ACRESIA
CONSULTING

GDPR

Nová právní úprava ochrany osobních údajů

Jak se připravit?

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Toto nařízení se použije ode dne 25. května 2018

15. 11. 2017

ACRESIA CONSULTING

Změny v ochraně osobních údajů

GDPR

- **Právo být zapomenut, přenositelnost a další rozšíření práv osob**
- **Povinnost vedení interních záznamů o činnostech zpracování**
- **Ohlášení porušení zabezpečení osobních údajů dozorovému úřadu**
- **Rozšíření povinností zpracovatele osobních údajů**
- Posouzení vlivu na ochranu osobních údajů při vysokém riziku
- Pověřenec pro ochranu osobních údajů
- Vydávání osvědčení, kodexy chování a podniková pravidla
- **Celoevropská působnost, evropský sbor pro ochranu osobních údajů (EU)**

Zpracování osobních údajů se nemusí registrovat

ACRESIA CONSULTING

GDPR dále přináší

- Ochrana „by design“ a „by default“
- Zvýšené sankce
- Úprava souhlasu dětí (dle návrhu zákona v ČR do 13 let)
- Více informací sdělovaných subjektu údajů (i při zpracování „ze zákona“)
- Snaha působit i mimo EU (při zpracování dat občanů EU)
- Možné rozpracování v národní legislativě

- **Stupňuje povinnosti dle rizikovosti**
- **Možnost výjimek z práv**
- **One stop shop**

ACRESIA CONSULTING

Sankce podle GDPR

Správní

Peněžitá pokuta až do 20 mil. EUR nebo do 4 % ročního obratu

- Národní legislativa může stanovit další správní sankce
- Národní legislativa může zmocnit neziskovou organizaci k podávání stížností i bez zmocnění dotčeným subjektem údajů

Civilní

Náhrada škody + **Náhrada nemajetkové újmy**

- Možnost žalovat u soudů v zemi bydliště subjektu údajů
- Možnost subjektu údajů nechat se zastoupit neziskovou organizací zaměřenou na ochranu osobních údajů
- Společná a nerozdílná odpovědnost správce a zpracovatele

ACRESIA CONSULTING

Osobní údaj

Jakákoliv informace o fyzické osobě podle níž lze danou osobu přímo či nepřímo identifikovat

- Jméno
- Pohlaví
- Věk
- Email
- Telefon
- Adresa
- Cookie
- IP adresa
- Fotografie
- Uživatelské jméno…

Zvláštní kategorie osobních údajů

- Rasa nebo etnický původ
- Politické názory
- Náboženství a filozofické přesvědčení
- Členství v odborech
- Genetické a biometrické údaje
- Zdravotní stav
- Sexuální život a orientace

ACRESIA CONSULTING

Jak se postavit k požadavkům GDPR?

V první řadě je potřebné upřesnit zpracování …

- Identifikovat zpracování osobních údajů v organizaci
- K těmto zpracováním určit:
  - Účel zpracování
  - Jaký je právní základ zpracování (souhlas, plnění právní povinnosti, plnění či uzavření smlouvy, oprávněný zájem, veřejný zájem či výkon veřejné moci …)
  - Kdo je správce a kdo zpracovatel
  - Kde jsou osobní údaje uloženy (manuální, IS)
  - Kdo se v rámci organizace s údaji seznamuje, interní odpovědnost za zpracování
  - Způsob zabezpečení osobních údajů

ACRESIA CONSULTING

Cíl identifikace zpracování

- Zjistit **jaká zpracování v organizaci probíhají**
- Určit **interní odpovědnost** za zpracování a ochranu
- Zjištění zda je:
  - zpracování **rizikové**
  - nutné vést **záznamy o zpracování**
  - nutné provést **posouzení vlivu na ochranu osobních údajů** pro konkrétní zpracování
  - nutné zřídit **pověřence pro ochranu osobních údajů**

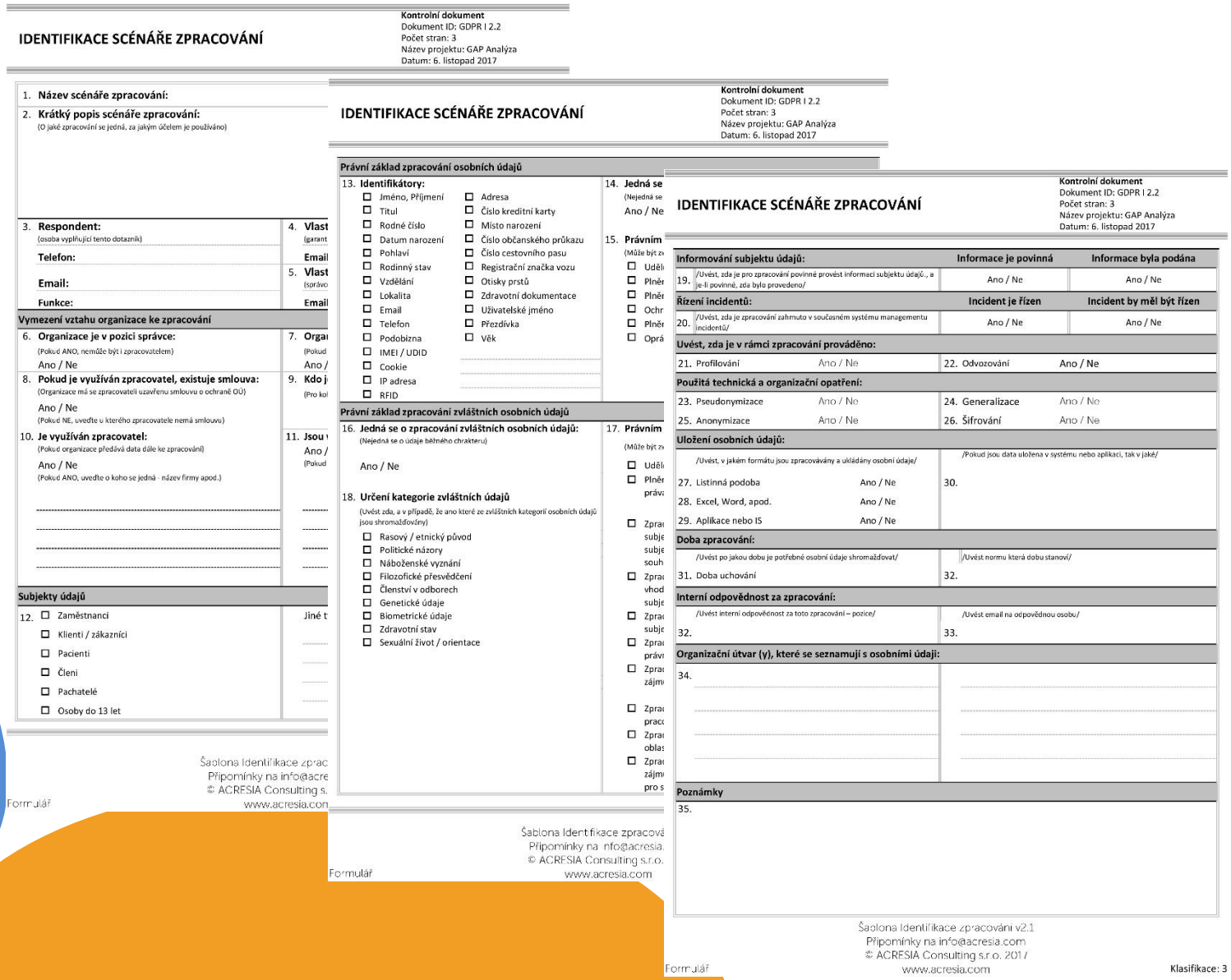
ACRESIA CONSULTING

Na co nezapomenout při identifikaci

- Identifikace zpracování osobních údajů je základní činnost při zahájení implementace GDPR
- Neustále je nutné mít na zřeteli, že **se jedná o ochranu osobních údajů fyzických osob**
- Důležité si **upřesnit zda se opravdu jedná o zpracování osobních údajů**
- V této oblasti odborný orgán může pomoci, ale vždy je třeba **zapojit zástupce organizačních útvarů**, které osobní údaje zpracovávají
- Zpracování osobních údajů **nezužovat na zpracování v informačních systémech**

ACRESIA CONSULTING

Tabulka k provedení identifikace



IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR I 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

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)
Telefon:
Email:
Funkce:

4. **Vlast**
(garant
Email

5. **Vlast**
(správc
Email

Vymezení vztahu organizace ke zpracování

6. **Organizace je v pozici správce:**
(Pokud ANO, nemůže být i zpracovatelem)
Ano / Ne

7. **Orga**
(Pokud
Ano /

8. **Pokud je využíván zpracovatel, existuje smlouva:**
(Organizace má se zpracovateli uzavřenu smlouvu o ochraně OÚ)
Ano / Ne
(Pokud NE, uveďte u kterého zpracovatele nemá smlouvu)

9. **Kdo j**
(Pro ko

10. **Je využíván zpracovatel:**
(Pokud organizace předává data dále ke zpracování)
Ano / Ne
(Pokud ANO, uveďte o koho se jedná - název firmy apod.)

11. **Jsou**
Ano /
(Pokud

Subjekty údajů

12.
- ☐ Zaměstnanci
- ☐ Klienti / zákazníci
- ☐ Pacienti
- ☐ Členi
- ☐ Pachatelé
- ☐ Osoby do 13 let

Jiné t

Šablona Identifikace zprac
Připomínky na info@acre
© ACRESIA Consulting s.
www.acresia.com

Formulář

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR I 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

Právní základ zpracování osobních údajů

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

14. **Jedná se**
(Nejedná se
Ano / Ne

15. **Právním**
(Může být z
- ☐ Udělí
- ☐ Plněr
- ☐ Plněr
- ☐ Ochr
- ☐ Plněr
- ☐ Oprá

Právní základ zpracování zvláštních osobních údajů

16. **Jedná se o zpracování zvláštních osobních údajů:**
(Nejedná se o údaje běžného charakteru)
Ano / Ne

17. **Právním**
(Může být z
- ☐ Udělí
- ☐ Plněr práv

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

- ☐ Zprac subje subje souh
- ☐ Zprac vhod subje
- ☐ Zprac subje
- ☐ Zprac práv
- ☐ Zprac zájm
- ☐ Zprac prac
- ☐ Zprac oblas
- ☐ Zprac zájm pro s

Šablona Identifikace zpracová
Připomínky na info@acresia.
© ACRESIA Consulting s.r.o.
www.acresia.com

Formulář

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR I 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

Informování subjektu údajů:		**Informace je povinná**	**Informace byla podána**
19. /Uvést, zda je pro zpracování povinné provést informaci subjektu údajů., a je-li povinné, zda bylo provedeno/		Ano / Ne	Ano / Ne
Řízení incidentů:		**Incident je řízen**	**Incident by měl být řízen**
20. /Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/		Ano / Ne	Ano / Ne
Uvést, zda je v rámci zpracování prováděno:			
21. Profilování	Ano / Ne	22. Odvozování	Ano / Ne
Použitá technická a organizační opatření:			
23. Pseudonymizace	Ano / Ne	24. Generalizace	Ano / Ne
25. Anonymizace	Ano / Ne	26. Šifrování	Ano / Ne
Uložení osobních údajů:			
/Uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/		/Pokud jsou data uložena v systému nebo aplikaci, tak v jaké/	
27. Listinná podoba	Ano / Ne	30.	
28. Excel, Word, apod.	Ano / Ne		
29. Aplikace nebo IS	Ano / Ne		
Doba zpracování:			
/Uvést po jakou dobu je potřebné osobní údaje shromažďovat/		/Uvést normu která dobu stanoví/	
31. Doba uchování		32.	
Interní odpovědnost za zpracování:			
/Uvést interní odpovědnost za toto zpracování – pozice/		/Uvést email na odpovědnou osobu/	
32.		33.	
Organizační útvar (y), které se seznamují s osobními údaji:			
34.			
Poznámky			
35.			

Šablona Identifikace zpracování v2.1
Připomínky na info@acresia.com
© ACRESIA Consulting s.r.o. 2017
www.acresia.com

Formulář

Klasifikace: 3

ACRESIA CONSULTING

Identifikace zpracování

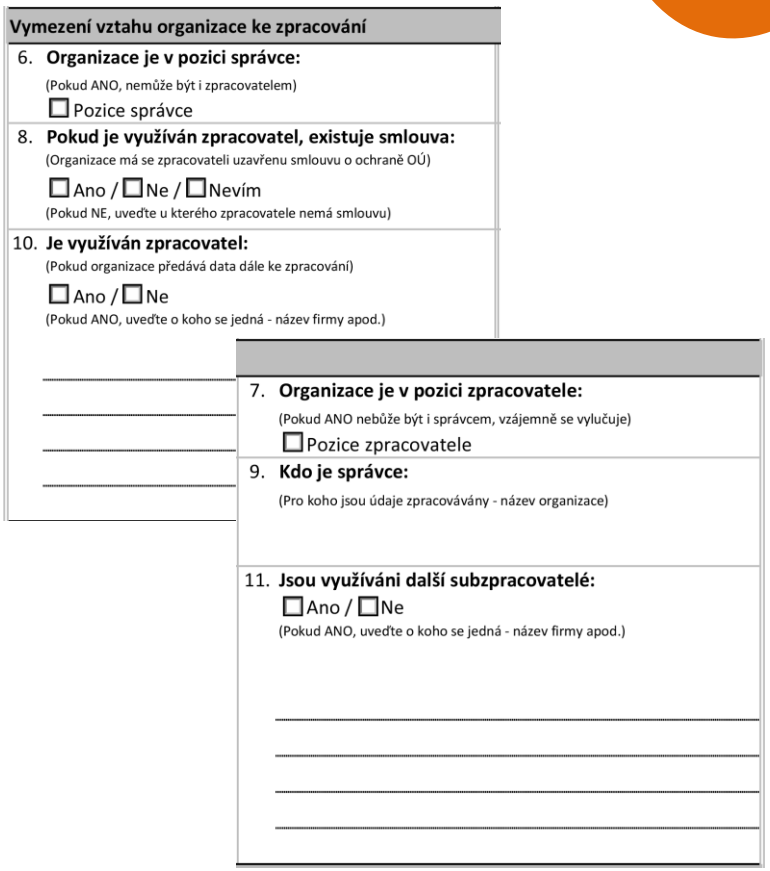
- Základní stavební kámen
- Desítky až stovky zpracování
- Zpracováním se rozumí například:
  - Nábor zaměstnanců a životopisy
  - Hlášení pracovního úrazu
  - Mzdové listy
  - Formulář na webu
  - Výroční zpráva
  - Faktury a smlouvy
  - CRM

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:**

ACRESIA CONSULTING

Správce a zpracovatel

- **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

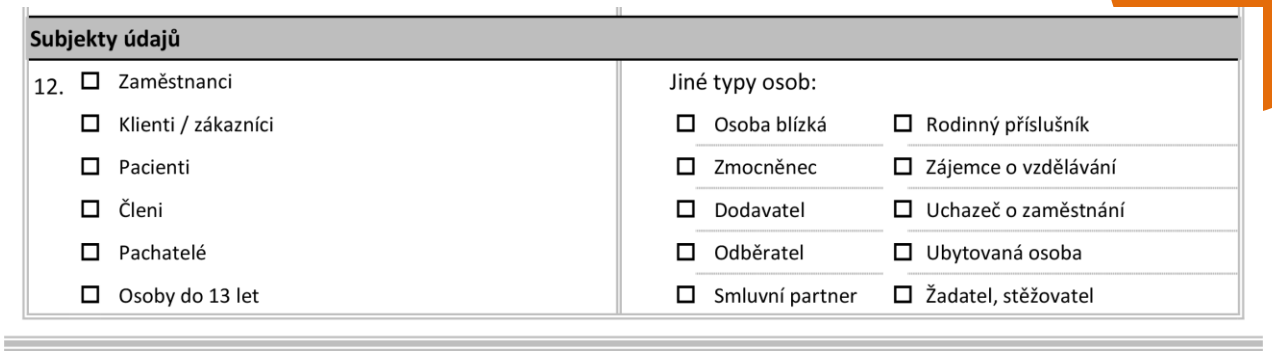
6. **Organizace je v pozici správce:**
   (Pokud ANO, nemůže být i zpracovatelem)
   ☐ Pozice správce
8. **Pokud je využíván zpracovatel, existuje smlouva:**
   (Organizace má se zpracovateli uzavřenu smlouvu o ochraně OÚ)
   ☐ Ano / ☐ Ne / ☐ Nevím
   (Pokud NE, uveďte u kterého zpracovatele nemá smlouvu)
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.)

ACRESIA CONSULTING

Subjekt údajů

- **Subjekt údajů** = fyzická osoba, které se údaj týká
  - Zaměstnanci
  - Klienti
  - Pacienti
  - Členi
  - 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 v souvislosti s nabídkou služeb informační společnosti přímo dítěti mladšímu **13 let** je platný pouze, pokud je vyjádřen nebo schválen jeho zákonným zástupcem

ACRESIA CONSULTING

Právní základ zpracování (čl. 6 GDPR)

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

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

ACRESIA CONSULTING

Právní základ pro zpracování os. údajů

Souhlas	Plnění či uzavření smlouvy
Právní povinnost	Oprávněný zájem
Veřejný zájem či výkon veřejné moci	Životně důležitý zájem

ACRESIA CONSULTING

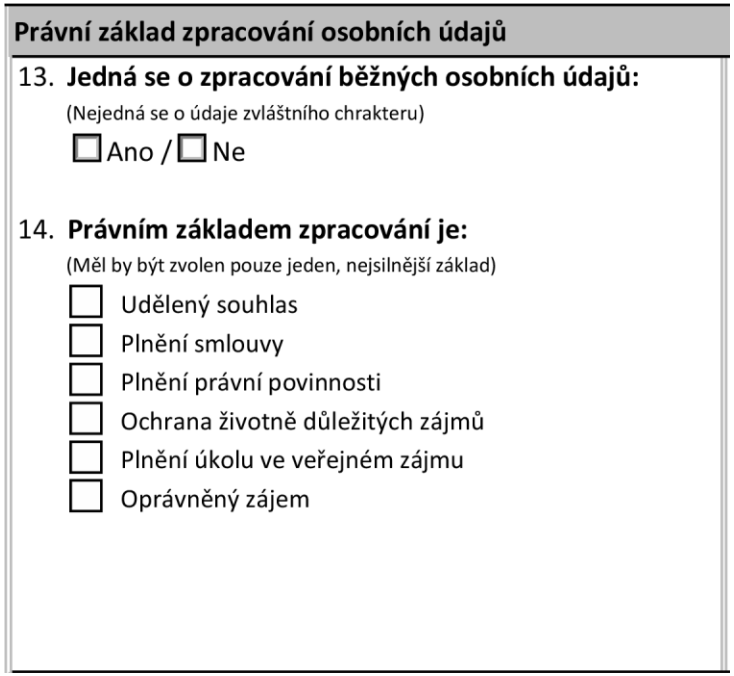
Další tituly pro zpracování zvláštních kategorií údajů

Výslovný souhlas	Povinnosti dle pracovního práva
Životně důležité zájmy	Pracovně-lékařské posudky
Zjevně zveřejněné údaje	Výkon nebo obhajoba právních nároků
Významný veřejný zájem	Veřejný zájem při ochraně veřejného zdraví či archivaci

ACRESIA CONSULTING

Právní povinnost zpracovávat

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



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

ACRESIA CONSULTING

Oprávněný zájem

Nesmí jej v daném případě převážit zájmy nebo základní práva a svobody subjektu údajů

Typicky: **ochrana majetku** (kamerový systém)

Nově také výslovně:

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

ACRESIA CONSULTING

Problémy oprávněného zájmu

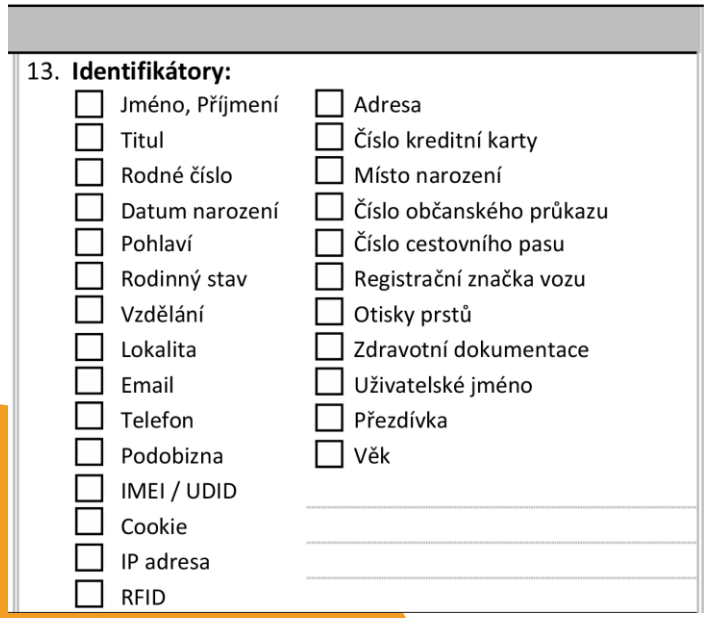
- Je třeba provést **vyvažování** mezi zájmy správce a subjektu údajů **– balanční analýza**
- Proti zpracování lze **vznést námitku** na základě osobní situace subjektu údajů
- Při námitce je třeba **omezit zpracování** a při vyhovění námitce (negativní výsledek testu přiměřenosti) údaje smazat

- **Široký právní základ, s jistou mírou rizika**

ACRESIA CONSULTING

Identifikátory osobních údajů

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



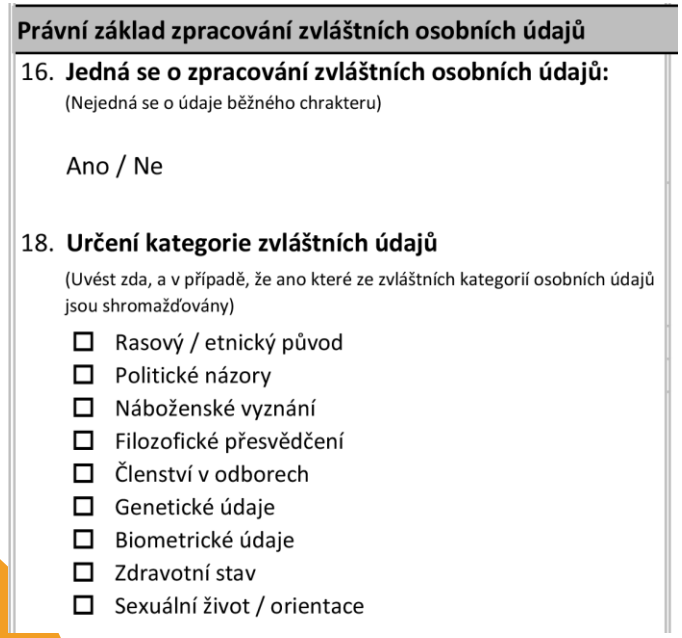
13. **Identifikátory:**

☐ 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	

ACRESIA CONSULTING

Zpracování zvláštních kategorií osobních údajů

- Bývalé citlivé údaje dle stávajícího zákona
- **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

ACRESIA CONSULTING

Operace zpracování

- Způsob, jakým je nakládáno s osobními daty
- Slouží k identifikaci, zda se opravdu jedná o zpracování osobních údajů
  - Cloud
  - Uložení dat v diagnostickém přístroji

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

ACRESIA CONSULTING

Informování subjektu údajů

- O zpracování osobních údajů musí být subjekt **transparentně informován**
- Informovat je třeba vždy, pokud již **subjekt informace nemá**
- Informovat nejpozději **do jednoho měsíce** nebo **při první komunikaci či zpřístupnění jinému příjemci**
- **Výjimky** z informování
  - 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

ACRESIA CONSULTING

Informace a přístup k osobním údajům

- Nový, doplněný obsah informace, která se podává subjektu údajů při převzetí osobních údajů
- Nově se podává i u zpracování k naplnění **právní povinnosti** u případů, kde nabíráte údaje od subjektu údajů
- Obsah informace uveden v článku **13 GDPR**

Informace by se měly podávat i u stávajících zpracování a to minimálně tam, kde je zřízen pověřenec pro ochranu osobních údajů

ACRESIA CONSULTING

Článek 13 GDPR

a) **totožnost a kontaktní údaje správce** a jeho případného zástupce
b) případně **kontaktní údaje** případného **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

ACRESIA CONSULTING

Článek 13 GDPR - Pokračování

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

ACRESIA CONSULTING

Použitá technická a organizační opatření

Ověření, zda existuje proces eskalace incidentu

- Zda je proces řízen a existuje
- Zda by měl být řízen

Ověření existence procesu práva nebýt automaticky zpracováván

- Profilování – Například skórování v bance, inzerce na internetu
- Odvozování – Například usouzení na míru schopnosti utrácet peníze

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 / ☐ Nevím	☐ Ano / ☐ Ne / ☐ Nevím
Řízení incidentů:		**Incident je řízen**	**Incident by měl být řízen**
21.	/Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/	☐ Ano / ☐ Ne / ☐ Nevím	☐ Ano / ☐ Ne / ☐ Nevím

ACRESIA CONSULTING

Použitá technická a organizační opatření

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

ACRESIA CONSULTING

Uložení osobních údajů

Cílem je zjistit v jaké formě jsou osobní údaje zpracovávány s důrazem na automatizovaní zpracování:

- **Manuální** (včetně Wordu a Excelu)
- IT (**automatizované** – 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	

ACRESIA CONSULTING

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

ACRESIA CONSULTING

Určit dobu zpracování

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

„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“** (čl. 13 GDPR)

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

ACRESIA CONSULTING

Interní účast na 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/	/Uvést email na odpovědnou osobu/
36.	37.
Organizační útvar (y), které se seznamují s osobními údaji:	
38.	

ACRESIA CONSULTING

Srovnávací analýza stavu

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

ACRESIA CONSULTING

Analýza rizik zpracování osobních údajů

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

- Určení kritérií analýzy a respondentů
- Návrh a schválení metodiky analýzy rizik
- Identifikace a ohodnocení jednotlivých zpracování
- Identifikace hrozeb
- Vyhodnocení rizik zpracování osobních údajů
- Zpracování, projednání a schválení zprávy o posouzení rizik spojených s jednotlivými zpracováními osobních údajů

ACRESIA CONSULTING

Posuzování vlivu na ochranu osobních údajů

Obsahem posouzení musí být:

- Popis zamýšlených operací, účelů zpracování a oprávněných zájmů správce
- Zhodnocení nezbytnosti a proporcionality operací ve vztahu k účelům
- Zhodnocení rizika právům a svobodám jednotlivců
- Popis zamýšlených opatření ke zmírnění rizika, včetně bezpečnostních opatření a mechanismů

Pokud riziko zůstává vysoké navzdory přijatým opatřením, je třeba **předchozí konzultace s dozorovým orgánem**

ACRESIA CONSULTING

Implementace požadavků GDPR

Implementace probíhá v závislosti na upřesnění z předešlých analýz

Typově se jedná o:

- Realizace **návrhu úpravy/vytvoření procesů** na manipulaci a ochranu osobních údajů včetně jejich zdokumentování
- Spolupráce při úpravě **bezpečnostní architektury IS** zpracovávající osobní údaje
- Podpora nebo **implementace nástrojů** k naplnění požadavků GDPR
- 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

ACRESIA CONSULTING

Na co dále nezapomenout

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 případného souhlasu
Zpracovatelské smlouvy	• Vymezení nových povinností Správce – Zpracovatel a úprava smluv
Posouzení vlivu a systém hlášení	• Příprava procesu (včetně zdokumentování) pro zpracování posouzení a hlášení
Vedení záznamů o zpracování	• Zdokumentování přijatých technických a organizačních opatření včetně testů a hodnocení

… je nutné zavedení komplexního systému ochrany a práce s osobními údaji, který je doložitelný

ACRESIA CONSULTING

Děkuji za pozornost

www.acresia.com

ACRESIA
CONSULTING