Vilímková Dudák &Partners

FORUM
Naše znalosti pro Váš úspěch

GDPR krok za krokem

Mgr. Klára Valentová

České Budějovice, 25. 4. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Cíl semináře

- poskytnout základní orientaci v problematice ochrany osobních údajů a přehled o povinnostech při zpracování osobních údajů
- seznámit s novou úpravou, kterou přinese obecné nařízení EU o ochraně osobních údajů po nabytí účinnosti v roce 2018
- objasnit pojem „osobní údaj“ a jednotlivé principy ochrany osobních údajů
- upozornit na důsledky a sankce vyplývající z porušování povinností
- poskytnout návod pro implementaci obecného nařízení o ochraně osobních údajů do praxe společnosti

Osnova

- Základní informace o GDPR
- Osobní údaje a další klíčové pojmy
- Postavení subjektů při zpracování osobních údajů
- Pravidla a povinnosti při zpracování osobních údajů
  - základní zásady
  - souhlas subjektu údajů
  - zabezpečení osobních údajů
  - nové povinnosti při zpracování osobních údajů
- Pověřenec pro ochranu osobních údajů
- Předávání osobních údajů do zahraničí

Osnova

- Sankce za porušení povinností
- Dozorové úřady, Evropský sbor pro ochranu osobních údajů
- Implementace GDPR do praxe organizace

Vývoj právní úpravy

- Evropská úprava ochrany osobních údajů
  - Dokumenty Rady Evropy
    - Úmluva o ochraně lidských práv a základních svobod (4.11.1950) (Článek 8 – právo na soukromí a rodinný život)
    - Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat (21.1.1981) a dodatkový protokol o orgánech dozoru a toku údajů přes hranice (8.11.2001)
    - Doporučení výboru ministrů členských států Rady Evropy

Vývoj právní úpravy

- Evropská úprava ochrany osobních údajů
  - Právní předpisy EU
    - Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů
    - Nařízení (EU) 2016/679 – obecné nařízení o ochraně osobních údajů – přímá účinnost od 25. 5. 2018
    - Dílčí úprava – např. Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
    - Rozhodnutí Komise
    - Stanoviska a pokyny Pracovní skupiny 29

Základní informace

- Nařízení (EU) 2016/679 – obecné nařízení o ochraně osobních údajů ze dne 27. 4. 2016
  - nová právní úprava pro všechny členské státy EU a EHP
    - platnost od 24. 5. 2016
    - přímá účinnost od 25. 5. 2018
    - nahrazení směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů a českého zákona o ochraně osobních údajů č. 101/2000 Sb. (ZOOÚ)
    - přebírá veškeré dosavadní zásady, na nichž stojí evropský systém ochrany osobních údajů

Základní informace

- Nařízení (EU) 2016/679 – obecné nařízení o ochraně osobních údajů ze dne 27. 4. 2016
  - jednotná úprava pro celou EU a EHP (nařízení x směrnice)
    - reaguje na technologický vývoj, rozvoj internetu a sociálních sítí, zakotvuje výkladová pravidla stanovená Soudním dvorem EU
    - výrazné rozšíření práv subjektů údajů
    - nové povinnosti pro správce a zpracovatele – důraz na aktivnější přístup
    - klíčové kritérium – rizikovost zpracování osobních údajů
    - vysoké sankce za porušení GDPR

Právní úprava v ČR

- Zrušení ZOOÚ
- Adaptační zákon - zákon o zpracování osobních údajů (sněmovní tisk 138)
- Doprovodný zákon k GDPR - změna zvláštních právních předpisů (sněmovní tisk 139)
- Zákon o některých službách informační společnosti
  - Problém nevyžádané pošty – obchodní sdělení (spamming)

Působnost GPDR

- Věcná působnost
  - Automatizované zpracování
  - Neautomatizované zpracování osobních údajů – jen v případě osobních údajů obsažených v evidenci (strukturovaný soubor osobních údajů)
- Místní působnost
  - činnost provozovny správce nebo zpracovatele v EU bez ohledu na to, zda zpracování probíhá v EU
  - zpracování osobních údajů subjektů údajů, které jsou v EU, správcem nebo zpracovatelem mimo EU – nabídka služeb nebo monitorování chování

Osobní údaje

- Pojem osobní údaj
  - veškeré informace o **identifikované** nebo **identifikovatelné** fyzické osobě (subjekt údajů)
    - Identifikovatelná fyzická osoba = fyzická osoba, kterou lze **přímo či nepřímo identifikovat**, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo ne jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
    - Mezi osobní údaje patří i údaje o lokalitě a síťové identifikátory jako jsou cookies, IP adresa nebo rádiová frekvence

Osobní údaje

- Zvláštní kategorie osobních údajů (citlivé údaje)
  - Osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech; genetické údaje, biometrické údaje sloužící k jedinečné identifikaci fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby
- Údaje týkající se rozsudků v trestních věcech a trestných činů
- Přísnější pravidla pro zpracování

Zpracování osobních údajů

- Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je:
  - Shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracování osobních údajů

Jaké činnosti jsou považovány za zpracovávání osobních údajů?

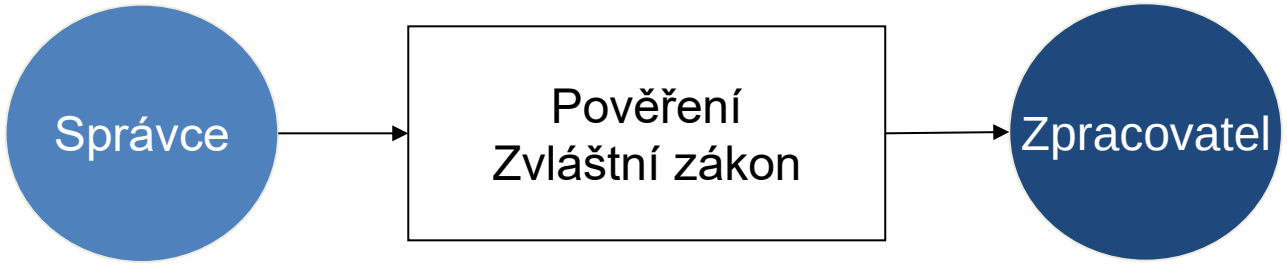
- Vedení mzdové agendy
- Předložení průkazu totožnosti k ověření totožnosti
- Fotografování
- Sepisování účastníků konference
- Vedení osobního deníku
- Vedení osobního spisu
- Vedení spisů o právnické osobě
- Systematické monitorování práce zaměstnanců
- Shromažďování navštívenek

Správce, zpracovatel, příjemce

- Správce
  - Fyzická osoba, právnická osoba
  - Určuje účel a prostředky zpracování
  - Provádí zpracování (Správce ➔ Zpracovatel)
  - Odpovídá za zpracování

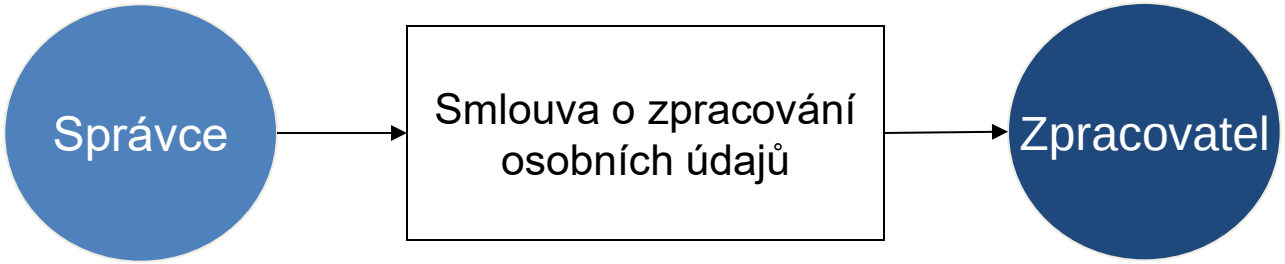
Správce, zpracovatel, příjemce

- Zpracovatel
  - Fyzická osoba, právnická osoba
  - Zpracování osobních údajů pouze v souladu se stanoveným účelem
  - Na základě zvláštního zákona nebo pověření správcem



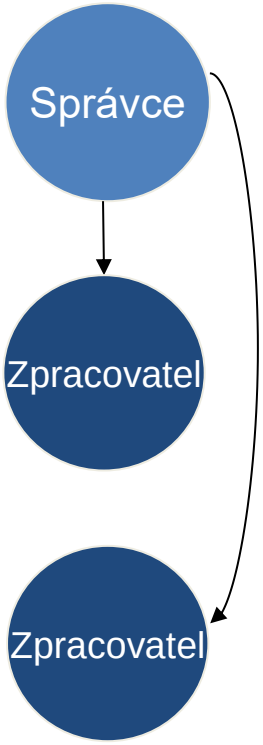
Správce, zpracovatel, příjemce

- Smlouva o zpracování osobních údajů
  - Mezi správcem a zpracovatelem
  - Písemná forma
  - Obsahové náležitosti



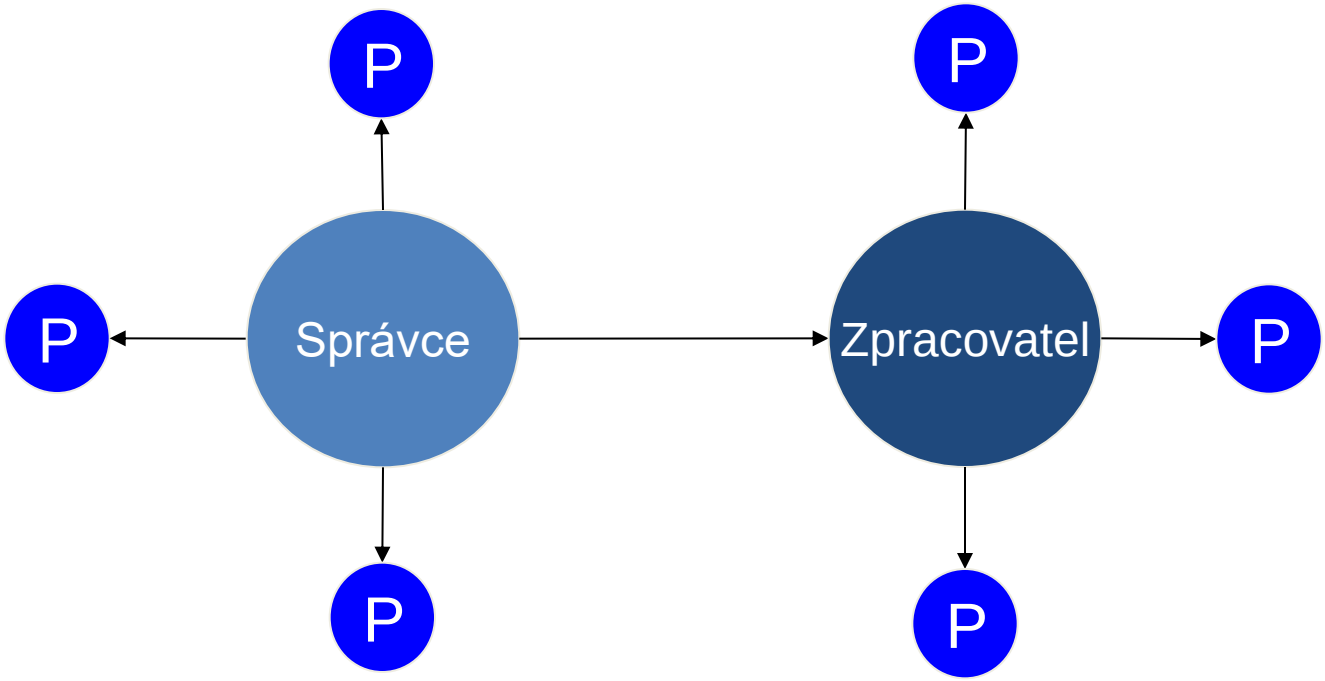
Správce, zpracovatel, příjemce

- Řetězení zpracovatelů



Správce, zpracovatel, příjemce

- Příjemce
  - Subjekt, kterému jsou osobní údaje poskytnuty



Pravidla při zpracování osobních údajů

- Zásady zpracování osobních údajů
  - zákonnost, korektnost a transparentnost
  - účelové omezení
  - minimalizace údajů
  - přesnost
  - omezení uložení
  - integrita a důvěrnost
  - odpovědnost

Pravidla při zpracování osobních údajů

- Odpovědnost správce
  - vhodná technická a organizační opatření k zajištění a doložení souladu zpracování osobních údajů s GDPR
- Kodexy chování
  - vypracovány sdruženími nebo jinými subjekty zastupujícími různé kategorie správců nebo zpracovatelů
  - schválení dozorovým úřadem nebo Komisí
- Vydávání osvědčení
  - akreditované subjekty pro vydávání osvědčení

Pravidla při zpracování osobních údajů

- Záznamy o činnostech zpracování
  - správce, zpracovatel, případný zástupce
    - jméno a kontaktní údaje správce (zpracovatele), případně společného správce, zástupce správce a pověřence pro ochranu osobních údajů
    - účely zpracování, popis kategorií subjektů údajů a osobních údajů, kategorie příjemců
    - předávání osobních údajů do třetí země, plánované lhůty pro výmaz, popis bezpečnostních opatření
  - výjimka? – zaměstnavatelé s méně než 250 zaměstnanci
  - povinnost poskytnout záznamy dozorovému úřadu

Pravidla při zpracování osobních údajů

- Zpracování bez souhlasu
  - splnění smlouvy uzavřené se subjektem údajů nebo provedení opatření před uzavřením smlouvy
  - splnění právní povinnosti
  - ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
  - splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
  - oprávněné zájmy správce nebo třetí strany (přímý marketing, předávání osobních údajů ve skupině podniků)

Pravidla při zpracování osobních údajů

- Souhlas subjektu údajů
  - musí být svobodný, konkrétní, informovaný a jednoznačný
  - je odvolatelný a o tomto právu musí být subjekt údajů informován.
  - specifické podmínky pro souhlas dítěte v souvislosti se službami informační společnosti (potvrzení od rodičů)
  - souhlas v písemném prohlášení, který se týká také jiných skutečností – žádost o vyjádření souhlasu musí být jasně odlišitelná, srozumitelná a snadno přístupná (jasné a jednoduché jazykové prostředky)

Pravidla při zpracování osobních údajů

- Souhlas subjektu údajů
  - svoboda souhlasu – důsledně zohlednit skutečnost, zda není plnění smlouvy podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění smlouvy nutné

Pravidla při zpracování osobních údajů

- Zpracování „citlivých údajů“
  - výslovný souhlas subjektu údajů, ledaže platí absolutní zákaz zpracování
  - pracovní právo, sociální zabezpečení a sociální ochrana
  - životně důležité zájmy subjektu údajů nebo jiné fyzické osoby
  - činnost nadace, sdružení nebo jiného neziskového subjektu
  - zveřejněné osobní údaje subjektem údajů

Pravidla při zpracování osobních údajů

- Zpracování „citlivých údajů“
  - významný veřejný zájem
  - preventivní nebo pracovní lékařství, posuzování pracovní schopnosti zaměstnance, lékařská diagnostika, poskytování zdravotní nebo sociální péče či léčby, řízení systémů a služeb zdravotní nebo sociální péče
  - veřejný zájem v oblasti veřejného zdraví
  - archivace, vědecký či historický výzkum, statistické účely

Pravidla při zpracování osobních údajů

- Zpracování osobních údajů o rozsudcích v trestních věcech a trestných činech
  - pod dozorem orgánu veřejné moci (souhrnné rejstříky trestů)
  - oprávněné zpracování podle práva EU nebo členského státu

Pravidla při zpracování osobních údajů

- Nové povinnosti v oblasti zabezpečení ochrany osobních údajů
  - povinnost vést evidenci všech bezpečnostních incidentů
  - povinnost oznamovat případy porušení zabezpečení osobních údajů Úřadu a subjektu údajů
- Posouzení vlivu na ochranu osobních údajů
  - vysoké riziko pro subjekty údajů
  - Vodítka Pracovní skupiny 29
- Předchozí konzultace s dozorovým úřadem
  - „zbytkové“ vysoké riziko pro subjekty údajů

Pravidla při zpracování osobních údajů

- Povinnost jmenovat v určitých případech pověřence pro ochranu osobních údajů
  - Vodítka Pracovní skupiny 29
  - Kdo musí mít pověřence?
    - orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí
    - hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů
    - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů
  - Interní nebo externí (FO i PO) pověřenec
  - Úkoly a odpovědnost pověřence

Ochrana práv subjektu údajů

- Rozšíření práv subjektu údajů
  - rozšířená informační povinnost
  - zakotvení práva být zapomenut
  - zakotvení práva na přenositelnost údajů
  - zakotvení práva na omezení zpracování
  - zakotvení práva vznést námitku proti zpracování
  - omezení možnosti profilace subjektu údajů

Ochrana práv subjektu údajů

- Postupy správce pro výkon práv subjektu údajů
  - povinnost správce poskytovat informace a sdělení subjektům údajů stručným, transparentním a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků
  - informace se lze poskytnout písemně, v elektronické formě a v některých případech i ústně

Ochrana práv subjektu údajů

- Postupy správce pro výkon práv subjektu údajů
  - žádost subjektu údajů
    - musí být vyřízena bez zbytečného odkladu, nejpozději do 1 měsíce (lze prodloužit od další 2 měsíce – nutné informovat subjekt údajů)
    - při nevyhovění žádosti – povinnost bezodkladně (nejpozději do 1 měsíce) informovat subjekt údajů o důvodech a možnosti podat stížnost u Úřadu pro ochranu osobních údajů („ÚOOÚ“) a žádat o soudní ochranu
  - bezplatné poskytnutí informace nebo sdělení (výjimky)

Ochrana práv subjektu údajů

- Informační povinnost
  - osobní údaje jsou získány od subjektu údajů
    - správce je povinen poskytnout informace v okamžiku získání osobních údajů (mohou být doplněny standardizovanými ikonami)

Ochrana práv subjektu údajů

- Informační povinnost
  - osobní údaje jsou získány od subjektu údajů
    - totožnost a kontaktní údaje správce a jeho případného zástupce
    - případně kontaktní údaje pověřence pro ochranu osobních údajů
    - účely zpracování a právní základ pro zpracování
    - případné příjemce nebo kategorie příjemců osobních údajů
    - případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci
    - doba po kterou budou osobní údaje uloženy
    - informace o právech subjektu údajů
    - informace o povinnosti/dobrovolnosti poskytnutí osobních údajů
    - informace o tom, že dochází k automatizovanému rozhodování, včetně profilování

Ochrana práv subjektu údajů

- Informační povinnost
  - osobní údaje nejsou získány od subjektu údajů
    - správce je povinen poskytnout informace nejpozději do 1 měsíce od získání osobních údajů nebo v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů nebo při prvním zpřístupnění osobních údajů příjemci (mohou být doplněny standardizovanými ikonami)
    - další informace – kategorie osobních údajů, zdroj osobních údajů

Ochrana práv subjektu údajů

- Informační povinnost
  - osobní údaje nejsou získány od subjektu údajů
    - výjimky – poskytnutí takové informace není možné nebo by vyžadovalo nepřiměřené úsilí; získávání nebo zpřístupnění osobních údajů je výslovně stanoveno právem EU nebo členského státu

Ochrana práv subjektu údajů

- Právo na přístup k osobním údajům
  - právo subjektu údajů získat potvrzení, zda jsou nebo nejsou jeho osobní údaje zpracovávány, a přístup k těmto údajům a dalším informacím
  - povinnost správce poskytnout kopii zpracovávaných osobních údajů (první kopie zdarma)

Ochrana práv subjektu údajů

- Právo na opravu
  - povinnost správce opravit bez zbytečného odkladu nepřesné osobní údaje
  - povinnost správce doplnit neúplné osobní údaje (s přihlédnutím k účelům zpracování)

Ochrana práv subjektu údajů

- Právo na výmaz
  - osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny
  - subjekt údajů odvolá souhlas
  - subjekt údajů vznese námitky
  - osobní údaje byly zpracovány protiprávně
  - osobní údaje musí být vymazány ke splnění právní povinnosti
  - osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační povinnosti

Ochrana práv subjektu údajů

- Právo na omezení zpracování
  - subjekt údajů popírá přesnost osobních údajů
  - zpracování osobních údajů je protiprávní
  - správce již osobní údaje nepotřebuje, ale požaduje je subjekt údajů
  - subjekt údajů vznesl námitku proti zpracování

Ochrana práv subjektu údajů

- Právo na přenositelnost údajů
  - subjekt údajů má právo získat osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci:
    - zpracování je založeno na souhlasu nebo smlouvě
    - zpracování se provádí automatizovaně
  - Pokyny Pracovní skupiny 29

Ochrana práv subjektu údajů

- Právo vznést námitku
  - právo subjektu údajů kdykoli vznést námitku
    - při zpracování osobních údajů pro splnění úkolu prováděného ve veřejném zájmu, při výkonu veřejné moci, nebo pro účely oprávněných zájmů správce nebo třetí strany
      - správce musí prokázat závažné oprávněné důvody pro zpracování nebo pro určení, výkon nebo obhajobu právních nároků
    - zpracování pro účely přímého marketingu (včetně profilování)
    - subjekt údajů musí být na toto právo výslovně upozorněn (informace musí být uvedena odděleně od jiných informací)

Ochrana práv subjektu údajů

- Automatizované rozhodování a profilování
  - právo subjektu údajů nebýt předmětem automatizovaného rozhodování, včetně profilování
  - výjimky:
    - rozhodnutí je nezbytné pro uzavření nebo plnění smlouvy
    - rozhodnutí je povoleno právem EU nebo členského státu
    - rozhodnutí je založeno na výslovném souhlasu subjektu údajů

Ochrana práv subjektu údajů

- Oznamovaní bezpečnostních incidentů
  - povinnost bez zbytečného odkladu informovat subjekt údajů
    - porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob
    - popis povahy porušení zabezpečení osobních údajů, pravděpodobných důsledků a následných opatření
  - výjimky:
    - správce provedl náležitá ochranná opatření (např. šifrování)
    - správce přijal následná opatření, která snižují riziko incidentu
    - oznámení by vyžadovalo nepřiměřené úsilí

Předávání osobních údajů do zahraničí

- Nová pravidla pro předávání osobních údajů do třetích zemí
  - omezení povolovacího řízení ze strany Úřadu
  - předání na základě rozhodnutí o odpovídající ochraně
  - předání založené na vhodných zárukách
  - závazná podniková pravidla
  - výjimky pro specifické situace
  - zavedení nových možností pro předávání osobních údajů do třetích zemí (např. na základě schválených kodexů chování nebo získaného osvědčení)

Úřad pro ochranu osobních údajů

- Činnost a působnost Úřadu
  - Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů
  - Přijímá podněty a stížnosti občanů na porušení zákona
  - Projednává porušení povinností a uděluje pokuty
  - Poskytuje konzultace v oblasti ochrany osobních údajů

www.uoou.cz

Úřad pro ochranu osobních údajů

- Odpovědnost za porušení zákonných povinností
  - Kontrolní činnost Úřadu
    - Na základě kontrolního plánu nebo na základě podnětů a stížností
    - Opatření k nápravě (odstranění zjištěných nedostatků) - při nápravě Úřad může upustit od uložení pokuty
    - Pokuty za nesplnění povinností při kontrole (až do výše 500.000 Kč)

Dozorové úřady

- Odpovědnost a sankce
  - možnost uložit pokuty až do výše 10 milionů EUR nebo 20 milionů EUR (podle porušené povinnosti) a v případě podniku až do výše 2 %/4 % celkového celosvětového ročního obratu – uplatní se vyšší pokuta
  - odrazující x likvidační pokuta
  - kritéria pro uložení pokuty (závažnost porušení, úmysl/nedbalost, délka porušení, předchozí jednání správce atd.)
  - nápravná opatření
  - Vodítka Pracovní skupiny 29
- Dotčený dozorový úřad x vedoucí dozorový úřad

Postup při implementaci GDPR

- Stanovení odpovědné osoby za implementaci GDPR
  - Primární odpovědnost – statutární orgán
  - Budoucí pověřenec, firemní právník, člen vrcholového vedení, vedoucí compliance oddělení nebo interního auditu…
- Sestavení realizačního týmu a jeho proškolení
  - Sestavit seznam oddělení a vybrat jednotlivé zástupce
  - Personalista, obchodní manažer, marketingový manažer, interní právník, IT specialista…
  - Úprava náplně práce
- Stanovení priorit, etap a termínu pro projekt

Mapování zpracování osobních údajů

Koncepce ochrany osobních údajů

Bezpečnostní opatření

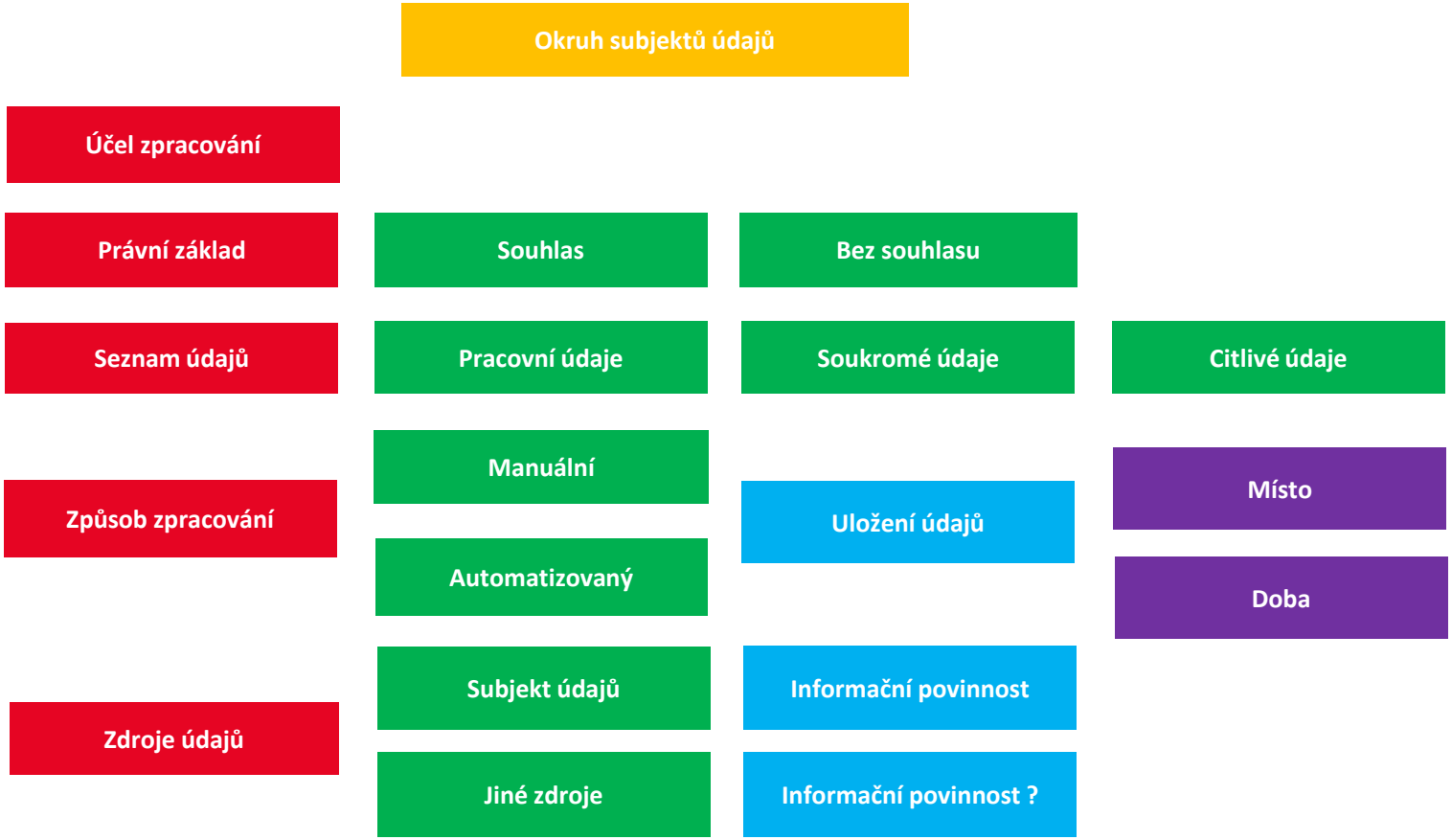
Revize/příprava dokumentů

Nastavení interních procesů

Úpravy v IT systému

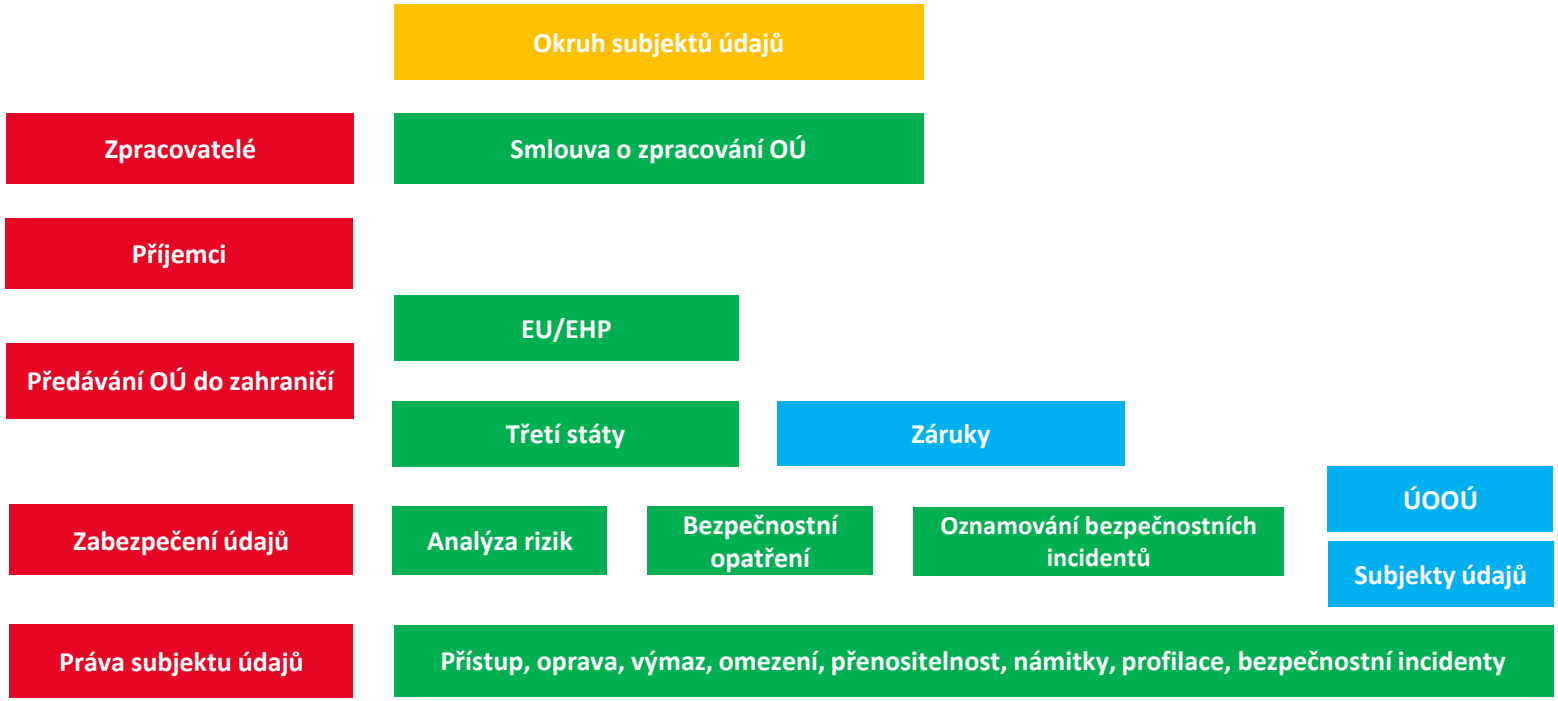
Postup při implementaci GDPR

Analýza zpracování osobních údajů – mapování



Postup při implementaci GDPR

Analýza zpracování osobních údajů – mapování



Postup při implementaci GDPR

- Příprava záznamů o činnostech zpracování
- Posouzení nových povinností
  - Pověřenec pro ochranu osobních údajů
  - Posouzení vlivu na ochranu osobních údajů, konzultace s ÚOOÚ
- Analýza rizik
  - Seznam všech rizik a jejich ohodnocení
    - Přírodní vlivy a události
    - Vnější a vnitřní útoky
  - Přijetí a dokumentace bezpečnostních opatření
  - Bezpečnostní směrnice, pokyny a školení pro zaměstnance

Postup při implementaci GDPR

- Zhodnocení stavu ochrany a zabezpečení osobních údajů podle ZOOÚ a GDPR
- Příprava koncepce ochrany osobních údajů
  - Osvědčení, kodexy chování
  - Vlastní přístup
- Návrh řešení a opatření
  - Akční plán

Postup při implementaci GDPR

- Implementace konkrétních kroků
  - např. revize textu souhlasu a informací pro subjekt údajů, příprava bezpečnostní směrnice, přijetí organizačních a technických opatření, příprava a implementace IT řešení
- Průběžně sledovat
  - webové stránky Úřadu (www.uoou.cz)
  - Pracovní skupiny 29 (http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)
  - odborný tisk a školení
- Testování a aktualizace zavedeného systému
- Pravidelná školení zaměstnanců

Závěrečné shrnutí

- Proč je důležité se začít připravovat na GDPR?
  - Nařízení je již v platnosti a od 25. 5. 2018 bude přímo účinné v České republice – právní úprava je tedy již v obecném rámci daná a známá. Česká legislativa bude řešit jen dílčí záležitosti. V tuto chvíli je tedy možné se již dostatečně začít připravovat.
  - Za nedodržení nařízení hrozí o mnoho vyšší pokuty než dnes.
  - Rozsah práv subjektů údajů se výrazně rozšířil a tomu odpovídají i nové povinnosti správců a zpracovatelů, které budou mít vliv na nastavení interních systémů (včetně IT) a procesů.

Dotazy?

Mgr. Klára Valentová, advokát

Vilímková Dudák & Partners,
advokátní kancelář, s.r.o.

www.vilimkovadudak.cz

Vilímková Dudák &Partners

FORUM
Naše znalosti pro Váš úspěch

Děkuji za pozornost!

Tento seminář pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání

Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz