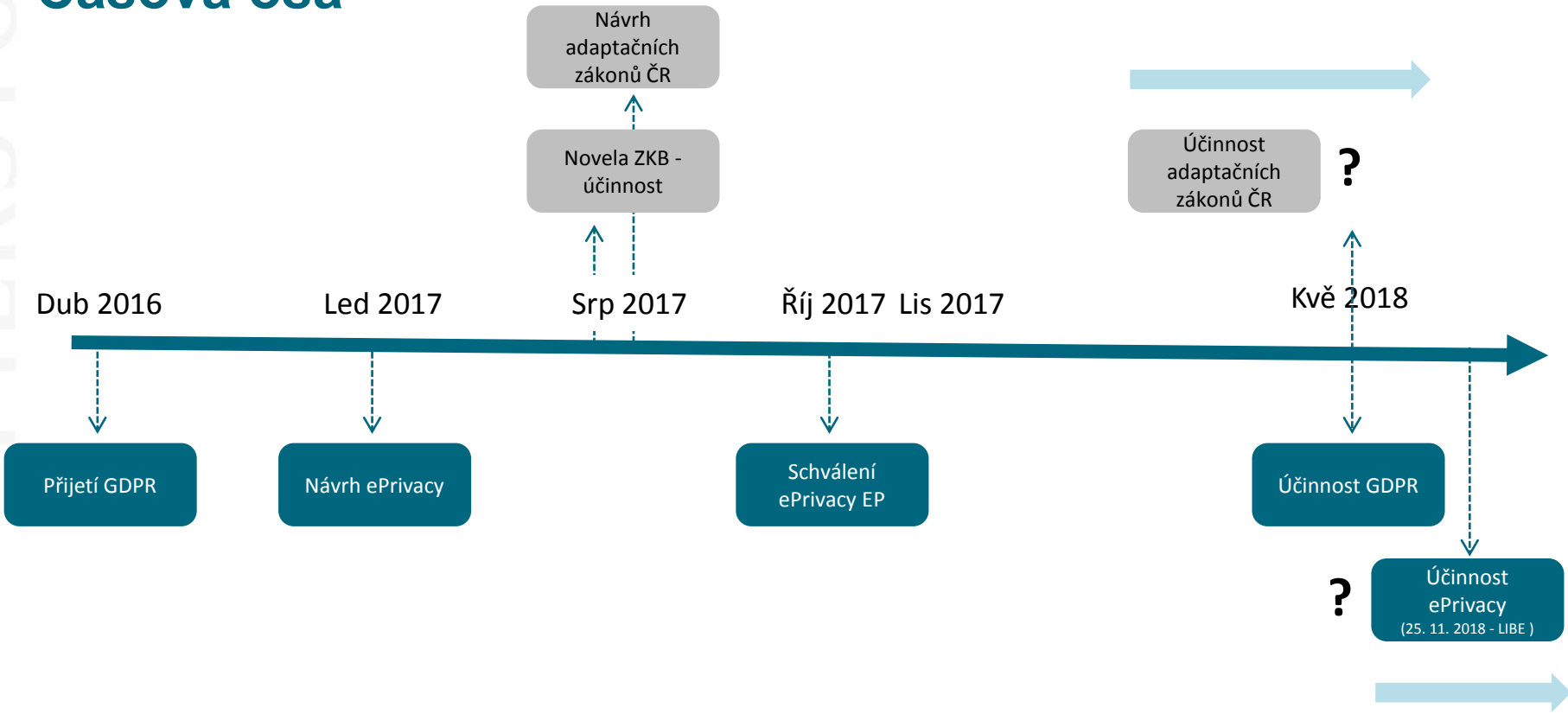
PIERSTONE

Přehled témat



STAV LEGISLATIVY

Časová osa


Návrh adaptačních zákonů ČR
Novela ZKB - účinnost
Účinnost adaptačních zákonů ČR
?
Dub 2016
Led 2017
Srp 2017
Říj 2017
Lis 2017
Kvě 2018
Přijetí GDPR
Návrh ePrivacy
Schválení ePrivacy EP
Účinnost GDPR
?
Účinnost ePrivacy
(25. 11. 2018 - LIBE)

Cílový stav legislativního vývoje (2018)

PRÁVO EU	GDPR	ePrivacy	NIS	Vertikální regulace
ČESKÉ PRÁVO	*Implementační zákon o ochraně osobních údajů*	*Novela ZEK a ZIS*	*Novela zákona o kybernetické bezpečnosti*	Vertikální regulace
Finanční instituce	✓	✓	✓	✓
Telekomunikační operátoři	✓	✓	✓	✓
Poskytovatelé zdr. služeb	✓	✓	✓	✓
Veřejný sektor	✓	✓	✓	✓
Energetika	✓	✓	✓	X
Poskytovatelé cloudu	✓	✓	✓	X
Poskytovatelé služeb	✓	✓	X	X
Výrobní společnosti	✓	✓	X	X
Maloobchodní řetězce	✓	✓	X	X

Související předpisy v České republice

Návrh zákona o zpracování osobních údajů

- Nový zákon nahrazující zákon č. 101/2000 Sb., o ochraně osobních údajů
  - Implementuje i směrnici (EU) 2016/680
  - Nevyužívá derogace, pouze upřesňuje
  - Souhlas mladistvého – min. 15 let
  - DPO – mlčenlivost
  - Definice subjektu veřejné správy
  - Pro veřejné subjekty pokuta „jen“ do 10.000.000 Kč
  - Vymáhání občanskoprávních nároků jako samostatný právní titul

Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů

- Implementace GDPR do ostatních relevantních zákonů
- Zákony, které jsou návrhem měněny (př.):
  - zákon o Policii České republiky;
  - zákon o státním zastupitelství;
  - zákon o Probační a mediační službě;
  - zákon o Rejstříku trestů;
  - zákon o Vězeňské službě a justiční stráži České republiky; zákon o trestním řízení soudním (trestní řád);
  - zákon o soudech a soudcích;
  - zákon o Ústavním soudu;
  - občanský soudní řád;
  - daňový řád;
  - zákon o Finanční správě České republiky;
  - zákon o Celní správě České republiky;
  - zákon o státní službě;
  - zákon o svobodném přístupu k informacím

VÝKLAD GDPR

Zdroje interpretace GDPR

Vodítka a pokyny WP 29

Schválená vodítka/pokyny

- K posouzení vlivu na ochranu osobních údajů (DPIA)
- K pověřenci (DPO)
- K přenositelnosti údajů
- K určení vedoucího dozorového úřadu správce nebo zpracovatele
- K uplatnění a stanovení správních pokut
- K automatizovanému individuálnímu rozhodování a profilování
- K oznamování porušení zabezpečení osobních údajů

Zveřejněná vodítka

- K souhlasu
- K transparentnosti

IMPLEMENTACE GDPR V ORGANIZACÍCH

Fáze implementace GDPR

Rozdílová analýza
(2 – 4 měsíce)

Implementace požadavků, včetně dodatečného mapování
(4 měsíce až 1 rok)

Reziduální rizika?

Analýza rizik, DPIA, zajištění udržitelnosti v čase, certifikace
(1 měsíc)

Stav implementace GDPR na českém trhu

Většina velkých a nadnárodních společností ukončila fázi mapování a zahajuje implementaci

SMEs a veřejná správa a samospráva (včetně škol a nemocnic) zahajují mapování

Doporučený postup efektivní implementace GDPR

Implementace zjevných požadavků (3 měsíce)

Mapování nutné pro implementaci zjevných požadavků

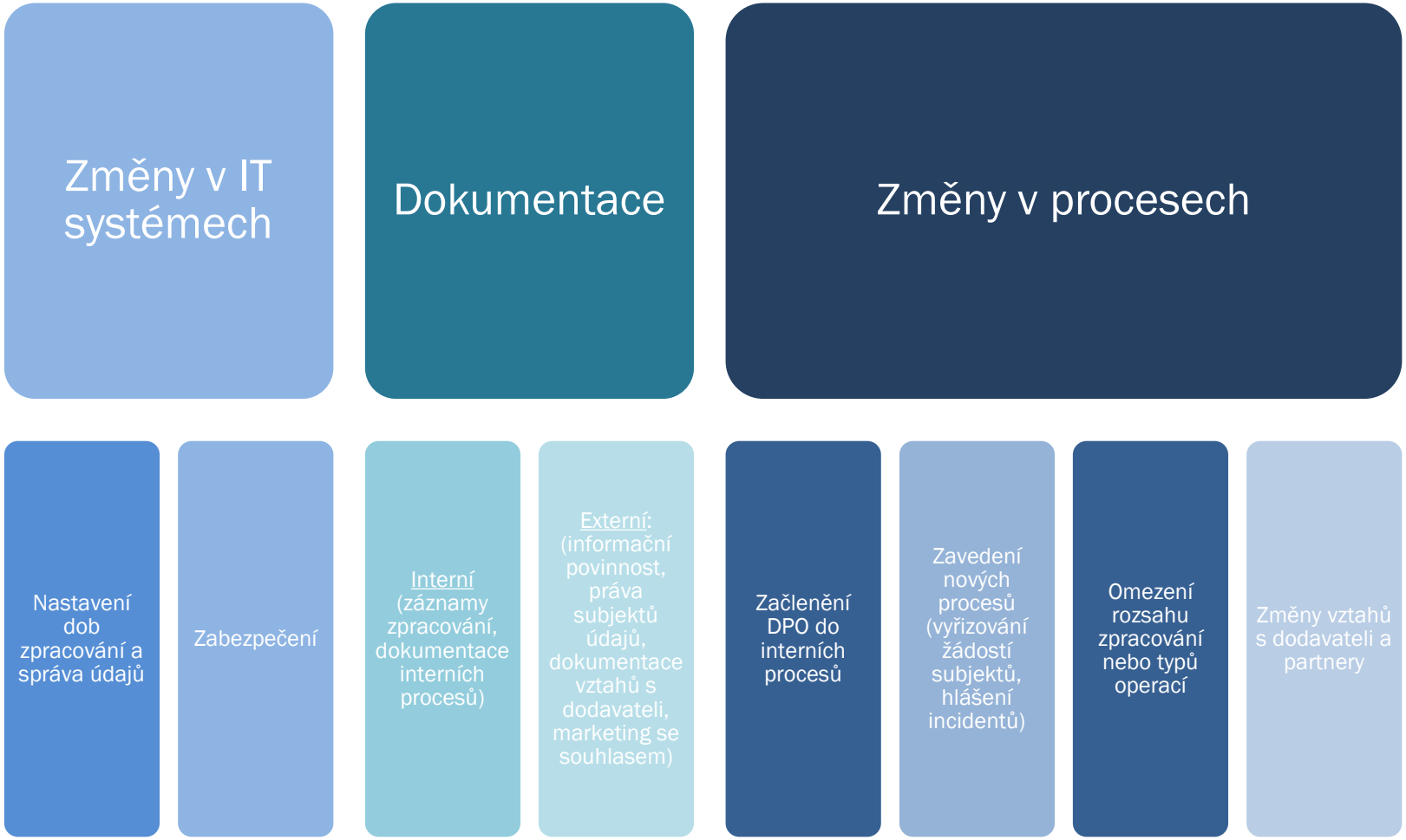
(3 měsíce, paralelně)

Rozdílová analýza

(několik měsíců, podle disponibility interních zdrojů)

Zajištění udržitelnost v čase

Oblasti implementace GDPR



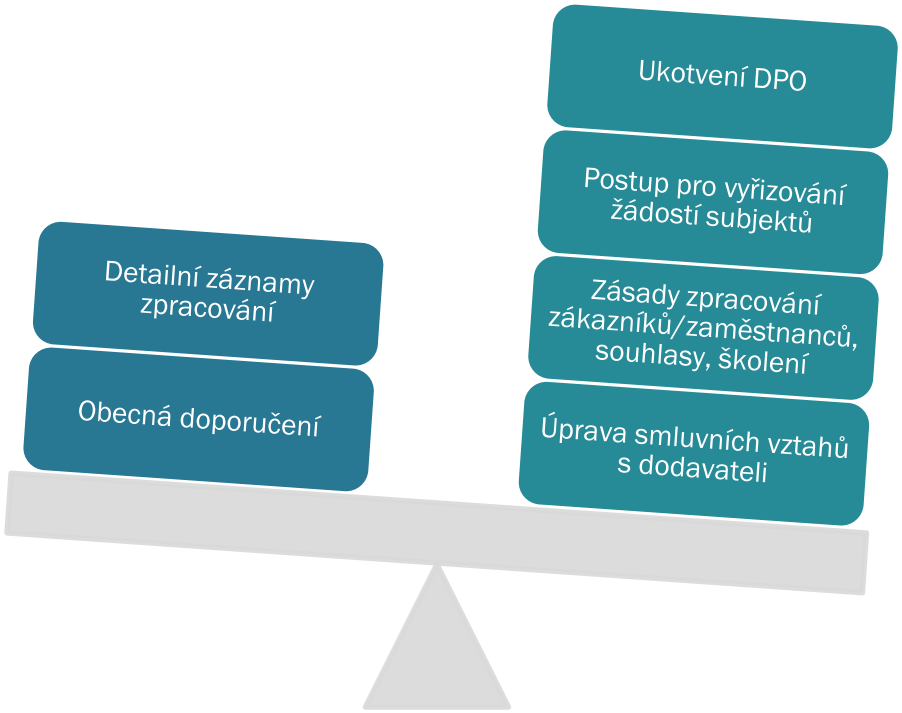
Implementace zjevných požadavků

DPO	• Ustanovení DPO a jeho ukotvení do interních procesů
Vyřizování žádostí subjektů údajů	• Stanovení kontaktního místa a kompetencí • Definice procesu, včetně nutných IT nástrojů • Příprava vzorových dokumentů
Zákazníci	• Zásady zpracování osobních údajů zákazníků • Revize a zrušení souhlasů
Zaměstnanci	• Zásady zpracování osobních údajů zaměstnanců • Souhlasy a zásady zpracování pro náborový proces • Školící program pro vedoucí i řadové zaměstnance
Záznamy zpracování	• Příprava efektivního nástroje pro katalog údajů a záznamy zpracování, včetně právních základů, účelů a dob zpracování
Zabezpečení	• Revize přístupových práv • Revize zranitelnosti koncových zařízení a aplikací instalovaných bez souhlasu správce
Dodavatelé	• Úprava smluvních vztahů s klíčovými dodavateli
Projektový plán dalšího mapování	• Zaměřeno zejména na minimalizaci zpracování, zpřesnění záznamů zpracování a stanovení dob zpracování • Automatizace vyřizování práv subjektů údajů

Rozdílová analýza vs. okamžitá implementace

Rozdílová analýza

Okamžitá implementace, omez. mapování



Okamžitá implementace = zajištění 80 % souladu s GDPR

Takeaway points

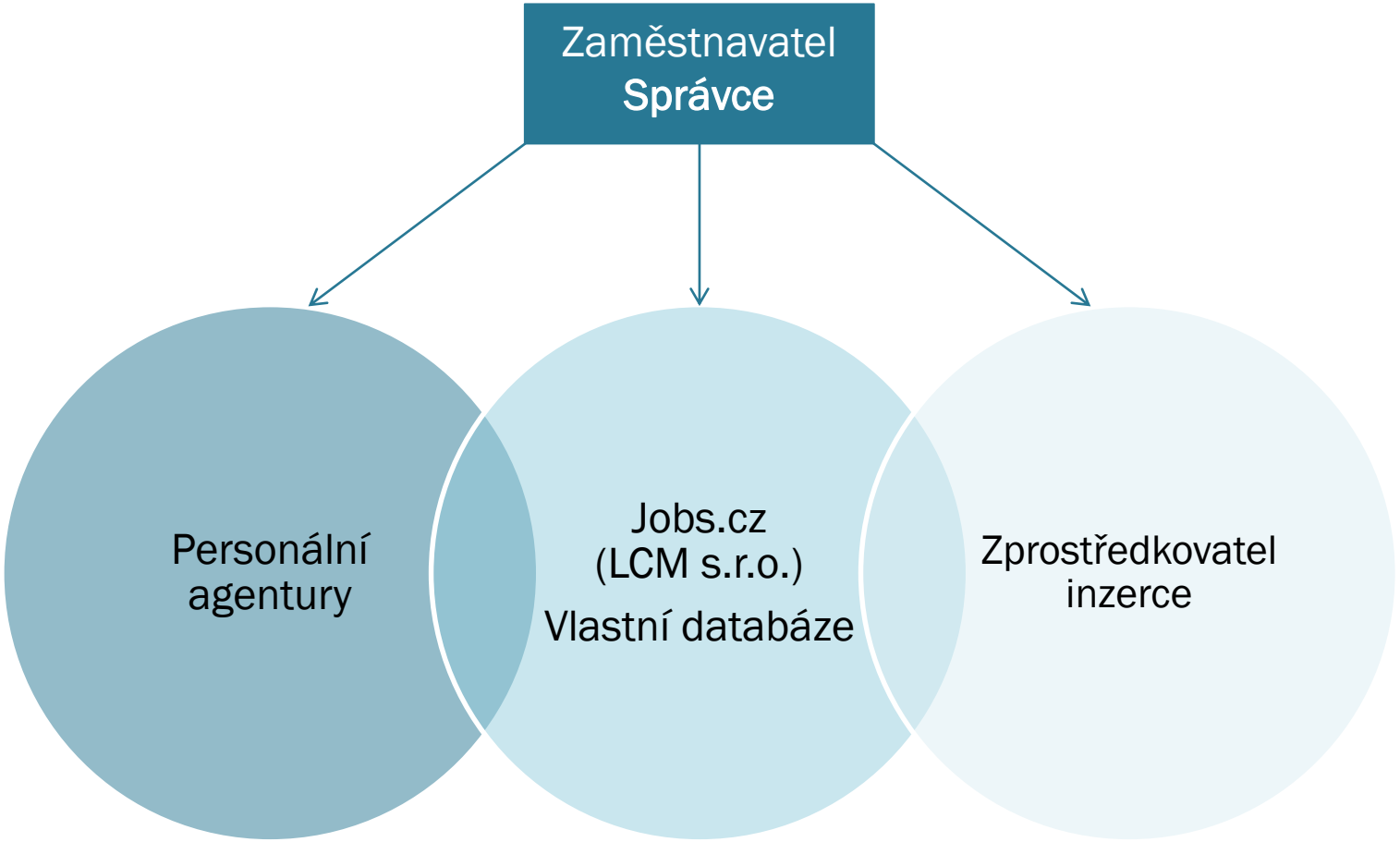
Vysoká rizika se týkají především zpracování údajů bez zákonného podkladu

Za rizikovou oblast je obecně považováno i HR

Mezi „quick wins“ patří záznamy zpracování, informační povinnosti a zavedení procesů k právům subjektů a DPO

NÁBOR ZAMĚSTNANCŮ

Postavení zaměstnavatelů



Doba zpracování

Obecně

- V rámci náborového procesu je primárně právním základem jednání o uzavření smlouvy (stanovisko WP 29 2/2017, rozsudek 6Ca 378/2008)
- Doba zpracování je omezena trváním náborového procesu, po jeho ukončení – výmaz údajů
- Pro jakékoli další účely nesouvisející s náborovým procesem je třeba zajistit souhlasy subjektů (např. analýza)

Přijatí uchazeči

- Přijatí uchazeči se dostávají do zaměstnaneckého režimu
- Informační povinnost – privacy policy

Odmítnutí uchazeči

- Pro účely případného budoucího kontaktu s odmítnutými uchazeči je třeba zajistit jejich souhlas
- Možnost prodloužit dobu zpracování o další 3 měsíce (zkušební doba přijatého zaměstnance)?
- Informační povinnost

Případová studie

Zaměstnavatel zadá personální agentuře inzerát poptávající zaměstnance na určitou pozici. Agentura dle instrukcí zaměstnavatele inzerát zveřejní na svých webových stránkách, prostřednictvím kterých mohou uchazeči na inzerát zaměstnavateli odpovědět. Kromě uchazečů, kteří si inzerát sami najdou na webu agentury a odpoví na něj, agentura zaměstnavateli poskytne i životopisy uchazečů z další databáze, kterou sama spravuje.

V jakém postavení (správce, zpracovatel, společní správci) jsou zaměstnavatel a agentura? Jak a za jakých podmínek může zaměstnavatel s životopisy nakládat?

MONITOROVÁNÍ IT SYSTÉMŮ

Stanovisko WP 29 č. 2/2017

Zásada proporcionality – zvolené řešení by mělo co nejméně zasahovat do práv a svobod zaměstnanců, pokud nelze monitorování omezit – zákaz užívání k soukromým účelům

Technická opatření ke zmírnění dopadů do práv a svobod zaměstnance

Prevence X Detekce

Monitorování X Blokace obsahu

Privacy policy + pokyny k užívání monitorovaných zařízení

Vymezení soukromého prostoru – zejména kalendáře

Home Office, dálkový přístup

- Stejná úroveň ochrany soukromí zaměstnanců
- Nutné přijmout dodatečná technická opatření
- Zásada proporcionality (př. pohyb myši, webová kamera)
- Vzdálený přístup
- „Wearable devices“ – citlivé údaje

BYOD

- Oddělení soukromého obsahu (např. složky s fotografiemi)
- Aplikace pro „sandboxing“

- X geolokalizační data
- X oddělení od soukromého užívání – trvání pracovní doby

- Zaměstnanci musí implementovat bezpečnostní opatření pro zabezpečení přístroje (např. otisk prstu)

Případová studie 1

Zaměstnavatel umožňuje práci z domu, nicméně koncové stanice pro práci z domu monitoruje, pokud jde o čas strávený na jednotlivých aplikacích, aby zajistil efektivní výkon činnosti mimo pracoviště.

Je zaměstnavatel oprávněn takto zajistit efektivitu práce a přitom umožnit benefit práce z domu?

Případová studie 2

Zaměstnanec má přístup ke zvláště chráněným údajům (např. zdravotnické dokumentaci). Zaměstnavatel monitoruje koncovou stanici zaměstnance, aby zamezil nestandardnímu chování a stahování zdravotnické dokumentace, mimo jiné i proto, aby byl schopen dostát povinnosti hlášení bezpečnostních incidentů.

Je zaměstnavatel oprávněn koncovou stanici za tímto účelem monitorovat, případně za jakých podmínek?

Případová studie 3

Zaměstnavatel loguje veškeré přístupy ke své dokumentaci obsahující osobní údaje zákazníků a tyto logy pravidelně vyhodnocuje. Log je spojen s identitou konkrétního zaměstnance. Zároveň má zaměstnavatel nastavena interní pravidla, za jakých okolností mohou zaměstnanci ke konkrétním údajům přistupovat. Zaměstnavatel zjistí, že konkrétní zaměstnanec přistupoval k údajům pravděpodobně v rozporu s interními pravidly, zaměstnance konfrontuje a po potvrzení podezření zahájí kroky vedoucí k ukončení pracovního poměru.

Jedná zaměstnavatel v souladu s GDPR?

ZPRACOVÁNÍ ÚDAJŮ TŘETÍCH OSOB

Případová studie

Zaměstnavatel musí zpracovávat osobní údaje zaměstnanců dodavatele, kteří přistupují k jeho IT infrastruktuře, pro účely zřízení přístupu. Obdobně zpracovává údaje kontaktních osob dodavatele, aby mohl s dodavatelem efektivně komunikovat.

Jak by měl zaměstnavatel ošetřit toto zpracování dle GDPR v případě, že jde o dodavatele právnickou osobu a v případě, že jde o dodavatele fyzickou osobu (OSVČ).

ZPRACOVÁNÍ ZVEŘEJNĚNÝCH ÚDAJŮ

Případová studie 1

Zaměstnavatel si vede databázi údajů zveřejněných subjekty údajů na sociálních sítích v rozsahu jméno, příjmení a fotografie osoby pro účely vedení evidence o odpovědích na nabídky/poptávky práce zveřejněné zaměstnavatelem na sociálních sítích. Zaměstnavatel zároveň nahlíží do profilů uchazečů, kteří do inzerátu nahlédli a kteří na inzerát zareagovali (ať už odpovědí, sdílením či komentářem nebo jiným označením).

Je takový postup možný, a pokud ano, za jakých podmínek?

Případová studie 2

Zaměstnavatel si ověřuje životopisy zaslané uchazeči s jejich veřejnými profily na sociálních sítích a webovými stránkami dřívějších zaměstnavatelů a v případě nesouladu uchazeče konfrontuje.

Jedná zaměstnavatel v souladu s GDPR?

Případová studie 3

Správce si ověřuje kontaktní osoby svých dodavatelů v obchodním rejstříku, případně dle profilu na sociálních sítích, aby si byl jist, že jedná s osobou oprávněnou dodavatele zastupovat. Pokud zjistí nesoulad, dodavatele konfrontuje.

Postupuje v souladu s GDPR?

Případová studie 4

Správce kontaktuje právnické osoby, které identifikuje jako potenciální zákazníky, prostřednictvím kontaktu na ředitele nákupu zveřejněného na internetových stránkách potenciálního zákazníka.

Postupuje v souladu s GDPR?

Může si z těchto kontaktů vytvářet databázi?

OSTATNÍ ZPRACOVÁNÍ

Případová studie 1

Zaměstnavatel sdílí v rámci skupiny se zahraničními společnostmi reporty o zaměstnancích, kterým se v průběhu roku stal pracovní úraz. Součástí reportu jsou i identifikační údaje zaměstnanců (jméno, příjmení, datum a druh úrazu, případně trvalých následků). Účelem je předcházet podobnému typu úrazů a spravovat tuto agendu v rámci jednoho úložiště, aby pokud možno nedocházelo k diskriminaci při odškodňování zaměstnanců z tohoto důvodu.

Je takový postup možný, a pokud ano, jaké povinnosti je zaměstnavatel povinen současně splnit?

Případová studie 2

Zaměstnavatel v rámci svého programu benefitů poskytuje zaměstnancům možnost využívat několik SIM karet dle výhodného firemního tarifu. Tyto SIM karty může zaměstnanec přenechat k využití i svým rodinným příslušníkům. Vzhledem k tomu, že vyúčtování služeb je vedeno na zaměstnavatele, zpracovává zaměstnavatel osobní údaje i těchto třetích osob, na které jsou SIM karty vedené.

Jakým způsobem může zaměstnavatel zpracování osobních údajů těchto třetích osob ošetřit, aby postupoval v souladu s GDPR?

Případová studie 3

Zaměstnavatel používá životopis a kvalifikaci zaměstnance (vzdělání, certifikáty, kursy, jazykové znalosti) k prokázání splnění požadavků výběrových řízení, do kterých zaměstnavatel vstupuje jako uchazeč.

Může zaměstnavatel tyto údaje pro účely účasti ve výběrových řízeních využívat, a pokud ano, z jakého důvodu zpracování?

Musí zaměstnavatel nějak zohlednit, že údaje mohou být v rámci výběrového řízení zpřístupněny dalším osobám a sdíleny případně i mimo EU/EHP?

A DALŠÍ VYBRANÉ OTÁZKY Z PRAXE…

1. Jak dlouho je nutné evidovat na straně e-shopu objednávky?

MINIMÁLNÍ DOBY ZPRACOVÁNÍ:

- Zpravidla po dobu vyřízení objednávky + promlčecí doba
- Nutné zohlednit **požadavky jiných zákonů** (např. uchování faktur po dobu 10 let od konce příslušného zdaňovacího období pro plátce DPH dle zákona o účetnictví)
- Minimální doba uchování nepředstavuje z pohledu GDPR problém za podmínky, že jsou uchovány jen údaje, které jsou pro daný účel potřebné (požadavek minimalizace údajů)

ZPRACOVÁNÍ PRO DALŠÍ ÚČELY:

- Zpracování pro **ochranu oprávněných zájmů provozovatele e-shopu** po dobu, kdy existuje možnost uplatnění případných nároků (vrácení zboží, reklamační lhůty atd.)
- Zpracování údajů pro účely **přímého marketingu** (oprávněný zájem)
    - Kontakt získaný v souvislosti s prodejem zboží/služby od zákazníka
    - Pouze k propagaci **vlastní činnosti**, nelze bez dalšího předávat třetím stranám
    - Doba uchování by měla být přiměřená (britský ICO stanoví obecně přípustné doby retence pro některá odvětví, neexistuje obecné vodítko)
    - V každém zaslaném sdělení musí být dána možnost **další obchodní sdělení odmítnout** (typicky unsubscribe link v zápatí)

2. V případě zaměstnaneckých mobilních telefonů/čísel - je nutné uzavírat zpracovatelskou smlouvu o geolokačních službách s operátorem?

OPERÁTOŘI:

- Operátoři zpracovávají tzv. provozní a lokalizační údaje **na základě zákona a v jeho mezích (jako správci)**
- V tomto ohledu tedy **není třeba po operátorovi aktivně vyžadovat uzavření zpracovatelské smlouvy** – údaje operátor získává přímo od uživatele na základě zákona, po nezbytné době je zpravidla anonymizuje
- Zákon operátorům stanovuje přesný postup pro zpracovávání a ochranu takových údajů
- V některých případech si musí operátor přímo od jednotlivého uživatele vyžádat souhlas se zpracováním provozních a lokalizačních údajů pro poskytování tzv. služeb s přidanou hodnotou (Video on Demand, Voice over IP)

MOBILNÍ APLIKACE:

- Souhlas s jakýmikoli údaji shromažďovanými mobilní aplikací je zpravidla vyžadován **přímo v rozhraní aplikace**
- S lokalizací uživatel musí souhlasit většinou před jejím započetím prostřednictvím dialogového okna

LOKALIZACE ZAMĚSTNANCŮ ZE STRANY ZAMĚSTNAVATELE:

- GPS lokalizace v automobilech je možná pro ochranu oprávněných zájmů zaměstnavatele (bezpečnost, ochrana majetku)
- Zaměstnanec musí být o monitorování informován, ideálně např. nálepkou uvnitř vozidla
- Při soukromém používání musí existovat možnost zařízení dočasně vypnout

3. Jaká je povinnost zaměstnavatele v případě firemních telefonů s ohledem na GDPR?

MOBILNÍ TELEFON POSKYTNUTÝ ZAMĚSTNAVATELEM:

- Zaměstnavatel by měl předně stanovit, zda může zaměstnanec používat mobilní telefon i pro soukromé účely
- Při použití mobilního telefonu pro soukromé účely by pravidla pro takové užití měla být stanovena vnitřním předpisem, který stanoví zejména:
    - Technická opatření, která musí zaměstnanec na svém telefonu udržovat (odemykání pomocí otisku prstu, firewall, nástroje data loss prevention atd.)
    - Postup hlášení v případě ztráty telefonu
    - Pravidla pro ukládání osobních údajů nesouvisejících se zaměstnáním
- Stanovení jasných pravidel umožňuje zaměstnavateli např. vymazat všechna data v mobilním telefonu v případě jeho ztráty a vyhnout se tak v některých případech hlášení porušení zabezpečení osobních údajů

BYOD:

- Nutné stanovit zejména pravidla s ohledem na zabezpečení a na umístění dat spojených se zaměstnáním
- Klíčové je oddělení pracovních a nepracovních dat (např. pomocí tzv. sandboxování v rámci zvláštní aplikace)
- Pro ochranu dat zaměstnavatele lze také stanovit pravidla pro připojení do interní sítě (např. pomocí VPN) apod.

4. Jak je to s CCS kartami pro tankování pohonných hmot - je nutné uzavírat zpracovatelskou smlouvu s vydavatelem karet CCS?

DVA NEJČASTĚJŠÍ MODELY VZTAHU S POSKYTOVATELI RŮZNÝCH ZAMĚSTNANECKÝCH BENEFITŮ:

1. Existuje přímý vztah nejen mezi zaměstnavatelem a poskytovatelem služby, ale i mezi zaměstnancem a poskytovatelem služby; osobní údaje poskytuje přímo zaměstnanec (model zvolený např. u American Express)
2. Neexistuje přímý vztah mezi zaměstnancem a poskytovatelem služby, údaje zaměstnance jsou poskytovateli předány zaměstnavatelem – u CCS bude většinou platit tato alternativa

PŘEDÁNÍ ZAMĚSTNAVATEL – POSKYTOVATEL SLUŽBY:

- Na základě zpracovatelské smlouvy
- Náležitosti zpracovatelské smlouvy – čl. 28 odst. 3 GDPR
- Předání pouze údajů nezbytných pro poskytnutí služby
- Předání na dobu poskytování služby

5. Je zpracování cca 30.000 zákazníků v rámci e-shopu "rozsáhlé pravidelné a systematické monitorování subjektů údajů"? Má e-shop povinnost mít DPO?

- Při běžné činnosti e-shopů zpravidla není třeba DPO jmenovat
- Konkrétní hodnocení záleží na okolnostech, zejména objemu zpracovávaných dat a počtu dotčených subjektů
    - Tj. je např. třeba vyhodnotit, zda e-shop se 30.000 zákazníky je v porovnání s konkurencí průměrný či malý/velký
- Některé typy věrnostních programů mohou naplnit znaky rozsáhlého pravidelného a systematického monitorování

?

PIERSTONE

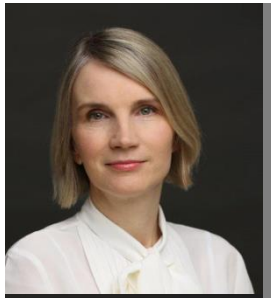
Spolu s kancelářemi v Londýně, Bruselu a Moskvě jeden z největších specializovaných právních týmů zaměřených na právo technologií, médií a komunikací

Hlavní oblasti praxe:

- Ochrana osobních údajů
- IT smlouvy, včetně smluv na cloudové produkty
- IoT
- M&A transakce v technologickém sektoru
- Podpora start-upů při vstupu na zahraniční trhy
- Pracovní právo (včetně technologických aspektů smluv zaměstnanců, BYOD)
- IP právo
- Média
- Telekomunikační právo

Více informací:
www.pierstone.com

Partneři odpovědní za GDPR projekty :



Jana Pattynová
jana.pattynova@pierstone.com
+420 777 738 040

Lenka Suchánková
lenka.suchankova@pierstone.com
+420 777 738 046

13 let nejvyšší nezávislá
hodnocení pro oblast technologie

TOP RANKED CHAMBERS EUROPE Leading firm 2004 - 2017

2017 právnická firma roku Velmi doporučovaná kancelář

The LEGAL 500 EMEA TOP TIER 2004 - 2017