Obecné nařízení na ochranu osobních údajů

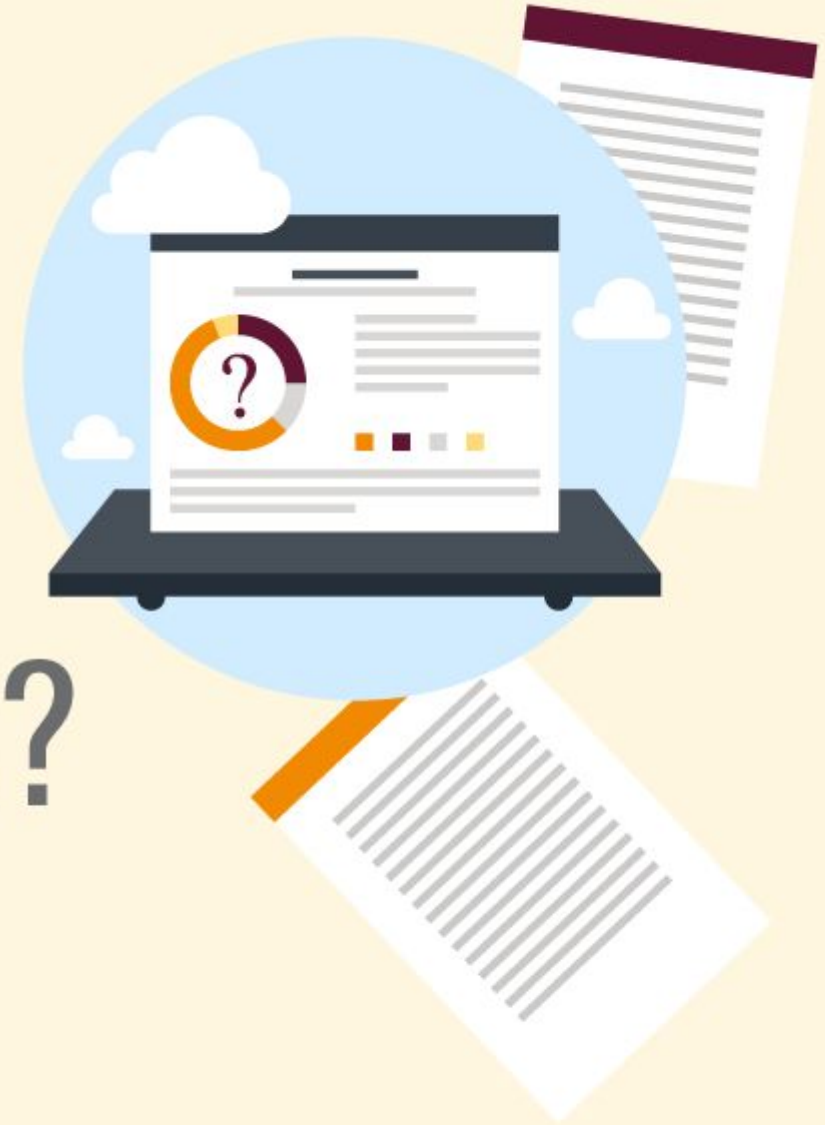
Úvod do GDPR

Mgr. Eva Škorničková

Právní konzultantka ochrany dat a bezpečnosti IT

EVA ŠKORNIČKOVÁ

Co je GDPR?



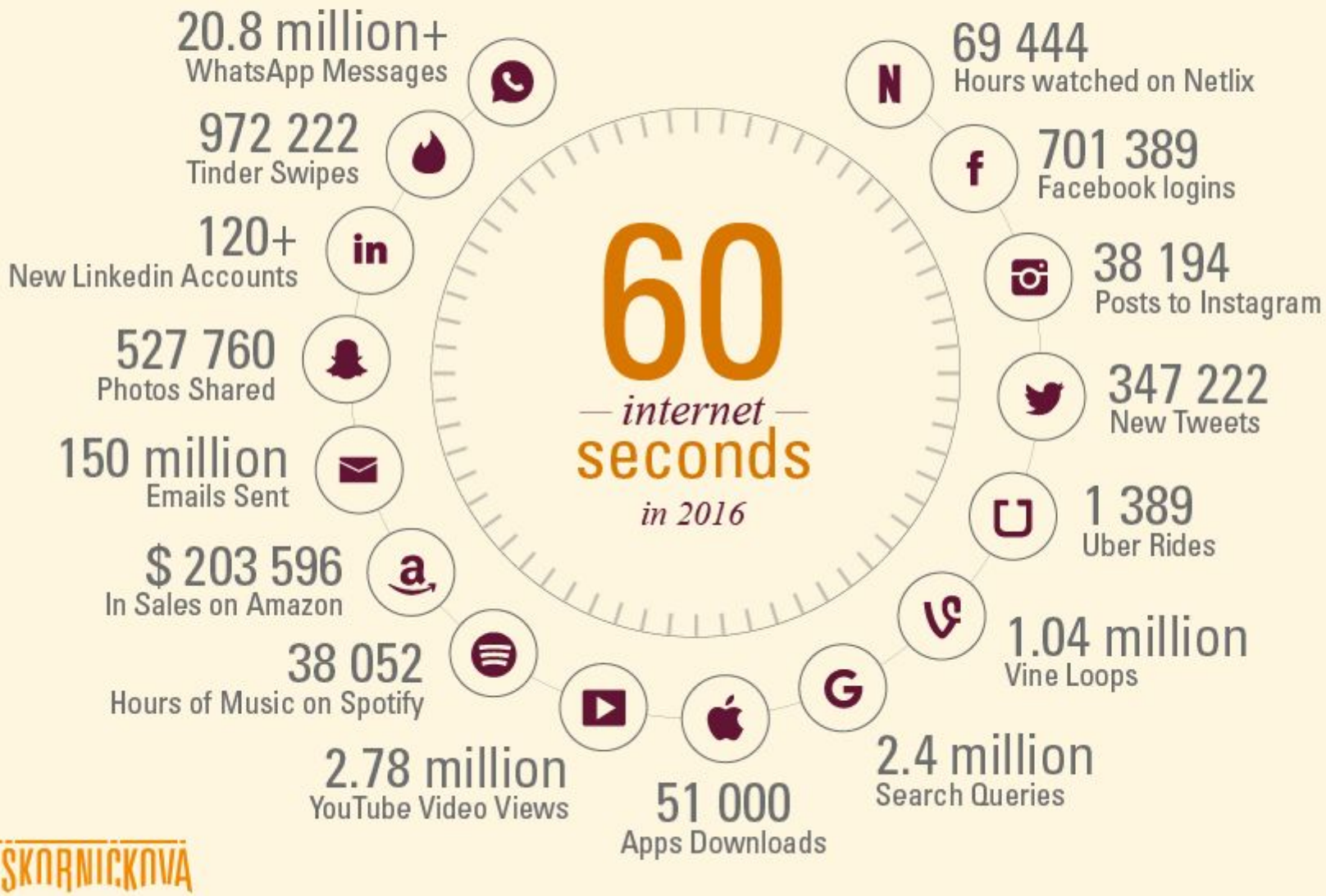
EVA ŠKORNIČKOVÁ

GDPR

- Nařízení bylo schváleno Evropským parlamentem 14. 4. 2016 po 4 letém vyjednávání
- Nahrazuje Směrnici 95/46 EC s účinností od 25.5. 2018 a v ČR zákon č. 101/2000 Sb. na ochranu osobních údajů
- Nejkomplexnější soubor pravidel na ochranu dat na světě
- Výrazným povýšením ochrany dat na úroveň evropského zákona se posiluje právo osob na lepší kontrolu nad jejich osobními údaji
- Harmonizace pravidel pro 28 států EU a EFTA zemí - Norsko, Island a Lichtenštejnsko = státy Evropského hospodářského prostoru - 31 národních zákonů bude zrušeno
- Rovnocenná vymahatelnost práva a stejné sankce pro všechny státy, konzistentní právní úprava, účinná spolupráce regulatorních orgánů
- Představuje rovnováhu mezi legitimními zájmy správců a zpracovatelů dat a právem osob na soukromí

EVA ŠKORNICKOVÁ

Proč potřebuje ochrana dat *reformu?*



EVA ŠKORNICKOVÁ

Správní *pokuty*

Výše závisí na řadě faktorů

- Povaha, závažnost a délka porušení s přihlédnutím k povaze, rozsahu či účelu zpracování
- Úmysl nebo nedbalost
- Počet dotčených subjektů a míra škody
- Kroky podniknuté správcem či zpracovatelem ke zmírnění škod
- Míra odpovědnosti s přihlédnutím na technické a organizační opatření
- Předchozí porušení
- Míra spolupráce s dozorovým úřadem za účelem nápravy
- Kategorie osobních údajů dotčené porušením
- Způsob, jakým se dozorový úřad dozvěděl o porušení

20 000 000 EUR

nebo *4 %* z celkového ročního obratu celosvětově za předchozí finanční rok

10 000 000 EUR

nebo *2 %*

EVA ŠKORNICKOVÁ

Článek 83

CO
se změní

EVA ŠKORNICKOVÁ

GDPR principy zpracování *osobních údajů*

- Zákonnost, spravedlivost a transparentnost vůči subjektu dat
- Shromáždění pro určité, výslovně vyjádřené a legitimní účely
- Minimalizace údajů
- Přesnost údajů a aktuálnost dat
- Omezení uložení
- Integrita a důvěrnost
- Odpovědnost

Směrnice *versus* nařízení

Směrnice

- Dokument přijatý na úrovni EU
- Národní implementace (“naklonování”)
- Místní variace (“genetické varianty”)

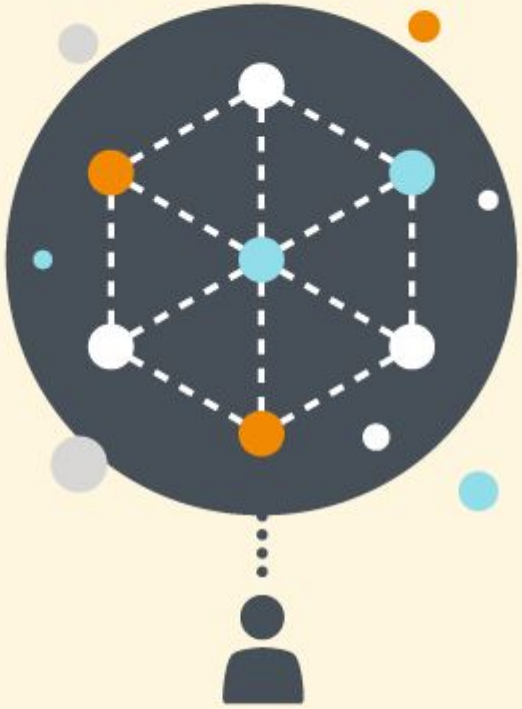
Nařízení

- Dokument přijatý na úrovni EU
- Není potřeba národní implementace
- “Jeden předpis řídí všechny”

EVA ŠKORNICKOVÁ

Osobní *údaje*

- Veškeré informace vztahující se k identifikované nebo identifikovatelné fyzické osobě
- Nevztahuje se na osobní údaje zesnulých osob a anonymizované údaje
- Vztahuje se na šifrované osobní údaje, protože někdo zná šifrovací klíč



Fyzické osoby

Podnikatelé

- OSVČ
- Právnické osoby

EVA ŠKORNICKOVÁ

článek 4 (1)
vysvětlivky 26 - 27

Osobní *údaje*

- *Veškeré informace*
  obrazové, slovní, rentgenové snímky, IP adresa
- *Vztahující se*
  Vztah daný obsahem - např. jméno, adresa, pracovní pozice
- *K identifikované nebo identifikovatelné osobě*
  Specifické charakteristiky, nepřímá identifikace přihlédnutím ke všem prostředkům, např. výběr vyčleněním

..... vše, co mne odlišuje od ostatních subjektů

EVA ŠKORNICKOVÁ

Osobní údaje
- jednotlivé prvky

Obecné

- Jméno
- Pohlaví
- Věk a datum narození
- Osobní stav
- Občanství
- IP adresa
- Fotografický údaj

Organizační

- pracovní nebo osobní adresa
- pracovní nebo osobní telefonní číslo
- pracovní nebo osobní e-mail
- ověřovací identifikační údaje
- identifikační čísla vydaná státem

ČÍM VÍCE OSOBNÍCH ÚDAJŮ MÁTE, TÍM VĚTŠÍM RIZIKŮM SPOJENÝM S JEJICH OCHRANOU SE VYSTAVUJETE!

EVA ŠKORNICKOVÁ

Citlivé osobní údaje
- speciální kategorie

Vypovídají o:

- Rasovém či etnickém původu
- Politických názorech
- Náboženském nebo filozofickém vyznání
- Členství v odborech
- Zdravotním stavu
- Sexuální orientaci
- Trestních deliktech či pravomocném odsouzení

Genetické a biometrické údaje

EVA ŠKORNICKOVÁ

Genetické údaje

- Osobní údaje vztahující se ke zděděným nebo získaným genetickým charakteristikám
- Poskytující jedinečné informace o fyziologii nebo zdraví
- Vyplývající z analýzy biologického vzorku

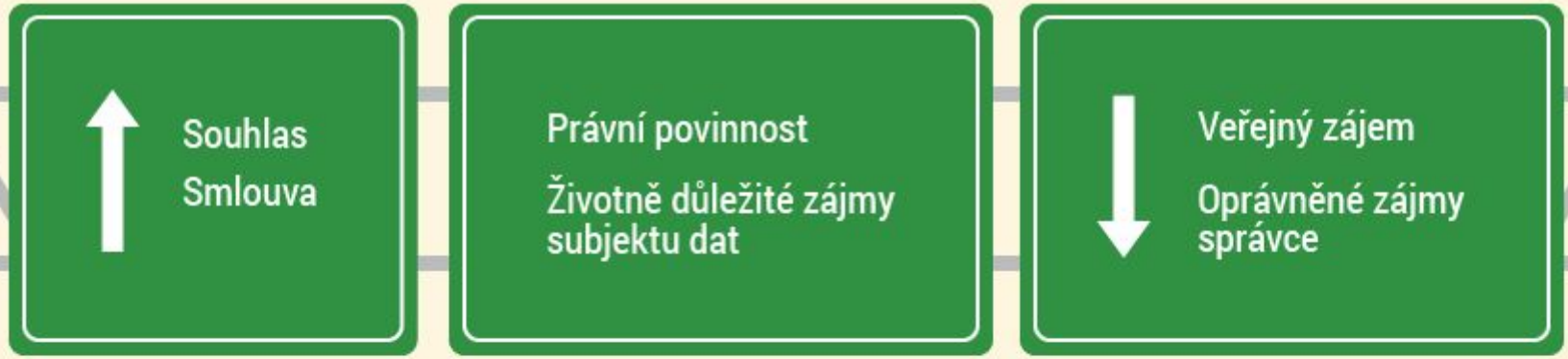
Biometrické údaje

- Osobní údaje vyplývající z konkrétního technického zpracování
- Vztahující se k fyzickým, fyziologickým nebo behaviorálním charakteristikám
- Ty, které dovolují nebo potvrzují jedinečnou identifikaci
- Například snímky obličeje nebo daktyloskopické údaje

EVA ŠKORNICKOVÁ

Zákonnost zpracování *osobních údajů*

- Musí být splněna aspoň 1 z podmínek



EVA SKORNICKOVÁ

Článek 6
vysvětlivka 40

Zákonnost zpracování *osobních údajů*

Souhlas subjektu údajů není nutný pro zpracování údajů na základě

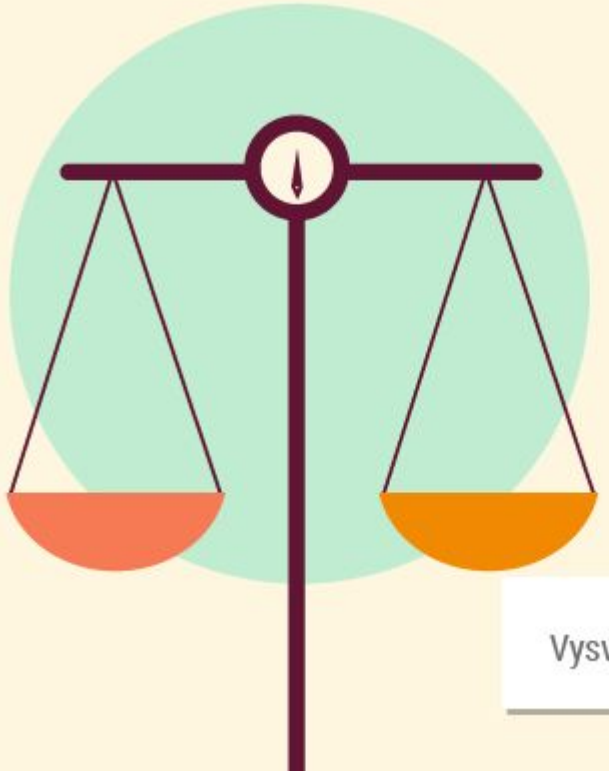
- smlouvy - nikdy nedávat souhlas do smlouvy
- pro ochranu životně důležitých zájmů subjektu - např. subjekt dat je v bezvědomí a není schopen udělit souhlas
- pro splnění právní povinnosti správce nebo pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci - např. soukromé pojišťovny, zdravotnická zařízení - může být specifikováno národní legislativou

Státní úřady mohou zpracovávat osobní údaje jen ve veřejném zájmu nebo pro splnění právní povinnosti - např. daňový úřad, policie atd.

Zpracování dat z důvodu oprávněného zájmu *správce nebo třetí strany*

- Oprávněné zájmy správce nesmí převažovat nad zájmy nebo právy a svobodami subjektu údajů = ROVNOVÁHA
- Např. předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely

Zpracování těchto údajů se doporučuje se souhlasem subjektu dat

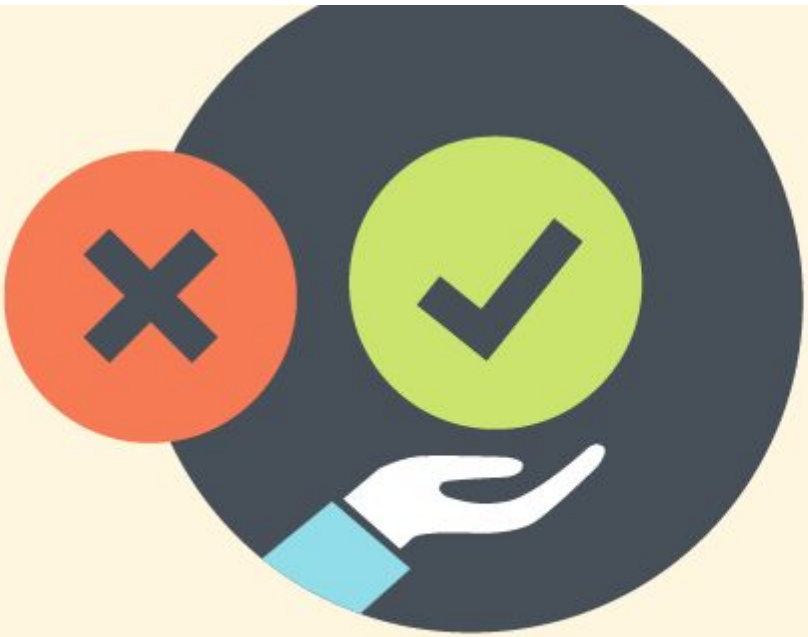


Vysvětlivky 47 - 49

Zpracování *citlivých dat*

Je možné jen za těchto předpokladů:

- Výslovný souhlas subjektu údajů se zpracováním
- Zpracování je nezbytné v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany
- Zpracování je nutné pro ochranu životně důležitých zájmů subjektu, v případě, že subjekt není fyzicky nebo právně schopen udělit souhlas
- Zpracování sleduje politické, filozofické, náboženské nebo odborové cíle - nadace, sdružení, neziskové organizace
- Zpracování se týká údajů zjevně zveřejněných subjektem údajů
- Zpracování je nezbytné pro obhajobu právních nároků nebo v rámci soudního řízení
- Z důvodu veřejného zájmu na základě EU nebo národního práva
- Pro účely preventivního lékařství, posouzení pracovní schopnosti zaměstnance, veřejného zájmu v oblasti veřejného zdraví
- Zpracování pro účely vědeckého, historického výzkumu nebo statistické účely



Souhlas

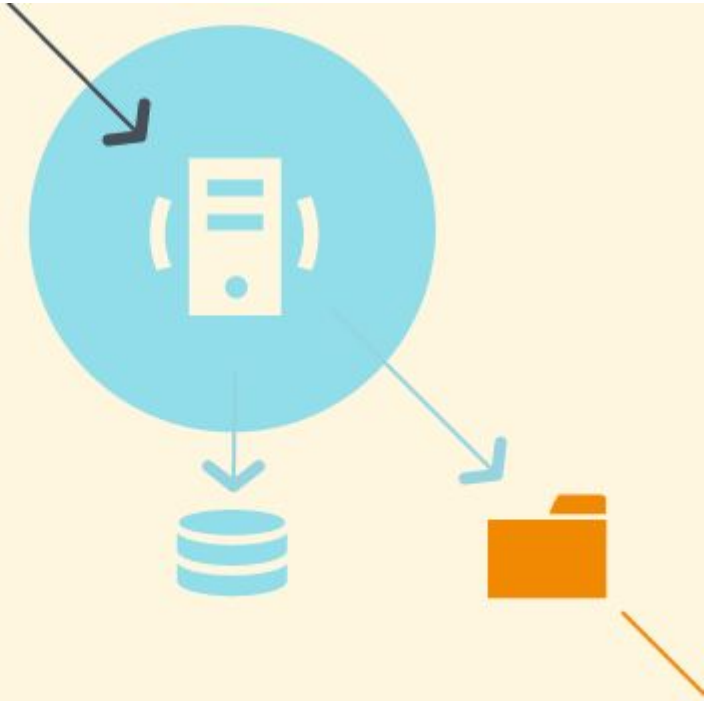
- Daný svobodně
- Konkrétní
- Informovaný
- Jednoznačný
- Vyjádření přání

Souhlas rodiče

- Do 16 let
- Nižší věk (podle práva členského státu)
- Minimálně 13 let

EVA ŠKORNICKOVÁ

Zpracování *osobních údajů*



Jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí nebo bez pomoci automatizovaných postupů spočívající v:

- Shromáždění
- Zaznamenání
- Uspořádání
- Strukturování
- Uložení
- Přizpůsobení nebo pozměnění
- Vyhledání
- Nahlédnutí
- Použití
- Zpřístupnění přenosem
- Šíření nebo jakékoliv jiné zpřístupnění
- Seřazení či zkombinování
- Omezení
- Výmaz nebo zničení

EVA ŠKORNICKOVÁ

článek 4 (2)

Věcná působnost zpracování *osobních údajů*

- Automatizované zpracování
- Manuální zpracování
- Data jsou obsažena v evidenci nebo do ní mají být zařazena

Výjimky:

- Při výkonu činností, které nespadají do působnosti práva EU (např. aktivity v rámci národní bezpečnosti)
- Kontrola hranic, azylové a imigrační řízení, veřejná bezpečnost
- Zpracování fyzickou osobou v rámci osobních a domácích činností
- Příslušnými orgány za účelem vyšetřování a odhalování trestných činů

Kdy je potřeba pamatovat *na osobní data?*

- Výběrové řízení
- Pracovní smlouva a výkon práce
- Skončení pracovního poměru
- Předávání v rámci skupiny
- Monitoring zaměstnanců

Výběrové *řízení*

Povinnost zajišťovat:

1. rovné zacházení se všemi FO (uchazeči o zaměstnání)
2. rovné příležitosti všem FO (uchazečům o zaměstnání)

- Zaměstnavatel smí vyžadovat pouze údaje bezprostředně související s uzavřením pracovní smlouvy (§ 30 odst. 2 ZP)
- Zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace, které (zákon o zaměstnanosti):
  - neslouží k plnění povinnosti zaměstnavatele
  - odporují dobrým mravům
  - se týkají národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu se zvláštním právním předpisem
- Background check - ne, pokud není speciální věcný důvod
- Předchozí reference - ano (souhlas není nutný)
- Sociální sítě, vstupní dotazníky

EVA ŠKORNICKOVÁ

Výběrové *řízení*

Co smí zaměstnavatel po uchazeči požadovat?

- potvrzení o posledním zaměstnání
- doklady o kvalifikaci, doklady ke mzdě
- trestní rejstřík (pokud vyžadováno zákonem nebo pokud je k tomu důvod)
- doklad o zdravotní způsobilosti (ne lékařské zprávy)
- cokoli dalšího, co je stanoveno zvláštními zákony

Co se nesmí?

- nesmí se pořizovat kopie občanského průkazu bez souhlasu zaměstnance/uchazeče
- jinak přestupek FO (ne zaměstnavatele)
- pokuta 10.000 Kč
- doporučuje se, aby zaměstnanec napsal na kopii, že s pořízením kopie souhlasí

EVA ŠKORNIČKOVÁ

Osobní data
v pracovním poměru

Trvání pracovního poměru

- obsah pracovní smlouvy
- vedení osobního spisu
- vedení databáze zaměstnanců, kterým se poskytují služby nebo zboží
- fotografie zaměstnanců
- whistleblowing policy
- omezení požadovat informace
    - zaměstnavatel nesmí od zaměstnance požadovat informace, které bezprostředně nesouvisí s prací (§ 316 odst. 4 ZP)
    - zaměstnavatel nesmí vyžadovat informace zejména o

        - těhotenství, rodinných a majetkových poměrech
        - sexuální orientaci
        - původu
        - členství v odborech, politických stranách nebo hnutích
        - příslušnosti k církvi nebo náboženské společnosti
        - trestněprávní bezúhonnosti

Pracovní poměr
- pracovní smlouva

Souhlas se zpracováním osobních údajů – NE!

- porušení informační povinnosti (stanovisko Úřadu)
- působí klamavě vůči zaměstnanci
- souhlas – jednostranné jednání zaměstnance, ne dohoda
- personální a mzdová agenda – kryto zákonem
- pokud zpracování nad rámec zákona
- souhlas nutný, ideálně ve zvláštním odděleném dokumentu

Nástup do práce

- vstupní dotazník - lze jím splnit informační povinnost
- osobní spis
- oznamovací povinnost vůči příslušným úřadům

EVA ŠKORNICKOVÁ

Osobní spis
– údaje související s pracovním poměrem

Slouží k plnění povinnosti zaměstnavatele:

- údaje ohledně odměňování včetně bonusů
- informace/souhlas se zpracováním
- informace o tom, do jaké kategorie byla práce zaměstnance zařazena
- informace o zdravotnickém zařízení (preventivní péče)
- potvrzení o absolvovaných školeních v oblasti BOZP
- potvrzení o seznámení s pracovním řádem, kolektivní smlouvou, vnitřními předpisy
- údaje o pracovních úrazech a nemocech z povolání
- údaje o disciplinárních řízeních (výzvy, upozornění, jejich řešení)

Fotografie

Fotografie zaměstnanců ve spisu nebo na vstupní kartě (průkazu):

v obecné rovině jde (dle Úřadu) o zpracování v rámci plnění povinností zaměstnavatele

Fotografie na firemním intranetu/internetu

- platí obecné principy
- není zvláštní zaměstnanecká úprava
- není vyžadováno zákonem (jde o zpracování nad rámec)
  - souhlas zaměstnance
  - informační povinnost
  - oznámení (registrace) Úřadu
  - účel (např. podpora komunikace), pozor – ideálně, aby kryl i marketingové materiály, teambuilding, apod.

Skončení *pracovního poměru*

- **Osobní spis (revize)**
  - změna účelu zpracování (již ne administrace personálně-mzdové agendy)
- **Oprávnění uchovávat osobní údaje**
  - pro ochranu práv zaměstnavatele (spory)
    - promlčení peněžitých nároků (3 roky)
    - rozsah uchovaných osobních dat omezen na daný účel (potřeba projít spis, ponechat - pouze potřebné dokumenty)
    - souhlas není nutný - nezbytné pro ochranu práv a zájmů zaměstnavatele
    - Úřad v praxi akceptoval i delší lhůty uchování dle vnitřního skartačního řádu
  - nabídky dalšího zaměstnání
- **Vydání potvrzení o zaměstnání, pracovního posudku (na žádost zaměstnance), splnění oznamovací povinnosti vůči státním institucím**

Skončení *pracovního poměru*

Archivace dokumentů

povinnost dle zvláštních právních předpisů, např.:

- evidenční listy důchodového pojištění (stejnopisy, 3 kalendářní roky)
- mzdové listy nebo účetní záznamy o údajích potřebných pro důchodové pojištění (originály, 30 a 10 kalendářních let)
- záznamy o poživatelích důchodu (10 kalendářních let)
- záznamy o zaměstnancích účastných nemocenského pojištění (10 kalendářních let)
- doklady o vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a nemocech z povolání, záznamy o evidenci pracovní doby (30? kalendářních let)
- účetní podklady (5 kalendářních let)
- od roku 2009 nemusí povinně soukromé subjekty uchovávat zásadní dokumenty o zaměstnaneckých záležitostech (povinnost vypadla ze zákona o archivnictví)
- jinak likvidace (např. vymazání, zničení) osobních údajů
- od 2007 (ZP) nemá zaměstnavatel povinnost vydat písemnosti týkající se jeho osobních údajů

Monitoring *zaměstnanců*

Právo zaměstnavatele na kontrolu zaměstnanců a ochranu majetku

- kontrola výkonu, efektivity a BOZP
- kontrola využívání prostředků zaměstnavatele
- ochrana majetku a informací

> **„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci."**

Právo zaměstnance na soukromí a ochranu osobních údajů

- ZP § 316, GDPR / výjimka – zvláštní povaha činnosti zaměstnavatele
- Informační povinnost

EVA ŠKORNICKOVÁ

Marketingové souhlasy

– pravidla pro marketingové sdílení informací

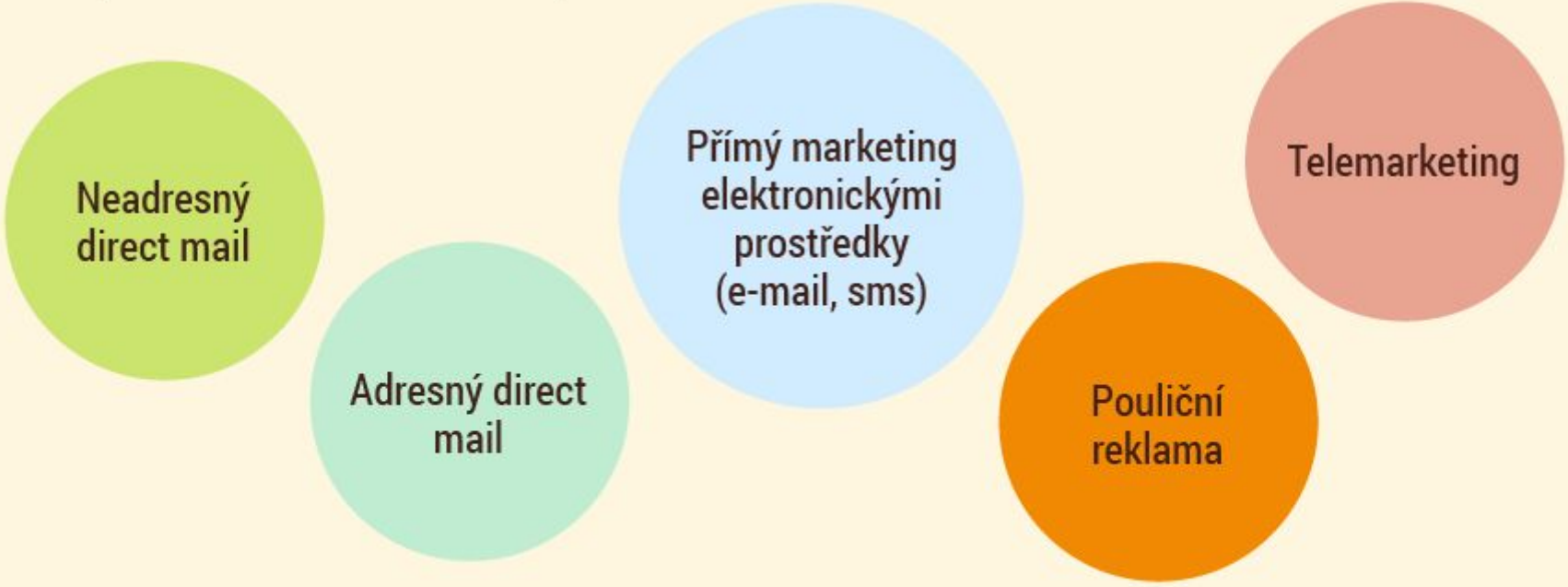
EVA ŠKORNICKOVÁ

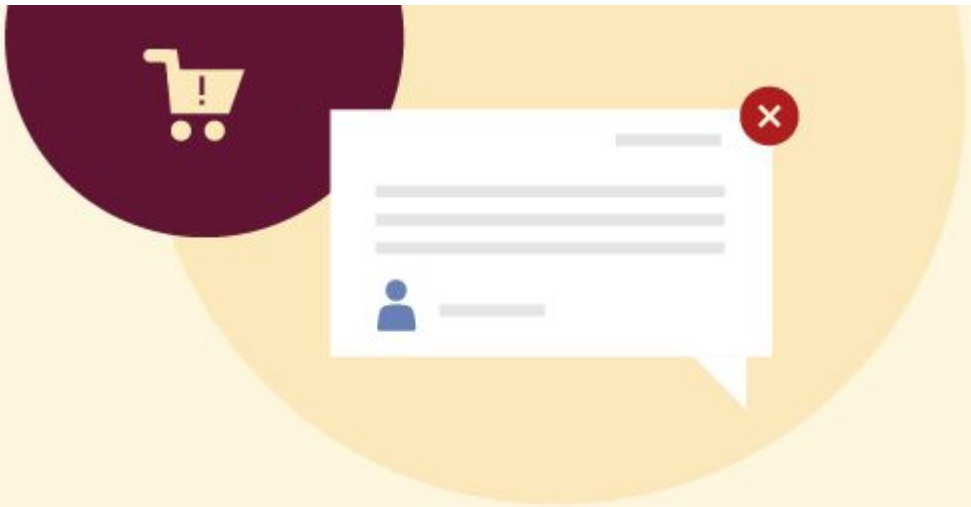
Direct marketingové nabídky

Neexistuje ucelená právní úprava

- nutná aplikace několika právních předpisů

Direct marketing – vždy reklamou
(zákon o regulaci reklamy)





Obchodní sdělení
(elektronicky)

Platí následující:

- V každé zprávě musí být začleněna možnost zdarma nebo na účet odesílatele odmítnout další zasílání reklam (včetně kontaktu na odesílatele)
- Režim opt-in (adresát musí udělit předchozí informovaný prokazatelný souhlas)
- U sms (např. uvedení linku na internetu, kde se dá odhlásit nebo zaslaní specifického kódu)
- Zákaz utajení identity odesílatele jehož jménem se zpráva posílá
- Zpráva musí být označená jako obchodní sdělení

EVA ŠKORNICKOVÁ

Využití elektronických kontaktů
z klientských vztahů

- Společnost musí získat e-mail od svého klienta v souvislosti s prodejem výrobku nebo služby
- Klientovi musí být v rámci el. komunikace nabízeny pouze obdobné výrobky nebo služby
- Klient má možnost při každém zaslání zprávy tuto odmítnout (opt-out)
- Obtěžování nevyžádaným obchodní sdělením:
  - žádost o ukončení
  - podnět na ÚOOÚ - jednoduchý formulář, vysoké sankce

Klient měl (při získání kontaktu / uzavření smlouvy)
možnost takové využití el. kontaktu odmítnout
a neodmítl

EVA SKORNICKOVÁ

Přímý marketing
v GDPR

Neposkytuje komplexní úpravu, upravuje pouze dílčí otázky (4):

- **Recitál 38** – zvláštní ochrana osobních údajů dětí
- **Recitál 47** – přímý marketing jako oprávněný zájem?

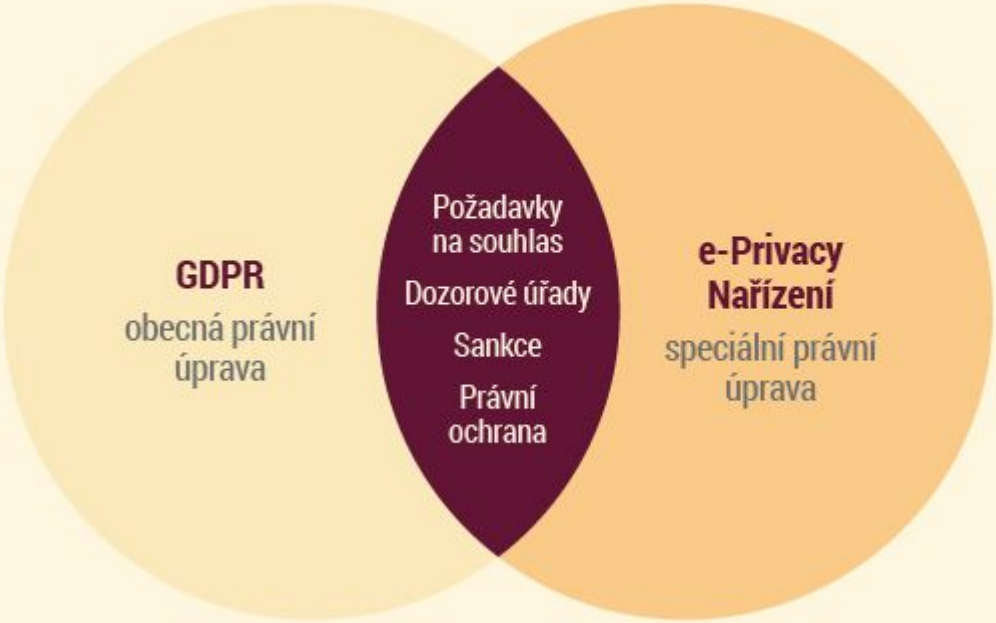
  … „Oprávněným zájmem dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům. Zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu".
- **Recitál 70** – právo vznést námitku
- **Článek 21 odst. 2 a 3** – právo vznést námitku

  „Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu."

  „Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány."

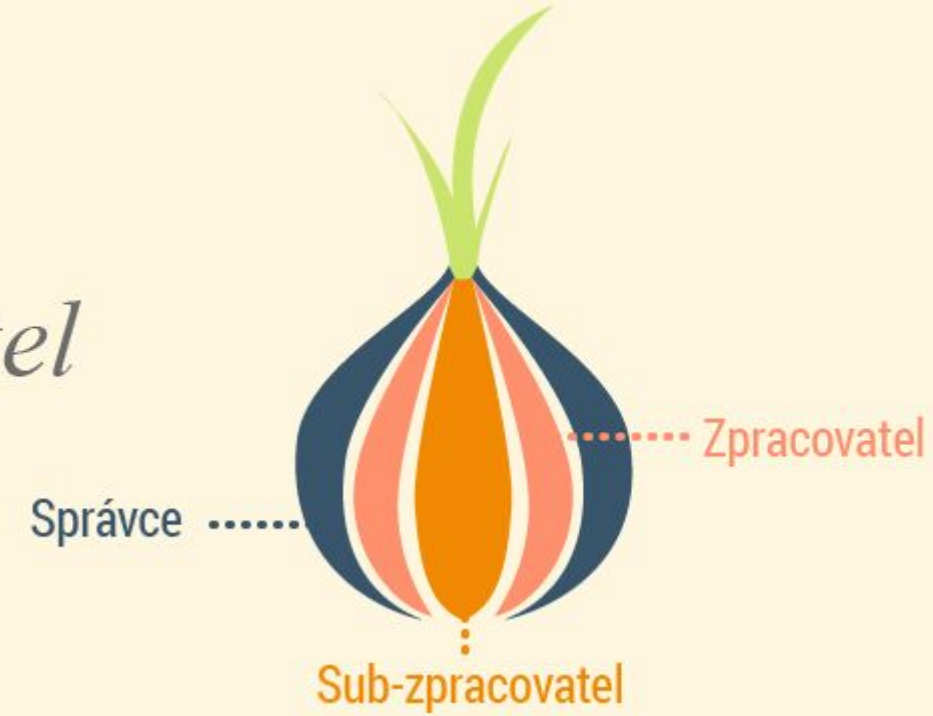
EVA SKORNICKOVÁ

Návrh nařízení
ePrivacy



- návrh ze dne 10. ledna 2017
- 29 článků, nové definice
- má regulovat povinnosti a práva související se sběrem, nakládáním a využíváním dat koncových uživatelů (netýká se uzavřených sítí uvnitř firem)
- má se vztahovat na všechny poskytovatele služeb el. komunikací, tj. i na nové typy služeb (tzv. over the top, OTT services – Skype, WhatsApp, Viber, Facetime, herní komunikační kanály, e-shopy, atd.)
- důvěrnost komunikace (komunikace + metadata)
- zjednodušení pravidel pro cookies

Správce
a Zpracovatel



Zpracovatel:

Fyzická nebo právnická osoba, která zpracovává data jménem správce

Správce:

Fyzická nebo právnická osoba, která sama nebo spolu s jinými určuje účel a způsoby zpracování

EVA ŠKORNICKOVÁ

Bezpečnost zpracování *osobních údajů*

Správce a zpracovatel jsou povinni provést:

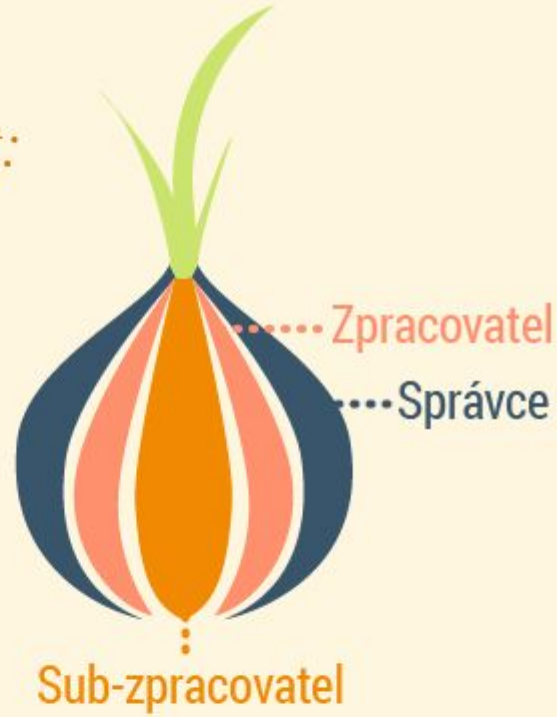
- Vhodná technická a organizační opatření

Aby zajistili

- Úroveň zabezpečení odpovídající danému riziku

S přihlédnutím

- Ke stavu techniky
- Nákladům na provedení
- Povaze, rozsahu, kontextu a účelům zpracování



Způsob zabezpečení zpracování dat by mělo být přesně upraveno ve smlouvě mezi správcem a zpracovatelem.

Porušení ochrany dat
musí být oznámeno

Nový zákon zavádí požadavek na podání oznámení o porušení ochrany:

- Správcům, pokud jste zpracovatelem dat
- Regulátorům do 72 hodin, pokud jste správcem - článek 33
- Postiženým subjektům dat v případě vysokého rizika - článek 34

Porušení ochrany osobních dat je

- Porušení bezpečnosti
- Vede k náhodnému nebo nezákonnému

  Zničení / Ztrátě / Změně

  Nepovolenému odhalení / Přístupu

Způsob a pravidla oznámení by měla být součástí interních směrnic a posouzení vlivu (PIA)

EVA ŠKORNICKOVÁ

Značně rozšířený *dosah*

Nový zákon platí pro:

- Podnik v EU
- Nabídku zboží a služeb rezidentům EU
- Monitorování chování rezidentů EU

Práva subjektů osobních údajů
- *výrazně posílena*

1. Přístup
2. Oprava
3. Výmaz a “právo být zapomenut”
4. Omezení zpracování
5. Přenositelnost údajů
6. Vznést námitku

Vztahuje se na všechny osobní údaje včetně tzv. nestrukturovaných, tj. uložených např. v přílohách k e-mailu, na různých úložištích

Toto právo může být ze strany nespokojených zákazníků nebo zaměstnanců zneužíváno!

OZNÁMENÍ (PRIVACY NOTICE) - měl by upravovat postup, jakým může subjekt osobních údaju uplatnit svoje práva

EVA ŠKORNICKOVÁ

Informační povinnost

osobní údaje získány od subjektu údajů

Stručně, srozumitelně, transparentně

Informovat subjekt údajů **v okamžiku jejich získání** o těchto skutečnostech:

- Kontaktní údaje správce, případně Pověřence
- Účel zpracování a právní titul
- Příjemce nebo kategorie příjemců osobních údajů
- Doba zpracování
- Důsledky neposkytnutí údajů
- Existence práva podat stížnost u dozorového úřadu
- Skutečnost, že dochází k automatizovanému rozhodování včetně profilování

Informační povinnost

osobní údaje nebyly získány od subjektu údajů

Stručně, srozumitelně, transparentně

Informovat subjekt údajů **v přiměřené lhůtě, nejpozději do jednoho měsíce nebo při prvním zpřístupnění údajů nebo v okamžiku komunikace se subjektem údajů** o těchto skutečnostech:

- Kontaktní údaje správce, případně Pověřence
- Účel zpracování a právní titul
- Příjemce nebo kategorie příjemců osobních údajů
- Doba zpracování
- Důsledky neposkytnutí údajů
- Existence práva podat stížnost u dozorového úřadu
- Skutečnost, že dochází k automatizovanému rozhodování včetně profilování
- Zdroj, ze kterého osobní údaje pochází včetně veřejně dostupných zdrojů

EVA SKORNICKOVA

Článek 14

1. Přístup

Jedná se o absolutní právo s vyjímkou případů stanovených v článku 23

K následujícím informacím:

- KDO: příjemce, kterým budou osobní údaje zpřístupněny včetně třetích zemí
- CO: kategorie dat
- KDE: kde jsou osobní údaje zpracovávány
- JAK DLOUHO: doba, po kterou budou osobní údaje uloženy, případně určení kritéria ke stanovení této doby
- PROČ: účel zpracování

- Jak podat stížnost u dozorového úřadu
- O zdroji osobních údajů, pokud nejsou poskytnuty samotnými subjekty
- Skutečnosti, že dochází k automatizovanému rozhodování včetně profilování
- Existenci práva požadovat od správce opravu nebo výmaz údajů, omezení jejich zpracování nebo vznést námitku proti zpracování

Správce musí poskytnout kopii zpracovávaných údajů ve formě, kterou je žádost podána, včetně elektronické

2. Oprava

- Bez zbytečného odkladu
- Oprava objektivně nepřesných údajů - např. špatně uvedené jméno subjektu
- Oprava subjektivně nepřesných údajů - např. založených na základě názoru, subjekt osobních údajů má právo názoru na např. osobní hodnocení

3. Výmaz *a právo být zapomenut*

Výmaz

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány
- Subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další důvod pro zpracování
- Subjekt údajů vznese námitku proti zpracování z důvodu oprávněných zájmů správce
- Osobní údaje byly zpracovány protiprávně
- Právní povinnost stanovená právem Unie nebo členským státem
- Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí

Právo být zapomenut

- Rozšíření práva výmazu
- Přiměřené kroky správce informovat další správce o vymázání odkazu, jejich kopie nebo replikace

EVA SKORNICKOVÁ

Článek 17

4. Omezení *zpracování*

Omezení zpracování = označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu - např. systém ve společnosti (SAP) musí tuto funkci již mít zabudovanou - viz "Privacy by design"

Spočívající např. v:

- Data budou dočasně nedostupná
- Restrikce zpracování bude v systému zabudována
- Přenesení dat do separátního systému
- Dočasné zablokování webové stránky
- Data budou pouze uložena

Jedná se v podstatě o alternativní řešení k právu být vymazán.

Důvody omezení:

- Subjekt dat popírá přesnost údajů
- Zpracování je protiprávní, subjekt odmítá výmaz a žádá místo něho omezení
- Subjekt vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad důvody subjektu

5. Přenositelnost *údajů*

- Rozšířené právo přístupu
- Musí být splněny současně tyto 2 podmínky
  - Zpracování je založeno na souhlasu subjektu údajů nebo na smlouvě
  - Zpracování se provádí automatizovaně
- Subjekt údajů má právo získat svoje údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci bez souhlasu původního správce
- Výjimky: zpracování nezbytné ve veřejném zájmu nebo při výkonu veřejné moci

6. Vznést *námitku*

Nejedná se o absolutní právo, musí být splněny následující podmínky -

Výslovné upozornění

Veřejný nebo oprávněný zájem správce

- Zpracování údajů se provádí ve veřejném zájmu nebo z důvodu oprávněných zájmů správce
- Zpracování údajů se týká konkrétní situace subjektu
- Správce musí prokázat, že jeho oprávněné zájmy převažují nad právy subjektu

Přímý marketing

- Subjekt údajů má vždycky právo (absolutní) vznést námitku proti tomuto zpracování včetně profilování - tzv. Opt-out

Vědecký, statistický a historický výzkum

- Právo vznést námitku z důvodů týkajících se konkrétní situace s vyjímkou zpracování z důvodu veřejného zájmu

Profilování

- *Automatizované zpracování osobních dat*
- *Zejména analyzovat nebo předpovídat:*
  - Výkon v práci
  - Ekonomickou situaci
  - Zdraví
  - Osobní preference
  - Zájmy
  - Spolehlivost
  - Chování
  - Polohu
  - Pohyb

EVA SKORNICKOVÁ

Článek 22 a 4/4

Profilování

Právo subjektu odmítnout profilování, resp. musí k němu udělit souhlas

- Profilování má pro něho právní účinky nebo se ho významně dotýká
- Výjimky:
  - Zpracování je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem - např. vyhodnocování pojistných rizik
  - Zpracování je povoleno právem Unie nebo členského státu
  - Zpracování je založeno na výslovném souhlasu subjektu

Příklady profilování:

- "Adware" a "freeware" - software instalovaný na počítači uživatele umožňující monitorování jeho chování za účelem cílené reklamy
- "Cookie" - část textu, který je uložen z webové stránky na hard disku uživatele a v případě další návštěvy je znovu použit - např. počet položek uložených v košíku při nákupu na e-shopu, automatické ukládání navštívených webů, zapamatování si hesel, čísla kreditních karet, autentizačních údajů, apod.

Zodpovědnost

- *Vhodná technická, organizační a procesní opatření k prokázání souladu (compliance)*
- *Mohou zahrnovat:*
  - Vyhodnocení dopadu na soukromí
  - Záměrná a nezbytná ochrana dat (Privacy by Design/by Default)
  - Implementace procedur na ochranu dat
  - Jmenování DPO
  - Pseudonymizace osobních dat
  - Povinnost uchovávání záznamů u správců a zpracovatelů
  - Spolupráce správců a zpracovatelů s dozorovými orgány

Zodpovědnost:
Posouzení vlivu na ochranu osobních údajů

DPIA = Data Protection Impact Assessment - nutný v těchto případech:

- Systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se osob, které je založeno na automatizovaném zpracování, profilování
- Vysoké riziko pro práva a svobody fyzických osob, závažný dopad na fyzické osoby
- Rozsáhlé zpracování citlivých dat
- Rozsáhlé systematické monitorování veřejně přístupných prostorů

Obsah DPIA:

- Popis zamýšlených operací zpracování
- Posouzení nezbytnosti a přiměřenosti operací z hlediska účelu
- Posouzení rizik pro práva a svobody subjektů
- Plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření

Povinnost předchozí konzultace s dozorovým orgánem

EVA ŠKORNICKOVÁ

Článek 35
vysvětlivky 84, 90-93

Zodpovědnost:
Záměrná a standardní ochrana dat

Záměrná ochrana data - tzv. By design

- Implementace vhodných organizačních a technických opatření v době určení prostředků pro zpracování, tak i v době samotného zpracování
- Vhodná opatření jsou do systému ochrany přímo integrována, např. pseudonymizace, minimalizace dat

Standardní ochrana dat - tzv. By default

- Zpracování pouze osobních údajů, které jsou pro každý konkrétní účel nezbytné - množství dat, rozsah zpracování, doba jejich uložení a jejich dostupnosti

Zodpovědnost:
Záznamy o činnostech zpracování

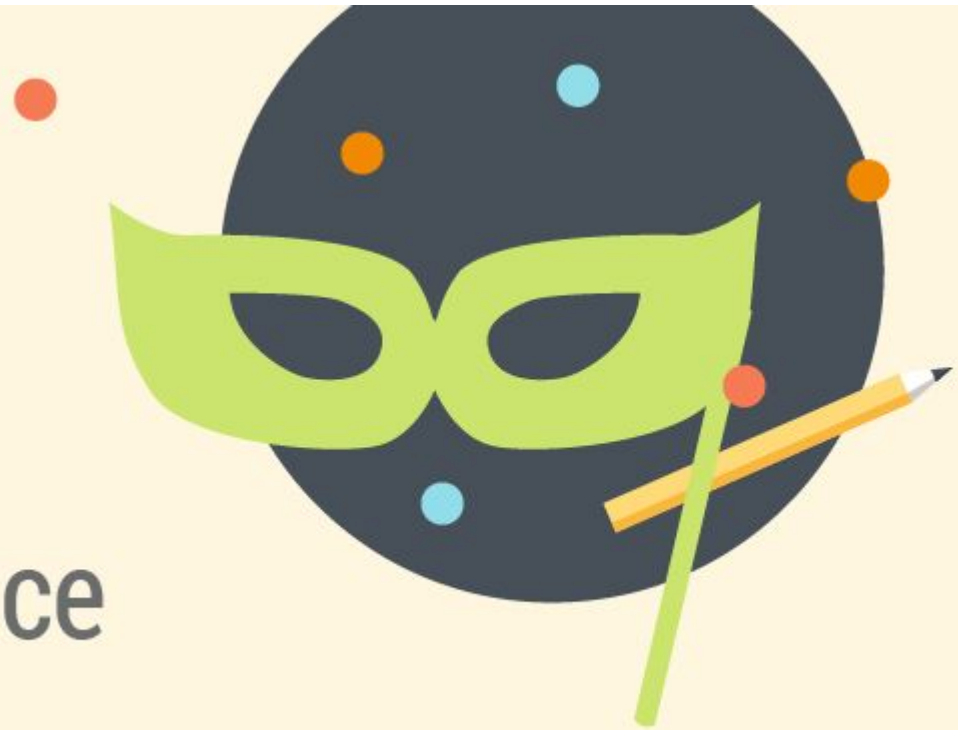
Správce a zpracovatel jsou povinni vést záznamy o činnostech zpracování:

- Jméno a kontaktní údaje správce a zpracovatele včetně jména DPO
- Účely zpracování
- Popis kategorií subjektů údajů a kategorií osobních údajů
- Kategorie příjemců, kterým byly nebo budou údaje zpřístupněny včetně 3. zemí
- Informace o mezinárodním předávání osobních údajů
- Lhůty pro výmaz jednotlivých kategorií údajů
- Popis technických a organizačních opatření

Záznamy musí být na požádání poskytnuty dozorovému orgánu.

Výjimky:

- Pro organizaci s méně než 250 zaměstnanci, pokud zpracování dat není jejich hlavní činností
- Neexistuje riziko pro práva subjektů dat
- Nejsou zpracovávány citlivé údaje



Pseudonymizace

Zpracování takovým způsobem:

- Aby data již nemohla být přiřazena ke konkrétnímu subjektu dat
- Bez použití dalších informací
- Dokud jsou tyto informace uchovávány samostatně a podléhají opatřením

EVA SKORNICKOVÁ

Zodpovědnost:

Povinný pověřenec pro ochranu osobních údajů (DPO)

Požadavek na správce a zpracovatele

Hranice pro jmenování:

- Povinný pro veřejné orgány
- Rozsáhlé systematické monitorování fyzických osob
- Rozsáhlé zpracování citlivých dat

Úkoly:

- Monitorování souladu
- Řízení činností interní ochrany dat
- Školení pracovníků ve zpracování dat
- Provádění interních auditů

EVA ŠKORNICKOVÁ

Článek 37 - 39

Zodpovědnost:
Povinný pověřenec pro ochranu osobních údajů (DPO)

- Musí být expertem v oblasti ochrany dat - prozatím nejasné a nespecifikované kvalifikační předpoklady
- Přímo je podřízen nejvýše postavené osobě v dané společnosti, nemůže být součástí právního či jiného oddělení
- Neměl by být v kumulované funkci, střet zájmů
- Skupina podniků může jmenovat jediného DPO, ale musí být snadno dosažitelný a schopen komunikovat s dozorovým orgánem
- Může být buď interním pracovníkem nebo externím na základě smlouvy o poskytování služeb

Dozorové *orgány*

Nezávislý orgán veřejné moci - role:

- Reprezentuje členský stát v Evropském sboru pro ochranu osobních údajů (EDPB)
- Spolupracuje s ostatními dozorovými orgány
- Monitoruje uplatňování GDPR
- Usnadňuje volný pohyb osobních údajů uvnitř EU
- Chrání základní práva a svobody fyzických osob

Pravomoci: článek 58

- Vyšetřovací
- Nápravné
- Povolovací a poradní

Eva Škornická

Článek 4/21,22
a 51-76

Právní ochrana
a sankce

- Každý subjekt dat má právo podat stížnost u dozorového úřadu dle svého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k porušení ochrany jeho dat
- Každý subjekt dat má právo na soudní ochranu - žaloba podána u soudu dle sídla provozovny správce nebo zpracovatele

Sankce

- Náhrada hmotné či nehmotné újmy od správce nebo zpracovatele - společná odpovědnost všech zapojených subjektů (obrázek "cibule") - na základě rozhodnutí příslušného soudu
- Správní pokuty udělené dozorovým úřadem
- Jiné sankce - stanovené pravidly členského státu - musí být účinné, přiměřené a odrazující i pro případ, kdy právo členského státu neumožňuje uložení správních pokut (Estonsko)
- Trestní odpovědnost právnických osob

Kam až může GDPR dosáhnout

v rámci organizace

Osobní informace

- Elektronické
- Listinné

Souhlasy

CRM

ERP

COM

HRM

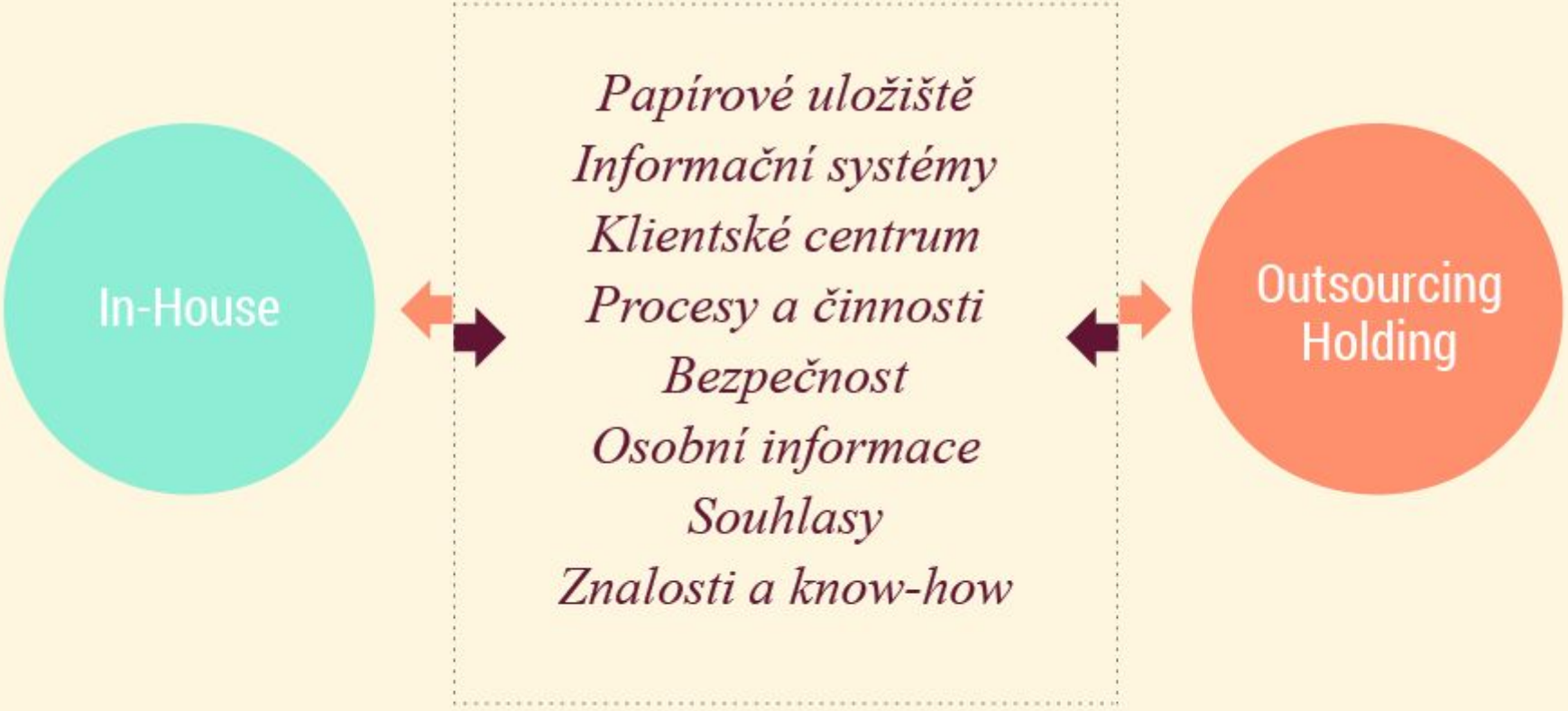
ZIS

...

- Bezpečnostní odd.
- Finanční odd.
- IT a Technické odd.
- Klientské odd.
- Legislativní a právní odd.
- Logistické a výrobní odd.
- Marketingové odd.
- Obchodní odd.
- Personální odd.

EVA ŠKORNICKOVÁ

Rozsah oblastí
s možným dopadem GDPR



EVA ŠKORNICKOVÁ

Oblasti dopadu
regulace

Obchodní procesy

- Většina prováděných

Podpůrné procesy

- Návštěvy
- Archivace
- Skartace
- Zálohování

Dokumenty

- Smlouvy (pracovní vztahy, dodavatelé)
- Obchodní podmínky
- Interní předpisy

IT systémy

- Aplikace
- Web
- Reporty
- Úložiště (i stanice)
- Archivy
- Zálohy

EVA ŠKORNICKOVÁ

Obohacená vazba
(Business, Technologie) - příklad

Statický model – čas (doba životnosti)

Proces	Aktivita	Účel	Právní důvod	O.Ú.	IT systémy	Zdroje dat
Obchodní proces	Shromažďování údajů - údaje pojistníka - údaje pojištěného - údaje zprostředkovatele - Údaje lékaře Modelace ceny - údaje pojistníka - údaje pojištěného	Uzavření smlouvy	Plnění smlouvy Plnění právních povinností Převažující oprávněný zájem nad subjektem	Jméno a další jméno Příjmení Rodné příjmení Rodné číslo Datum narození Místo narození Pohlaví Stát narození Státní příslušnost Stát daňové rezidence Titul před jménem Titul za jménem Typ dokladu Kopie dokladu Číslo dokladu Platnost dokladu	APP1	DB1

EVA ŠKORNICKOVÁ

Jak by mohl vypadat konečný výsledek

(na jednu FO)

Proces	Aktivita	Účel	Právní důvod	O.Ú.	IS	Zdroj	Expirace
Uzavření smlouvy	Shromažďování údajů - údaje pojistníka - údaje pojištěného	Uzavření smlouvy s klientem	Plnění smlouvy	Jméno Příjmení Rodné číslo Datum narození Místo narození Stát narození Státní příslušnost Typ dokladu Kopie dokladu Číslo dokladu Platnost dokladu	APP1	DB1	1. 1. 2019
Uzavření smlouvy	Shromažďování údajů - údaje zprostředkovatele	Vyplacení zprostředkovatelské provize na základě smlouvy	Plnění smlouvy	Jméno Příjmení Rodné číslo Typ dokladu Číslo dokladu Banka Číslo účtu	APP1	DB1	1. 6. 2019
Uzavření smlouvy	Shromažďování údajů - údaje lékaře	Splnění zdravotních předpokladů	Převažující oprávněný zájem nad subjektem	Název lékaře ID Doklad Datum vystavení			1. 1. 2020
Uzavření smlouvy	Shromažďování údajů - plátce	Fakturace	Plnění právních povinností	Stát daň. Rez. Daň. doklad DIČ	APP3	DB3	1. 1. 2029

Funkční požadavky na software
- *výmaz*

- **Možnost propojit subjekt na základě jednotného identifikátoru (primary key) pro různé systémy**
  V rámci implementace systémového řešení pro katalogizaci osobních údajů realizovat možnost jednotného identifikátoru pro dohledání konkrétního subjektu a všech jeho zpracovávaných osobních údajů. Zvolit primární klíč, na základě kterého bude možné vyhledat/vymazat/upravit veškeré osobní údaje dotčeného subjektu (nebo jen jejich část).

- **Možnost procesovat žádost o výmaz**
  Implementovat možnost procesování žádosti o výmaz. Sjednotit výše uvedené funkcionality, kde bude možné vyhledat všechny osobní údaje dotčeného subjektu a označit je k vymazání.

- **Zavést kontrolu procesu a oprávněnosti výmazu odpovědnými osobami**
  Implementovat možnost notifikace na workflow systém a vazbu na proces schválení.

- **Možnost notifikace administrátorů systémů, kde bude docházet ke skutečným výmazům (proces, workflow)**
  Implementovat možnost zaslat notifikaci se žádostí o výmaz administrátorům všech systémů, kde se bude uskutečňovat výmaz. (Označení všech osobních údajů nebo jen některých, podle toho, zda se jedná o celkový výmaz, nebo jen odstranění těch osobních údajů, k nimž byl odebrán souhlas.)

- **Možnost uskutečnění výmazu kompletních osobních údajů**
  Implementovat možnost vyhledání pomocí jednotného identifikátoru a označení/notifikace všech osobních údajů určených k vymazání.

GDPR a nové požadavky na IT

aneb příprava na těžko řešitelné požadavky

Aktuálně palčivé otázky ne/jen pro IT:

- Umíme vést záznamy zpracování, kde zpracováváme?
- Pod který účel které zpracování náleží a po jakou dobu?
- Jaká množina osobních údajů je pro účel aktuálně potřebná?
- Známe obsažené subjekty / typy subjektů údajů u jednotlivých zpracování?
- Víme které zdroje obsahují aktuálně které kategorie údajů (bezpečnostní incidenty)?
- Máme přehled nad aktuálním rizikem pro subjekty údajů?
- Jsme schopni veškeré naše úvahy, kroky a návaznosti doložit a čím?
- Jak jsme schopni implementovat případné kodexy?
- Jaké bezpečnostní incidenty umíme vyhodnotit a jak je zabezpečen postup jejich analýzy, případného forenzního zajištění a eskalace k vyhodnocení hlášení do 72hod.? A co DPO?
- Umíme zabezpečit všechna práva subjektů údajů?

EVA ŠKORNICKOVÁ

Přístup
k implementaci GDPR

Organizace musí zejména:

1. Upravit procesy a systémy tak, aby byly dodržovány principy zpracování prostřednictvím zejména „privacy by default“ a „privacy by design“;
2. Zajistit zpracování osobních údajů v souladu s ustanoveními GDPR, zejména se zásadami zpracování;
3. Upravit procesy umožňujících výkon nových práv subjektů údajů a informační povinností;
4. Upravit procesy a technologie v souladu s požadovanou bezpečností;
5. Nastavit procesy zjišťování a oznamování porušení zabezpečení OÚ a další povinnosti typu „compliance“;
6. Zřízení (po analýze) pozice pověřence pro ochranu osobních údajů (Data Protection Officer, „DPO“) a nastavení jeho úkolů, resp. zajištění výkonu funkce.
7. Připravit dokumentaci k doložení souladu s Obecným nařízením.

EVA ŠKORNICKOVÁ

Doporučený přístup
k zajištění shody s GDPR

- Zajištění shody s GDPR proto vyžaduje komplexní přístup. Nabídka služeb v rámci implementace GDPR pravidel se skládá z jednotlivých na sebe navazujících fází. S ohledem na skutečnost, že se aplikace GDPR pravidel dotkne celé organizace jako celku s výrazným dopadem na řadu interních činností a procesů, tak i tato nabídka vychází z nutnosti zapojení týmu expertů, kteří budou aplikaci pravidel nařízení řídit ve spolupráci s vrcholným managementem dané společnosti.

1. Definice rozsahu posuzování
2. Analýza stávajícího stavu zpracování osobních údajů
3. Příprava projektových záměrů a harmonogramu implementace
4. Realizace projektových záměrů

EVA ŠKORNICKOVÁ

1. Definice rozsahu posuzování

Před samotným vyhodnocováním potenciálních změn, které GDPR pro organizaci představuje, je nejprve nezbytné předběžně vyhodnotit stávající stav organizace v oblasti shromažďování, zpracovávání a užití osobních údajů a identifikovat činnosti a informační systémy organizace, na které může GDPR dopadat.

Cíl:

- Zúžit povinnosti GDPR na ty, které jsou pro organizaci relevantní
- Definovat rozsah projektu, jeho harmonogram a rozpočet

A *Úvodní školení*

Před samotnou analýzou stávajícího stavu zpracování osobních údajů bude v prvním kroku provedeno seznámení klíčových zaměstnanců organizace s problematikou GDPR.
Obsahem školení bude seznámení se základními změnami plynoucími z GDPR, představení základních povinností a představení postupu dalších prací.

1.

B *Definice rozsahu posuzování*

Druhým krokem bude definice rozsahu posuzování. Tento krok je důležitý proto, že na každou organizaci se budou vztahovat jiné povinnosti plynoucí z GDPR. Bez tohoto kroku by nebylo možné seriózně definovat rozsah projektu a tedy ani připravit harmonogram a rozpočet. Definice rozsahu posuzování bude provedena formou pracovních schůzek s cílem:

- identifikovat typy dat a vymezit pouze ta data, která mají charakter osobních údajů – vymezení rozsahu;
- identifikovat základní kategorie osobních údajů, způsoby a účel jejich zpracování;
- identifikovat přibližný objem osobních údajů;
- identifikovat nástroje informační podpory (IS, databáze, atd.), které jsou pro zpracovávání osobních údajů organizací používané;
- identifikovat základní povinnosti a roli organizace dle GDPR.

Výstup

Projektový záměr definující rozsah, harmonogram a rozpočet, který bude sloužit i jako nabídka expertního týmu.

2. Analýza stávajícího stavu zpracování osobních údajů

Cíl:

- Analyzovat povinnosti organizace plynoucí z GDPR a získat důkazy o jejich (ne)plnění
- Popsat rozdíly mezi současným stavem a stavem, kdy organizace plnění povinnosti plynoucí z GDPR

Tato fáze si klade za cíl provést základní rozbor společnosti prostřednictvím poskytnutých softwarových modulů a seznamu otázek, jehož výsledkem bude souhrnná zpráva expertního týmu s výčtem kritických bodů, identifikací a analýzou rizik a doporučených následných opatření k nápravě. Výsledná zpráva bude zpracována na základě klientem poskytnutých informací a materiálů a bude sloužit managementu společnosti jako podklad pro rozhodnutí o dalších krocích v realizační fázi.

A *Analýza povinností a shromáždění důkazů o jejich (ne)plnění*

Předmětem činností v rámci této analýzy bude:

- analýza zdrojů osobních údajů, právních titulů k jejich zpracování a způsobu jejich dokumentace;
- kategorizace typů osobních údajů;
- kategorizace způsobů zpracování a typů zpracovatelských operací;
- analýza životního cyklu dat;
- analýza interních a externích datových toků a způsobu jejich dokumentace;
- analýza interní legislativy popisující zpracování osobních údajů;
- analýza organizačních a technických opatření sloužících k zabezpečení informačních systémů;
- analýza dalších procesů relevantních pro GDPR (identifikace rizik, apod.).

Výstup

Souhrnná zpráva popisující rozdíly stávajícího stavu zpracování osobních údajů a stavu odpovídajícího legislativě GDPR. Zpráva bude obsahovat manažerské shrnutí a přehledné tabulky s jednotlivými zjištěními. Součástí výsledné zprávy bude právní, datový, bezpečnostní a procesní audit.

Právní audit

- S využitím speciálního softwarového modulu, který slouží k detailnímu zmapování interního nakládání s osobními údaji získáme ucelený přehled o současném účelu zpracování osobních údajů klientem, množství a charakteru osobních údajů, které má k dispozici a přehledu aktuálně používaných právních dokumentů a interních směrnic.
- Výsledkem právního auditu bude identifikace rizikových oblastí a činností, které budou muset být uvedeny do souladu s pravidly GDPR, doporučení sestavy dokumentů a směrnic odpovídajících požadavkům nařízení a vyhodnocení povinnosti jmenovat pověřence pro ochranu osobních údajů.
- Nedílnou součástí právního auditu jsou i firemní školení nebo workshopy coby úvod do problematiky nových požadavků na zpracování osobních údajů pro členy vrcholového managementu nebo jím pověřených osob, které budou následně rozhodovat o rozsahu implementace GDPR.

B *Rozdílová analýza*

Rozdílová analýza vychází z porovnání stávajícího stavu zpracování osobních údajů a stavu odpovídajícího legislativě GDPR.

Jednotlivé v analýze identifikované povinnosti budou popsány a ke každé povinnosti bude uveden závěr, zda je povinnost plněna, zda je plněna jen částečně, nebo zda plněna není. Vždy bude uveden odkaz na relevantní podkladový materiál, na základě kterého byl závěr učiněn a odkaz na článek nařízení GDPR, který povinnost ukládá.

Datový a bezpečnostní audit

- Tato analýza je zaměřena na zmapování výskytu osobních údajů fyzických osob napříč datovou infrastrukturou, tj. síťovými, cloudovými úložišti a různorodými databázemi klienta. Dojde ke zmapování technických HW a SW prostředků pro zpracování a přenosy dat včetně stavu jejich kybernetického zabezpečení, tzn. provozního a bezpečnostního monitoringu, dohledu, aktivních restriktivních a ochranných nástrojů, incident managementu a smluvního zajištění.V rámci analýzy proběhnou konzultace s vlastníky aktiv (osobních údajů) u klienta, v jejichž rámci dojde k identifikaci klíčových systémů, lokalit, oblastí a procesů práce s osobními údaji. Následnou implementací technického řešení na audit nakládání s osobními údaji proběhne u klienta monitoring toku dat po dobu cca 2 týdnů až 1 měsíce, jehož výsledkem bude analýza nasbíraných dat, jejich vyhodnocení a porovnání s procesy zákazníka.

- Výsledná datová analýza zachycených incidentů, potenciálních rizik a doporučení pro další kroky k řešení nalezených problémů bude součástí souhrnné auditní zprávy expertního týmu. Zpráva bude rovněž obsahovat k jednotlivým zjištěním a rizikům formulaci jak v oblasti práce s osobními daty, tak v oblasti jejich pokrytí bezpečnostními prvky ICT infrastruktury, doporučení technických a organizačních opatření k zajištění maxima možného při ošetření těchto rizik ve vazbě na požadavky GDPR.

3.

Příprava projektových záměrů a harmonogramu implementace

Cíl:

- Připravit projektové záměry, které budou obsahovat návrhy na eliminaci všech identifikovaných rozdílů mezi současným stavem a stavem odpovídajícím GDPR
- Připravit harmonogram implementace reflektující priority jednotlivých zjištění

A

Stanovení priorit

Zajištění souladu s GDPR je dlouhodobý proces. Prioritizace nejdůležitějších projektových záměrů proto napomůže zajistit maximální možnou shodu v co nejkratším čase. Priority realizace budou hodnoceny dle několika kritérií, mezi které patří například náročnost implementace, rizika implementace, nebo výše případné sankce za nesplnění povinnosti.

B

Příprava projektových záměrů

Rozdíly identifikované v rámci analýzy stávajícího stavu zpracování osobních údajů budou sloučeny do homogenních skupin, které budou představovat zadání projektu jehož cílem bude eliminace rozdílů. Na základě tohoto zadání budou zpracovány kroky, které je pro eliminaci rozdílů nutné provést a budou rovněž odhadnuty délky trvání jejich eliminace. Takto zpracované projektové záměry bude možné využít i jako zadávací dokumentaci. Ne všechny rozdíly však bude možné eliminovat (např. z důvodu časové nebo finanční náročnosti). Tyto rozdíly budou identifikovány jako tzv. reziduální rizika, které se organizace rozhodla akceptovat.

C

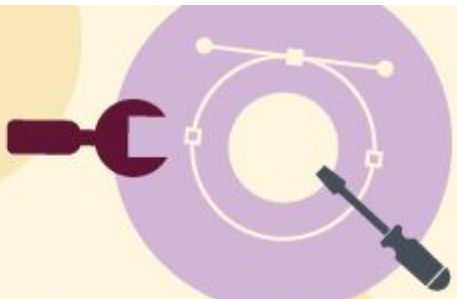
Implementační harmonogram

Jednotlivé projektové záměry budou obsahově tvořit ucelený projektový program. Časové závislosti mezi jednotlivými projektovými záměry budou zachyceny formou implementačního harmonogramu.

Výstup

Jednotlivé projektové záměry budou obsahově tvořit ucelený projektový program. Časové závislosti mezi jednotlivými projektovými záměry budou zachyceny formou implementačního harmonogramu.

4. Realizace projektových záměrů



Cíl:

- Zabezpečit realizaci jednotlivých projektových záměrů a tím zajistit shodu s GDPR

Realizace projektových záměrů je souhrn specifických řídících a odborných činností, které budou pro každou organizaci jiné, a které vyplývají z typů realizovaných projektových záměrů. Bez naplnění výše popsaných kroků nelze odhadnout ani jejich délku trvání, ani náklady na tyto činnosti.

Mezi tyto specifické řídící a odborné činnosti typicky patří:

- Zpracování dokumentu posouzení vlivu zpracování na ochranu osobních údajů dle § 35 odst. 1 GDPR, v souladu s požadavky stanovenými v § 31 odst. 7 a 8 GDPR;
- zabezpečení projektového řízení a podpory při realizaci projektových záměrů včetně řízení externích dodavatelů;
- zabezpečení technického dohledu nad implementací bezpečnostních opatření;
- zabezpečení technického dohledu nad revizemi ICT a bezpečnostní architektury;
- zajištění kapacit pověřence osobních údajů.

Všechny výše uvedené činnosti spolu s realizací vybraných projektových záměrů (typicky revize smluv, revize produktů, procesní změny) je možné zajisti rovněž externími kapacitami.

Výstup

Jednotlivé projektové záměry budou obsahově tvořit ucelený projektový program. Časové závislosti mezi jednotlivými projektovými záměry budou zachyceny formou implementačního harmonogramu.

Kdo s problematikou *může pomoci*

Varianta č.1

GDPR SuperExpert

Varianta č.2

Tým expertů GDPR

- Právo
- IT
- Procesy
- Bezpečnost
- Management

Minimální počet oblastí

Ideálním týmem jsou experti disponující průřezově znalostmi a dovednostmi z více než jedné oblasti. Pro jednotlivé oblasti následně zajistit specialisty s kombinací znalostí know-how GDPR.

EVA ŠKORNIČKOVÁ

EVA ŠKORNIČKOVÁ

Nejste v tom sami,
dejte mi vědět!

WWW.GDPR.CZ

+420 602 655 008 | eva@skornickova.eu | www.skornickova.eu