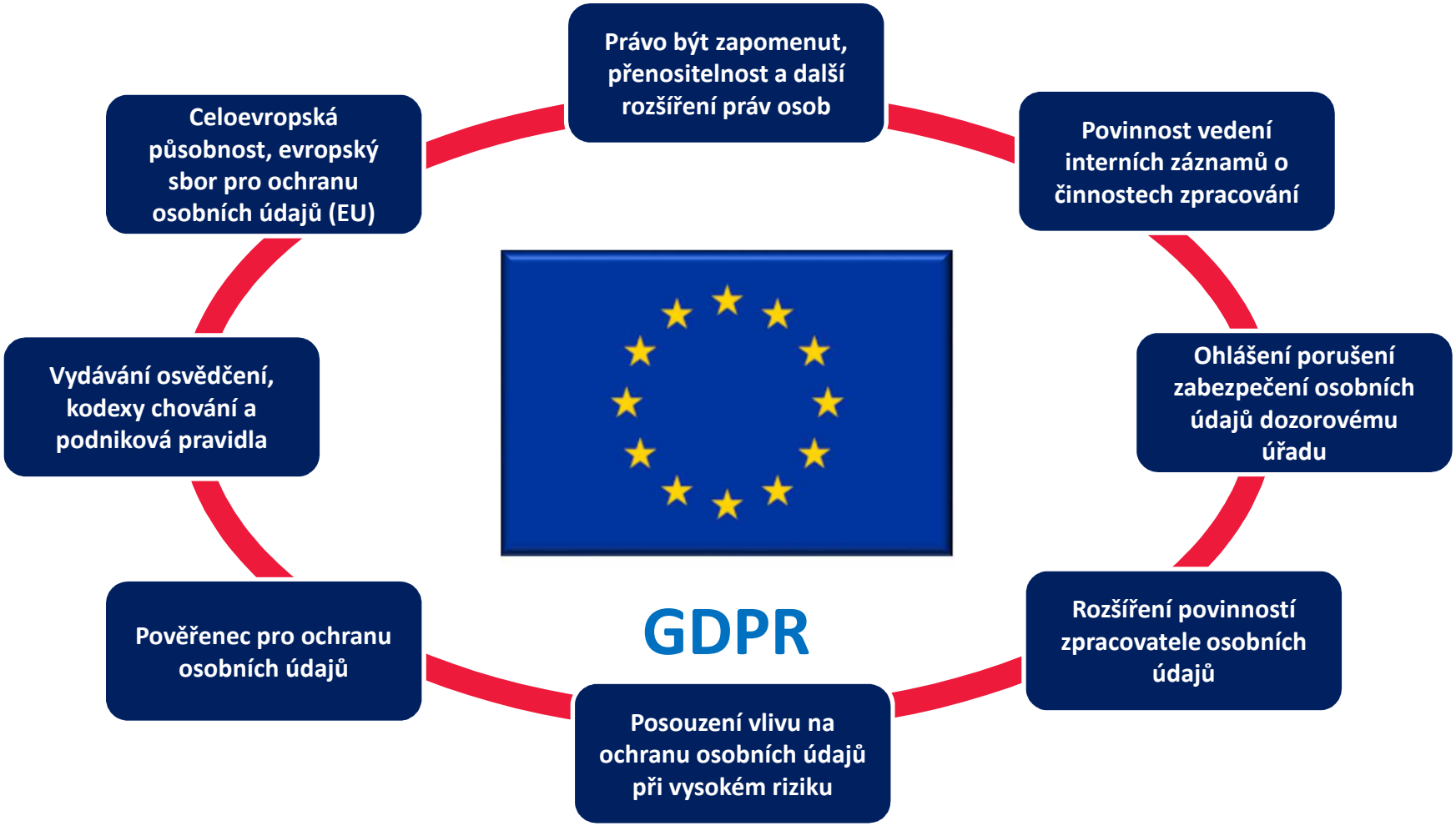
Obecné nařízení č.2016/679 o ochraně osobních údajů (GDPR)

Vstupní (GAP) analýza

Implementace GDPR

Změny v ochraně osobních údajů



Vstupní (GAP) analýza

Vstupní analýza má za cíl:

- zmapovat a identifikovat jednotlivá zpracování osobních údajů, probíhajících v rámci organizace
- zmapovat způsob zacházení s osobními údaji a jejich předávání v rámci organizace a mimo ni
- zjištění mezer v ochraně zpracovávaných osobních údajů
- prověření využití a funkčnosti použitých technických a organizačních opatření k ochraně osobních údajů
- identifikaci soulad či nesouladu mezi stavem zpracování osobních údajů a požadavky GDPR

Výsledkem vstupní analýzy je zpracovaná zpráva o zjištěných skutečnostech s návrhy na provedení jednotlivých opatření

Identifikace zpracování

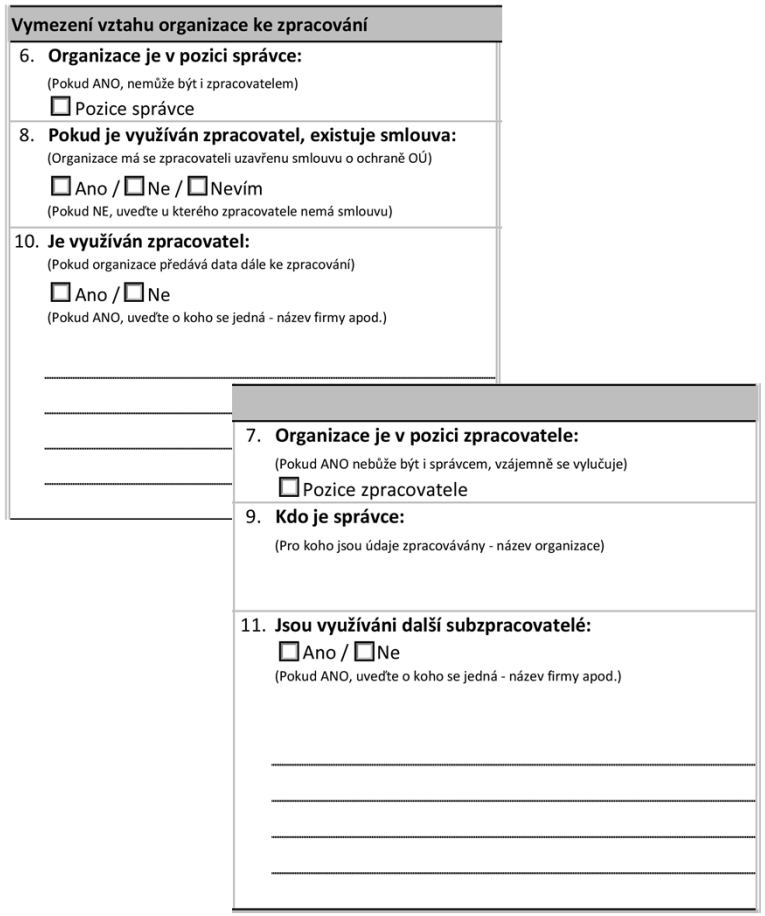
- První krok ke zpracování vstupní analýzy
- Mohou být desítky až stovky zpracování
- **Příklady zpracování**

- dotazník žadatele o zaměstnání
- mzdový list, hlášení OSSZ
- zaslání upomínky
- faktury, smlouvy
- evidence neschopenky
- kniha návštěv

1. **Název scénáře zpracování:**	
2. **Krátký popis scénáře zpracování:** (O jaké zpracování se jedná, za jakým účelem je používáno)	
3. **Respondent:** (osoba vyplňující tento dotazník)	4. **Vlastník údajů:** (garant daného zpracování)
Telefon:	**Email:**
Email:	5. **Vlastník aplikace:** (správce aplikace / systému ve kterém ke zpracování dochází)
Funkce:	**Email:**

Identifikace zpracování

- **Správce =** osoba určující účel a způsob zpracování osobních údajů
  - Základní odpovědnost za údaje
  - Nové povinnosti
- **Zpracovatel =** zpracovává osobní údaje jménem správce
  - Povinnosti jsou stanoveny nově
  - Sdílená odpovědnost
  - Možnost řetězení zpracovatelů
  - Zpracování osobních údajů



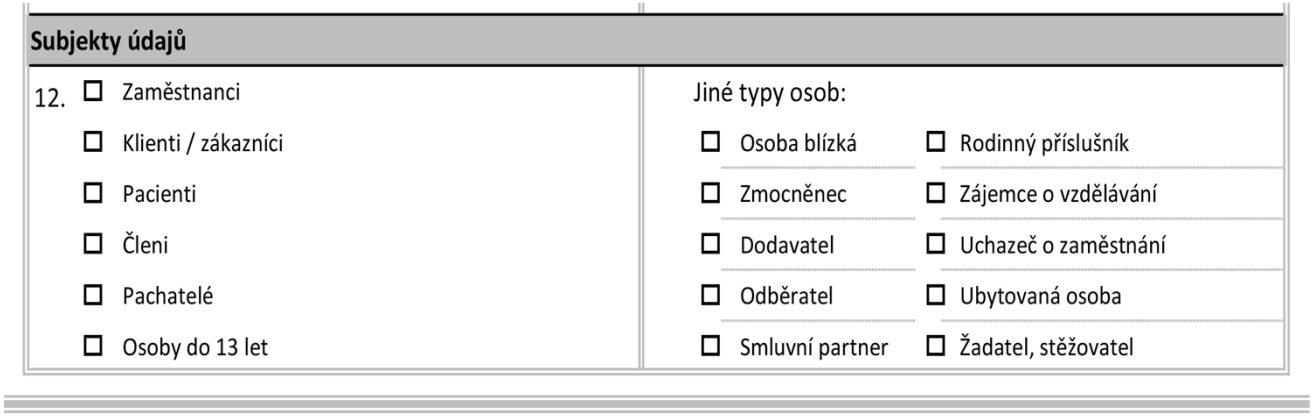
Vymezení vztahu organizace ke zpracování

6. **Organizace je v pozici správce:**
   (Pokud ANO, nemůže být i zpracovatelem)
   ☐ Pozice správce
8. **Pokud je využíván zpracovatel, existuje smlouva:**
   (Organizace má se zpracovateli uzavřenu smlouvu o ochraně OÚ)
   ☐ Ano / ☐ Ne / ☐ Nevím
   (Pokud NE, uveďte u kterého zpracovatele nemá smlouvu)
10. **Je využíván zpracovatel:**
    (Pokud organizace předává data dále ke zpracování)
    ☐ Ano / ☐ Ne
    (Pokud ANO, uveďte o koho se jedná - název firmy apod.)

7. **Organizace je v pozici zpracovatele:**
   (Pokud ANO nebůže být i správcem, vzájemně se vylučuje)
   ☐ Pozice zpracovatele
9. **Kdo je správce:**
   (Pro koho jsou údaje zpracovávány - název organizace)
11. **Jsou využíváni další subzpracovatelé:**
    ☐ Ano / ☐ Ne
    (Pokud ANO, uveďte o koho se jedná - název firmy apod.)

Subjekt údajů

- **Subjekt údajů** = fyzická osoba, které se údaj týká
  - Zaměstnanci
  - Klienti
  - Pacienti
  - Členové statut. org.
  - Pachatelé
  - Osoby do 13 let



Subjekty údajů			
12.	☐ Zaměstnanci	Jiné typy osob:	
	☐ Klienti / zákazníci	☐ Osoba blízká	☐ Rodinný příslušník
	☐ Pacienti	☐ Zmocněnec	☐ Zájemce o vzdělávání
	☐ Členi	☐ Dodavatel	☐ Uchazeč o zaměstnání
	☐ Pachatelé	☐ Odběratel	☐ Ubytovaná osoba
	☐ Osoby do 13 let	☐ Smluvní partner	☐ Žadatel, stěžovatel

Souhlas se zpracováním osobních údajů dítěte mladšího **13 let** je platný pouze, pokud je vyjádřen nebo schválen jeho zákonným zástupcem

Právní základ zpracování OÚ

Zákonnost zpracování (čl.6 Nařízení)

Souhlas SÚ	**Splnění smlouvy**
Splnění právní povinnosti	**Ochrana životně důležitých zájmů SÚ nebo jiné FO**
Veřejný zájem nebo výkon veřejné moci	**Oprávněný zájem správce nebo třetí strany**

Právní základ zpracování

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů **udělil souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů

b) zpracování je **nezbytné pro splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů

c) zpracování je **nezbytné pro splnění právní povinnosti**, která se na správce vztahuje

d) zpracování je **nezbytné pro ochranu životně důležitých zájmů subjektu údajů** nebo jiné fyzické osoby

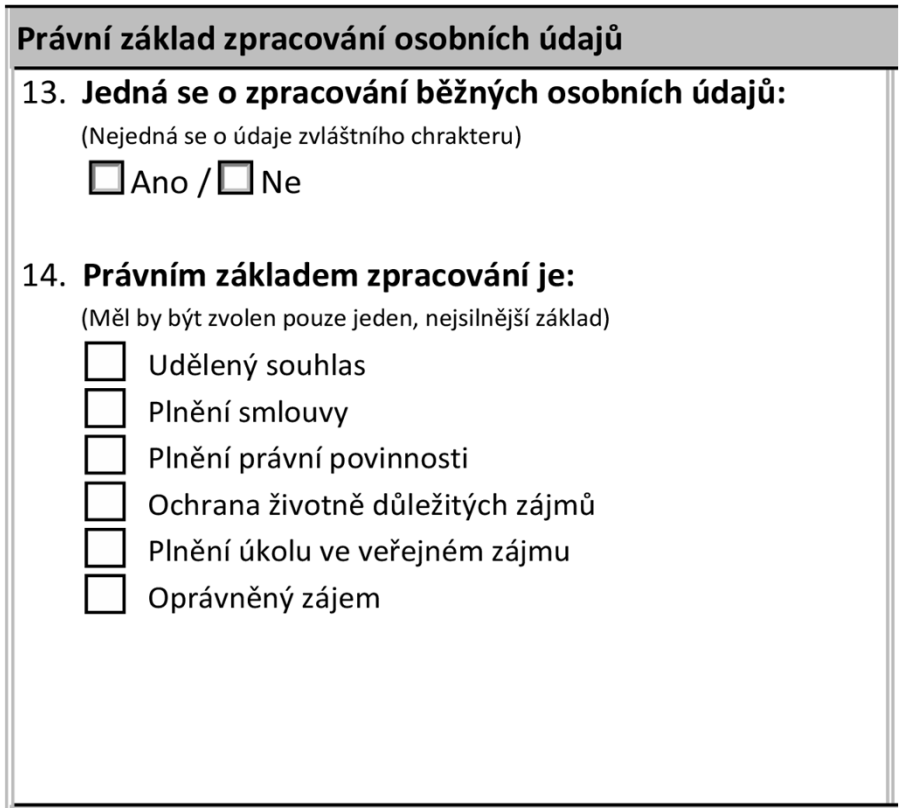
e) zpracování je nezbytné pro **splnění úkolu prováděného ve veřejném zájmu** nebo při výkonu veřejné moci, kterým je pověřen správce

f) zpracování je nezbytné pro **účely oprávněných zájmů příslušného správce** či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě

Právní povinnost zpracování

- Zákony v oblasti soc. zabezpečení a zaměstnanosti
- Zákon o legalizaci výnosů z trestné činnosti
- Zákon o místních poplatcích
- Zákon o pojišťovnictví
- Zákon o účetnictví
- Zákon o archivaci
- Zákoník práce

  atd.....



Právní základ zpracování osobních údajů

13. **Jedná se o zpracování běžných osobních údajů:**
(Nejedná se o údaje zvláštního chrakteru)
☐ Ano / ☐ Ne

14. **Právním základem zpracování je:**
(Měl by být zvolen pouze jeden, nejsilnější základ)
☐ Udělený souhlas
☐ Plnění smlouvy
☐ Plnění právní povinnosti
☐ Ochrana životně důležitých zájmů
☐ Plnění úkolu ve veřejném zájmu
☐ Oprávněný zájem

Oprávněný zájem

Oprávněné zájmy nebo základní práva a svobody subjektu údajů nesmí převážit nad zájmy správce

Typicky: instalace kamerových systémů za účelem ochrany majetku nebo zdraví osob

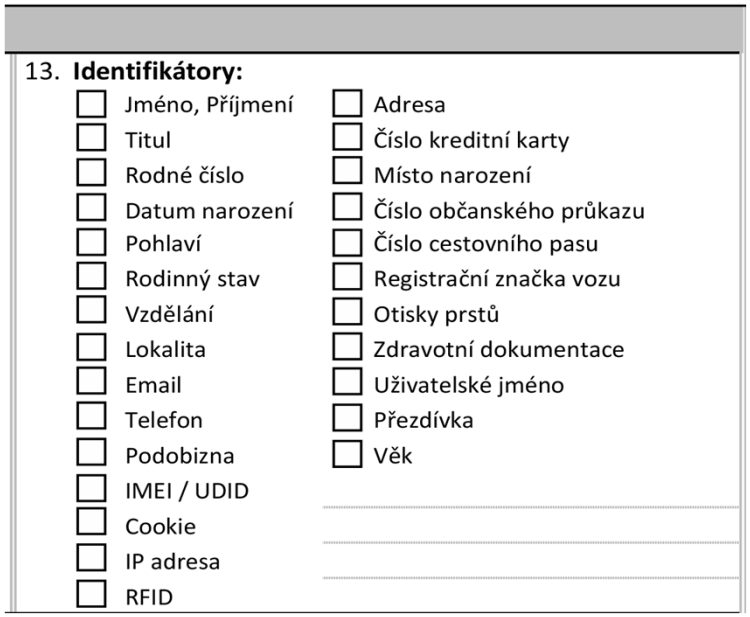
Nově také výslovně:

- **Přímý marketing** v mezích legitimního očekávání
- **Předávání OÚ ve skupině** pro administrativní účely

Je třeba provést posouzení **vyváženosti** mezi zájmy správce a subjektu údajů **– balanční test**

Zpracovávané OÚ - identifikátory

Osobními údaji jsou **veškeré informace o identifikované nebo identifikovatelné fyzické osobě** (dále jen ”subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, **zejména odkazem na určitý identifikátor**, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby



13. **Identifikátory:**

☐ Jméno, Příjmení	☐ Adresa
☐ Titul	☐ Číslo kreditní karty
☐ Rodné číslo	☐ Místo narození
☐ Datum narození	☐ Číslo občanského průkazu
☐ Pohlaví	☐ Číslo cestovního pasu
☐ Rodinný stav	☐ Registrační značka vozu
☐ Vzdělání	☐ Otisky prstů
☐ Lokalita	☐ Zdravotní dokumentace
☐ Email	☐ Uživatelské jméno
☐ Telefon	☐ Přezdívka
☐ Podobizna	☐ Věk
☐ IMEI / UDID	
☐ Cookie	
☐ IP adresa	
☐ RFID	

Právní základ zpracování

Zpracování zvláštních kategorií OÚ (čl.9 Nařízení)

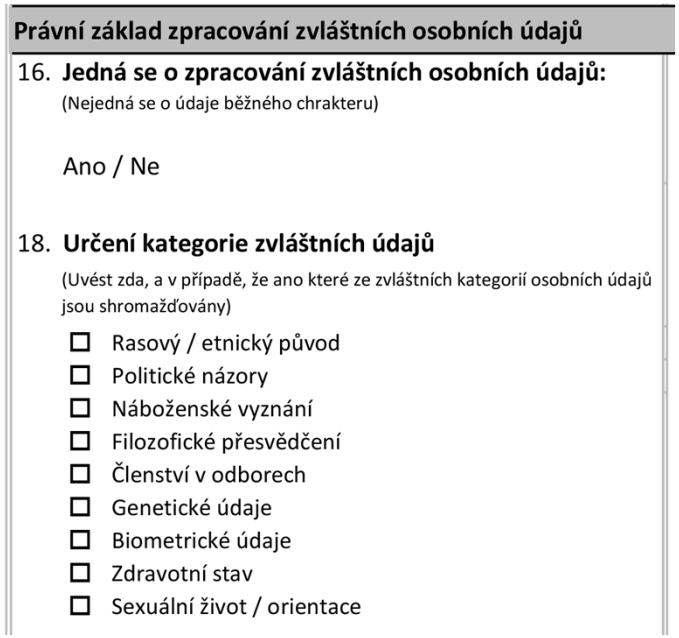
Výslovný souhlas	**Plnění povinností dle pracovního práva**
Životně důležité zájmy	**Zdravotní a soc. péče**
Zjevně zveřejněné údaje	**Výkon nebo obhajoba právních nároků**
Významný veřejný zájem	**Veřejný zájem při ochraně veřejného zdraví či archivaci**

Zvláštní kategorie OÚ

- Dříve citlivé údaje dle zákona č. 101/2000 Sb., o ochraně os. údajů
- **Zakazuje se zpracování osobních údajů**, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby (čl. 9 GDPR)
- Jejich přítomnost signalizuje

  vysoká rizika a **nutnost**

  vedení záznamů o zpracování



Právní základ zpracování zvláštních osobních údajů

16. **Jedná se o zpracování zvláštních osobních údajů:**
(Nejedná se o údaje běžného chrakteru)

Ano / Ne

18. **Určení kategorie zvláštních údajů**
(Uvést zda, a v případě, že ano které ze zvláštních kategorií osobních údajů jsou shromažďovány)

- ☐ Rasový / etnický původ
- ☐ Politické názory
- ☐ Náboženské vyznání
- ☐ Filozofické přesvědčení
- ☐ Členství v odborech
- ☐ Genetické údaje
- ☐ Biometrické údaje
- ☐ Zdravotní stav
- ☐ Sexuální život / orientace

Operace zpracování

Zpracování osobních údajů je jakýkoli úkon nebo soubor úkonů, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky

Jedná se zejména o shromažďování, zaznamenání, uspořádání, strukturování, vyhledávání, nahlédnutí, ukládání na nosiče, zpřístupňování, úprava nebo pozměňování, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování, výmaz či zničení

Operace zpracování osobních údajů		
19.	☐ Sběr	Další nespecifikované /Doplňte další případné operace s daty/
	☐ Uchovávání	
	☐ Validace, kontrola	
	☐ Používání	
	☐ Předávání	
	☐ Nahlížení	
	☐ Archivace	
	☐ Likvidace	

Informování subjektu údajů

- O zpracování osobních údajů musí být subjekt **transparentně informován – ještě před zahájením zpracování**
- Informovat je třeba vždy, pokud již **subjekt informace nemá**
- Informovat nejpozději **do jednoho měsíce** nebo **při první komunikaci či zpřístupnění jinému příjemci**
- **Výjimky** z informační povinnosti
  - Nemožnost
  - Nepřiměřené úsilí
  - Znemožnění dosažení cílů
  - Zpracování probíhá na základě právní povinnosti a údaje nejsou získány od subjektu údajů
  - Osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti

Informování subjektu údajů:		Informace je povinná	Informace byla podána
20.	/Uvést, zda je pro zpracování povinné provést informaci subjektu údajů., a je-li povinné, zda bylo provedeno/	Ano / Ne	Ano / Ne

Obsah informace podávané SÚ

a) **totožnost a kontaktní údaje správce** a jeho případného zástupce
b) **kontaktní údaje pověřence pro ochranu osobních údajů**
c) **účely zpracování**, pro které jsou osobní údaje určeny, a právní základ pro zpracování
d) **oprávněné zájmy správce nebo třetí strany** v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f)
e) **případné příjemce nebo kategorie příjemců osobních údajů**
f) **případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci** nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny

Obsah informace podávané SÚ

Je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování:

a) **doba**, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, **kritéria použitá pro stanovení této doby**

b) existence **práva** požadovat od správce **přístup k osobním údajům** týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů

c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), **existence práva odvolat kdykoli souhlas**, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním

d) **existence práva podat stížnost** u dozorového úřadu

e) skutečnost, **zda poskytování osobních údajů je zákonným či smluvním požadavkem**, nebo požadavkem, který je nutné uvést do smlouvy, a zda má **subjekt údajů povinnost osobní údaje poskytnout**, a ohledně možných důsledků neposkytnutí těchto údajů

f) skutečnost, že **dochází k automatizovanému rozhodování, včetně profilování**, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů

Použitá technická a organizační opatření

- Profilování – například skórování v bance, skoring zaměstnanců

Cílem je získat informaci, zda je použité některé z následujících opatření:

- Pseudonymizace
- Šifrování
- Obnova dostupnosti
- Pravidelné testování a hodnocení

Získáváno spíše od odborných orgánů (IT a bezpečnost)

Použitá technická a organizační opatření:			
24. Pseudonymizace	☐ Ano / ☐ Ne / ☐ Nevím	25. Generalizace	☐ Ano / ☐ Ne / ☐ Nevím
26. Obnova dostupnosti	☐ Ano / ☐ Ne / ☐ Nevím	27. Pravidelné testy	☐ Ano / ☐ Ne / ☐ Nevím
28. Anonymizace	☐ Ano / ☐ Ne / ☐ Nevím	29. Šifrování	☐ Ano / ☐ Ne / ☐ Nevím

Uložení osobních údajů

Cílem je zjistit jakým způsobem jsou osobní údaje zpracovávány s důrazem na automatizovaní zpracování:

- **Manuální** (včetně Wordu a Excelu)
- **Automatizované (IT)** – právo na přenositelnost a kritérium pro provádění posouzení vlivu na ochranu osobních údajů)

Uložení osobních údajů:		
/Uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/		/Pokud jsou data uložena v systému nebo aplikaci, tak v jaké/
30. Listinná podoba	☐ Ano / ☐ Ne	31.
32. Excel, Word, apod.	☐ Ano / ☐ Ne	
33. Aplikace nebo IS	☐ Ano / ☐ Ne	

Rozsah a systematičnost zpracování

Rozsah

Cílem je zjistit zda je zpracování osobních údajů rozsáhlé

Příklad z vodítek skupiny WP29:

- Zpracování – praktický lékař
- **Rozsáhlé zpracování – nemocnice**

Systematické zpracování

Probíhá **pravidelné a stejným způsobem** (dle zavedeného systému)

Rozsah zpracování:	**Systematické zpracování:**
34. /Uvést kolik subjektů údajů zpracování zahrnuje za časový úsek/	35. /Uvést, zda je zpracování systematické/ ☐ Ano / ☐ Ne

Doba zpracování OÚ

Cílem je určit dobu, po kterou budou osobní údaje zpracovávat aby tato doba mohla být sdělena subjektu údajů

Čl 13, odst. 2 Nařízení

„Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:“

a) **„doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby“**

Doba zpracování:	
/Uvést po jakou dobu je potřebné osobní údaje shromažďovat/	/Uvést normu která dobu stanoví/
34. Doba uchování	35.

Interní odpovědnost za zpracování

Cílem je určit kdo interně odpovídá za zpracování (vedoucí útvaru) a ve kterých útvarech, respektive kteří zaměstnanci se zpracování účastní

„Zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat **pouze na pokyn správce**, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu. “ (čl. 29 GDPR)

Interní odpovědnost za zpracování:	
/Uvést interní odpovědnost za toto zpracování – pozice/ 36.	/Uvést email na odpovědnou osobu/ 37.
Organizační útvar (y), které se seznamují s osobními údaji:	
38.	

Srovnávací analýza

Cílem prověření stavu je:

- Zjistit jaké nároky na mne GDPR klade
- Identifikovat zpracování osobních údajů
- Provést posouzení rizik pro práva a svobody subjektu údajů
- Jakým způsobem musím doplnit procesy ke zpracování a ochraně osobních údajů včetně procesů posouzení vlivu a ohlašování porušení zabezpečení
- Jak upravit souhlasy a oznámení předávané subjektu údajů
- Jakou vést dokumentaci
- Jak zavést roli Pověřence pro ochranu osobních údajů a další role potřebné (využití stávajících pro zajištění zpracování a ochrany osobních údajů
- Zda bude využito kodexů chování nebo bude absolvován proces získání osvědčení

Analýza rizik zpracování OÚ

Posouzení rizik, či jak GDPR definuje „vyhodnocení hrozeb pro práva a svobody fyzických osob“ je možné provést v následujících krocích:

- Identifikace možných hrozeb u jednotlivých zpracování
- Vyhodnocení a klasifikace rizik jednotlivých zpracování
- Pravděpodobnost vzniku škody
- Typizace případné škody – materiální, nemateriální, společenská..
- Klasifikace závažnosti možné škody v závislosti na míře citlivosti osobních údajů, objemu zpracovávaných OÚ, míře zranitelnosti dotčených osob
- Posouzení vztahu míry rizika a přínosu zpracování OÚ pro organizaci atd…

Posouzení rizik

Posouzení rizik pro práva a svobody osob:	
/Uvést, zda je u tohoto zpracování přítomen některý z níže uvedených rizikových faktorů/	
• Automatizované, systematické vyhodnocování osobních aspektů týkající se fyzických osob včetně profilování s následným rozhodováním s právním nebo obdobně významným účinkem	
• Rozsáhlé systematické monitorování veřejně přístupných prostorů	
• Zpracování OÚ zvláštní kategorie	
• Zpracování je rozsáhlé	
• Soubory dat, které byly porovnány nebo zkombinovány	
• Zahrnutí údajů týkající se zranitelných subjektů údajů	
• Inovativní používání nebo uplatňování technologických nebo organizačních řešení (např. biometrika)	
• Přesun dat přes hranice mimo Evropskou unii	
• Pokud samotné zpracování zabraňuje subjektům údajů vykonávat právo nebo využívat službu nebo smlouvu	
Jedná se o zpracování s vysokým rizikem pro práva a svobody osob:	Ano/Ne

Posuzování vlivu na ochranu OÚ

Posouzení je nutné v případech, kdy:

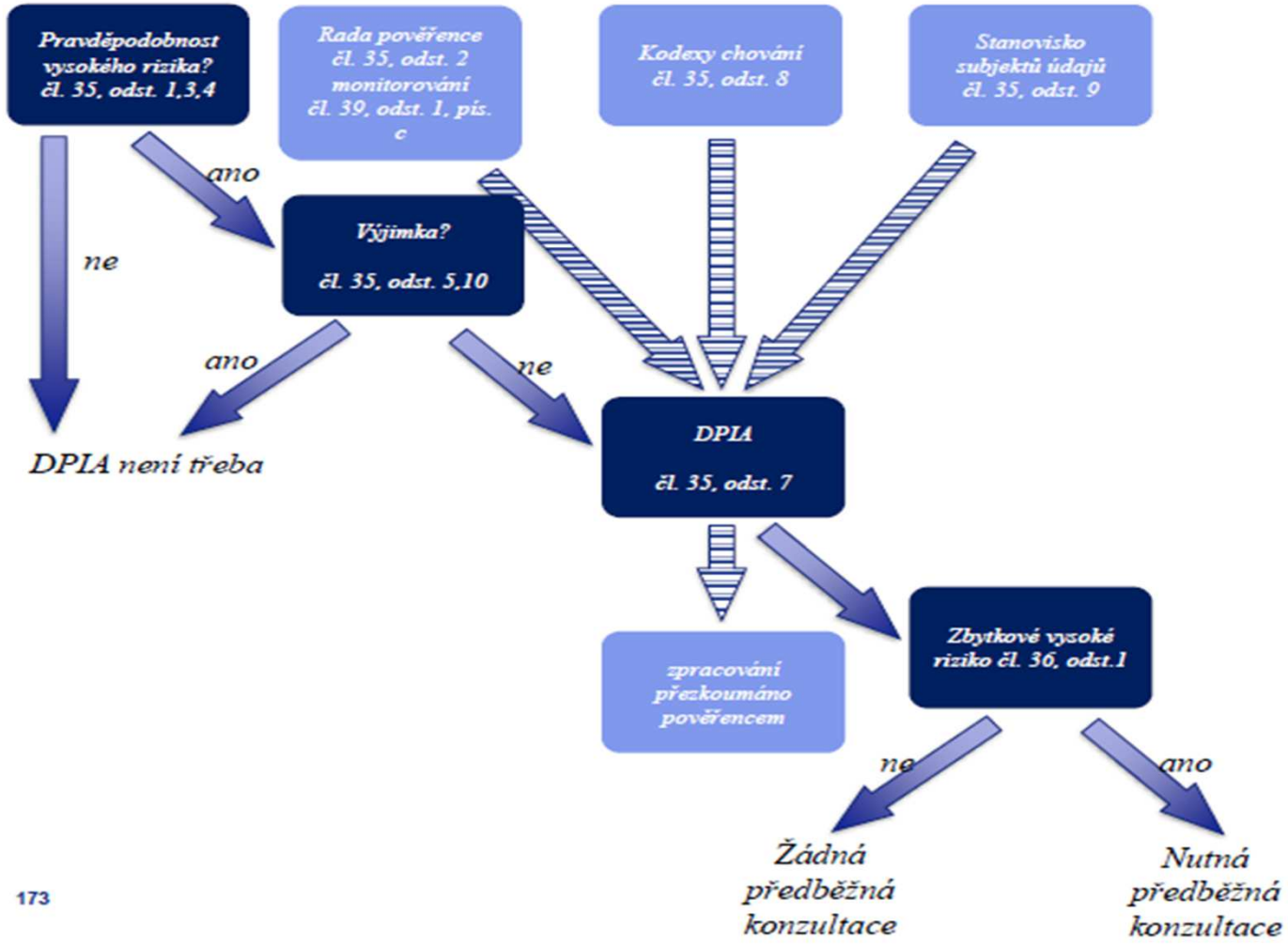
- zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob, a to s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a využitím nových technologií

Jedná se zejména o:

- kategorie údajů shromažďovaných o subjektech údajů
- určení míry zranitelnosti subjektů údajů
- dostupnost osobních údajů
- rozsah a soustavnost zpracování osobních údajů
- přístupnost osobních údajů
- vazby na další subjekty zpracování (jednoznačné vymezení)

Posouzení vlivu na ochranu OÚ

Schéma posouzení vlivu na ochranu OÚ (DPIA)



Audit smluv, souhlasů a interní dokumentace

- **Audit** a případná revize **zpracovatelských smluv**
- **Kontrola** a případná **úprava** udělených **souhlasů** se zpracováním OÚ
  - **oddělení o ostatních skutečností** (mimo smlouvy, mimo obchodní podmínky) – **zásada svobodného udělení**
- **Kontrola balančních testů** při použití **oprávněného zájmu**
- **Spisový, archivační a skartační řád**
- **Ostatní interní agenda** – vnitřní směrnice, metodiky, školení odpovědných pracovníků – interních zpracovatelů
- **Kontrola uložení** veškeré „papírové“ agendy v organizaci

Implementace požadavků GDPR

Implementace probíhá v závislosti na upřesnění z předešlých analýz

Typově se jedná o:

- Realizace **návrhu úpravy/vytvoření procesů** na zpracování a ochranu osobních údajů včetně jejich zdokumentování
- Spolupráce při úpravě **bezpečnostní architektury IS** zpracovávajících osobní údaje
- Spolupráce při přípravě **pověřence pro ochranu osobních údajů**
- Spolupráce při provedení **posouzení vlivu** zamýšlených operací zpracování na ochranu osobních údajů
- Příprava na **vydání osvědčení** o ochraně osobních údajů bude-li požadováno

Implementace požadavků GDPR

Identifikace zpracování	• Určení účelů a titulů zpracování • Určení podmínek zpracování
Pověřenec	• Vymezit činnosti, nasmlouvat jeho činnost • Vhodné hned po srovnávací analýze
Úprava klientských smluv a způsobu informování	• Úprava klientských smluv, zapracování povinných informací a úprava případných souhlasů se zpracováním OÚ
Zpracovatelské smlouvy	• Vymezení nových povinností Správce – Zpracovatel a úprava smluv
Posouzení vlivu a systém hlášení	• Příprava procesu (včetně zdokumentování) pro zpracování posouzení a hlášení porušení zabezpečení
Vedení záznamů o zpracování	• Zdokumentování přijatých technických a organizačních opatření včetně testů a hodnocení