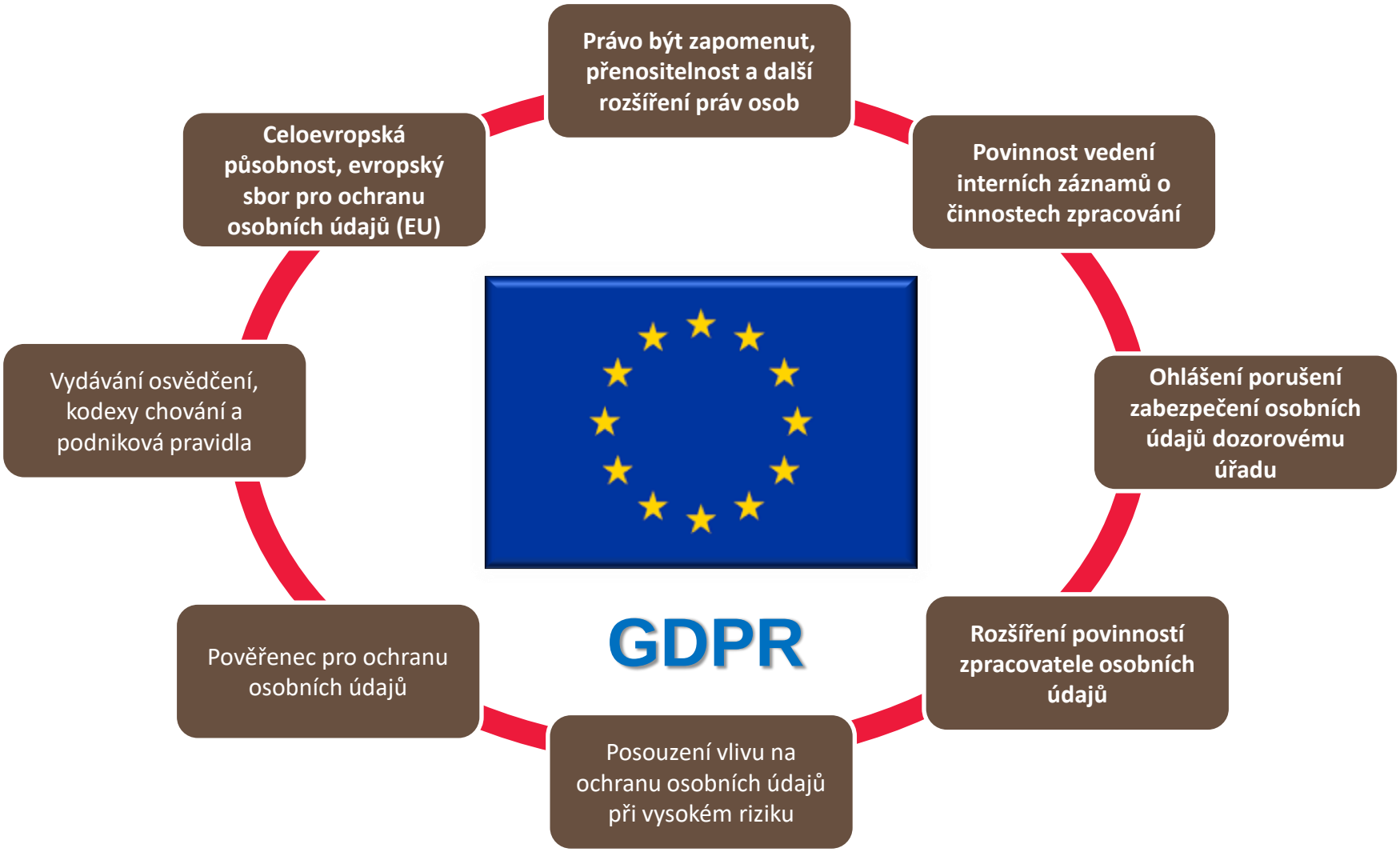
GDPR za humny

Ing., Mgr. Luděk Nezmar, MBA

15. května 2018

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

Změny v ochraně osobních údajů



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

Nástroje a zdroje GDPR

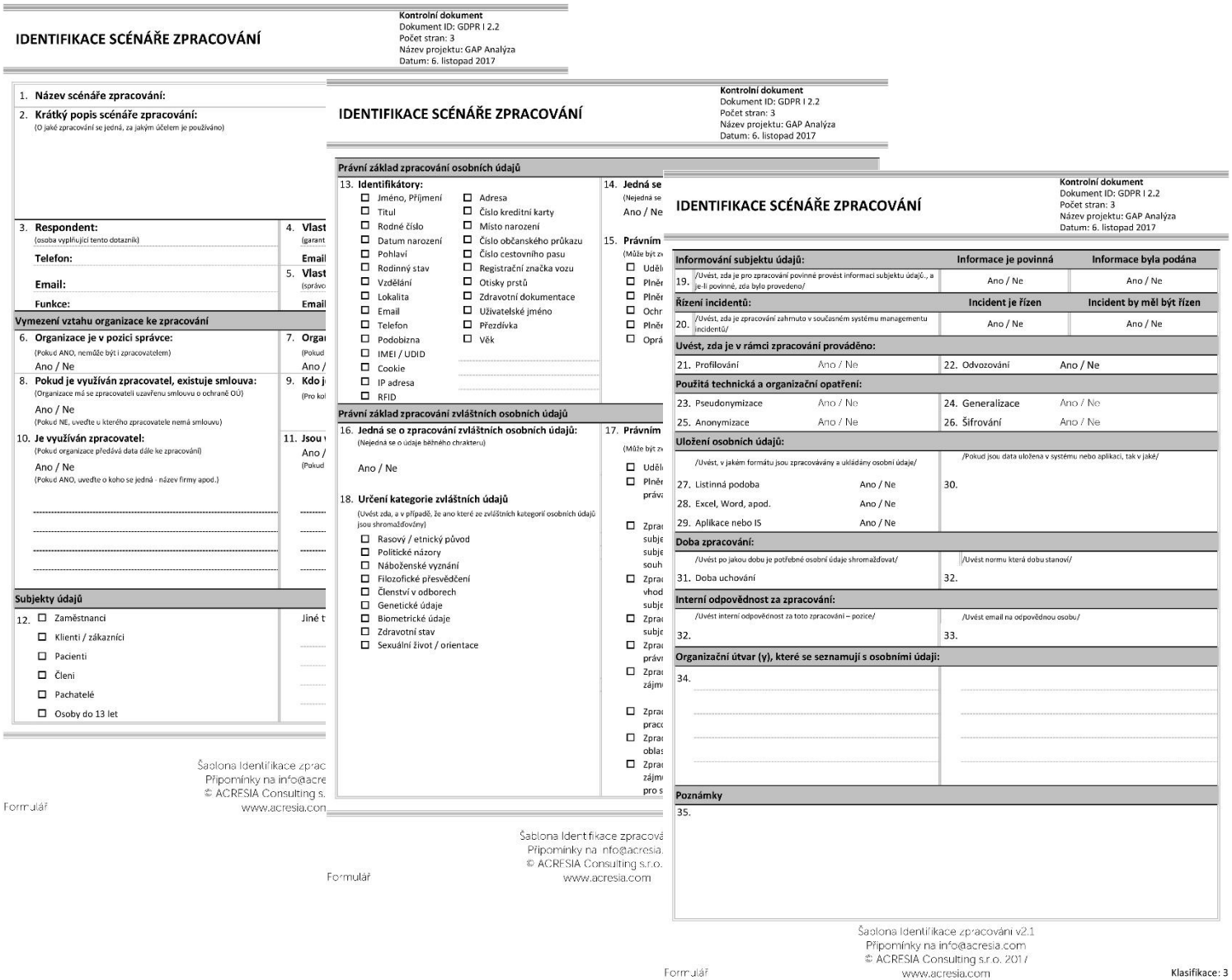
- www.gdpr.cz
- www.acresia.com
- www.forum-media.cz
- www.helpgdpr.cz
- www.24lcs.com/cs/

Zahraniční zdroje

- www.ico.uk.org
- onetrust.com
- www.cnil.fr
- iapp.org
- www.bfdi.bund.de
- www.cookiebot.com

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

Formulář 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**
(správo
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
- ☐ Uděl
- ☐ 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
- ☐ Uděl
- ☐ Plněr práv
- ☐ Zprac subje subje souh
- ☐ Zprac vhod subje
- ☐ Zprac subje
- ☐ Zprac právi
- ☐ Zprac zájm
- ☐ Zprac prac
- ☐ Zprac oblas
- ☐ Zprac zájm pro s

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

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.			

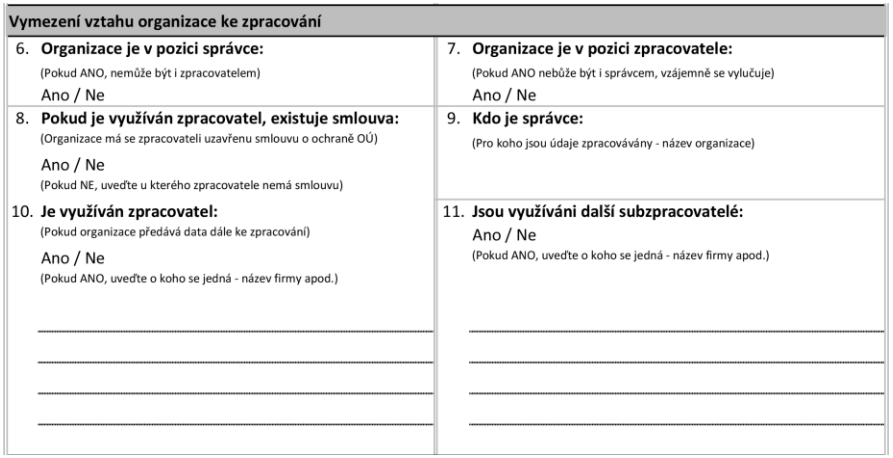
Šablona Identifikace zpracování v2.1
Připomínky na info@acresia.com
© ACRESIA Consulting s.r.o. 2017
www.acresia.com

Formulář

Klasifikace: 3

Správce a zpracovatel

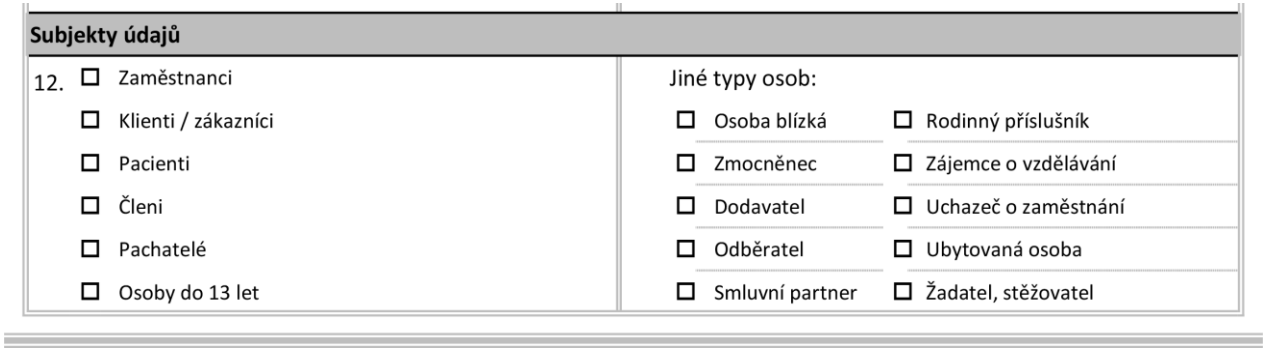
- **Správce =** osoba určující účel a způsob zpracování osobních údajů
  - Základní odpovědnost za údaje
  - Nové povinnosti
- **Zpracovatel =** zpracovává osobní údaje jménem správce
  - Povinnosti jsou stanoveny nově
  - Sdílená odpovědnost
  - Možnost řetězení zpracovatelů
  - Zpracování osobních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



Vymezení vztahu organizace ke zpracování	
6. **Organizace je v pozici správce:** (Pokud ANO, nemůže být i zpracovatelem) Ano / Ne	7. **Organizace je v pozici zpracovatele:** (Pokud ANO nebůže být i správcem, vzájemně se vylučuje) Ano / Ne
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 je správce:** (Pro koho jsou údaje zpracovávány - název organizace)
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 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
  - 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

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

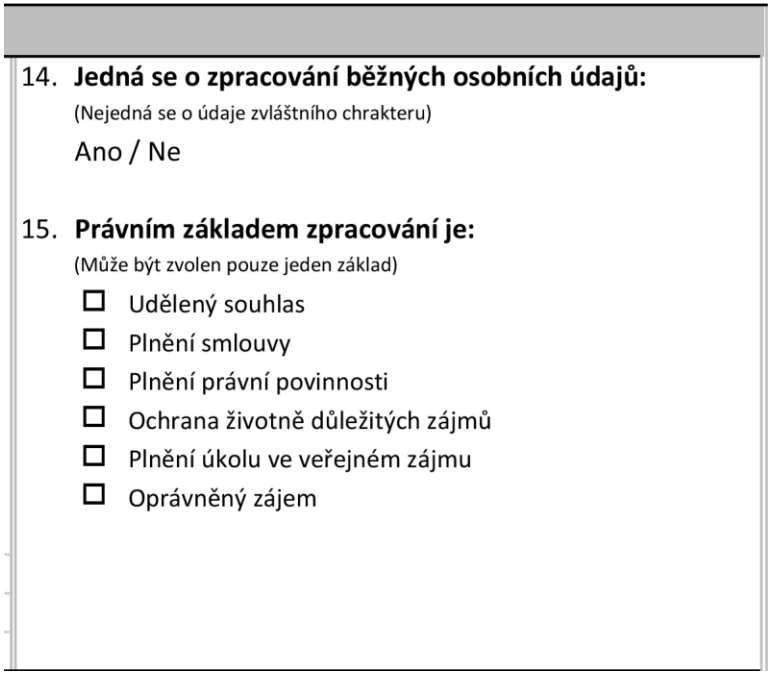
První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Právní základ pro zpracování os. údajů

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

Změny v ochraně osobních údajů

- 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
- …



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

15. **Právním základem zpracování je:**
(Může být zvolen pouze jeden základ)
- ☐ Udělený souhlas
- ☐ Plnění smlouvy
- ☐ Plnění právní povinnosti
- ☐ Ochrana životně důležitých zájmů
- ☐ Plnění úkolu ve veřejném zájmu
- ☐ Oprávněný zájem

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

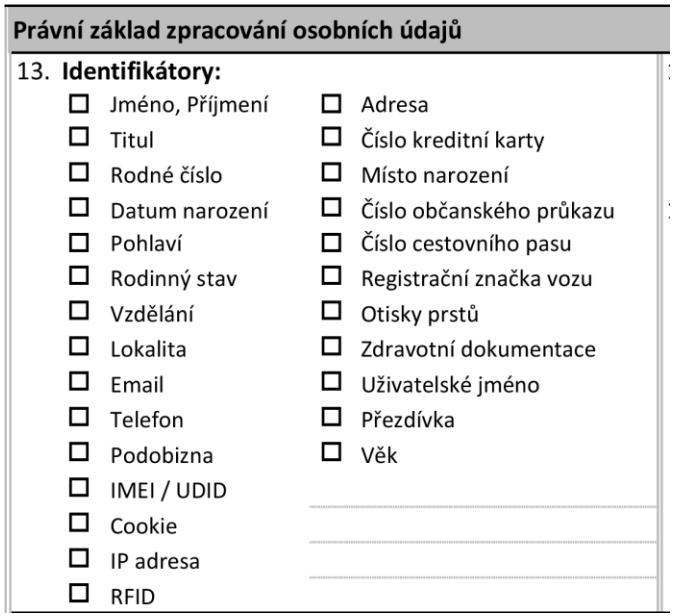
Problémy oprávněného zájmu

- 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**

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



Právní základ zpracování osobních údajů

13. **Identifikátory:**

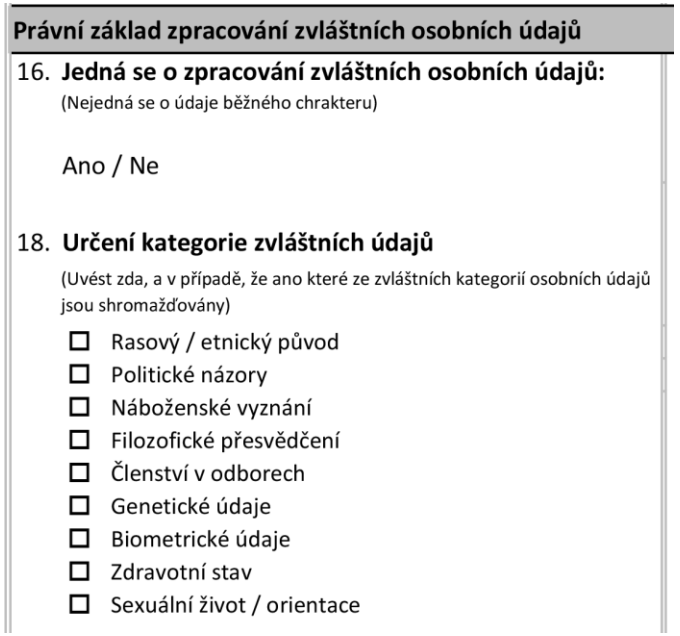
☐ Jméno, Příjmení	☐ Adresa
☐ Titul	☐ Číslo kreditní karty
☐ Rodné číslo	☐ Místo narození
☐ Datum narození	☐ Číslo občanského průkazu
☐ Pohlaví	☐ Číslo cestovního pasu
☐ Rodinný stav	☐ Registrační značka vozu
☐ Vzdělání	☐ Otisky prstů
☐ Lokalita	☐ Zdravotní dokumentace
☐ Email	☐ Uživatelské jméno
☐ Telefon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

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

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:	

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	

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

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

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

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

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

Řízení incidentů:		**Incident je řízen**	**Incident by měl být řízen**
21.	/Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/	Ano / Ne	Ano / Ne
Uvést, zda je v rámci zpracování prováděno:			
22. Profilování	Ano / Ne	23. Odvozování	Ano / Ne

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	25. Generalizace	Ano / Ne
26. Obnova dostupnosti		27. Pravidelné testy	
28. Anonymizace	Ano / Ne	29. Šifrování	Ano / Ne

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	

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.

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)

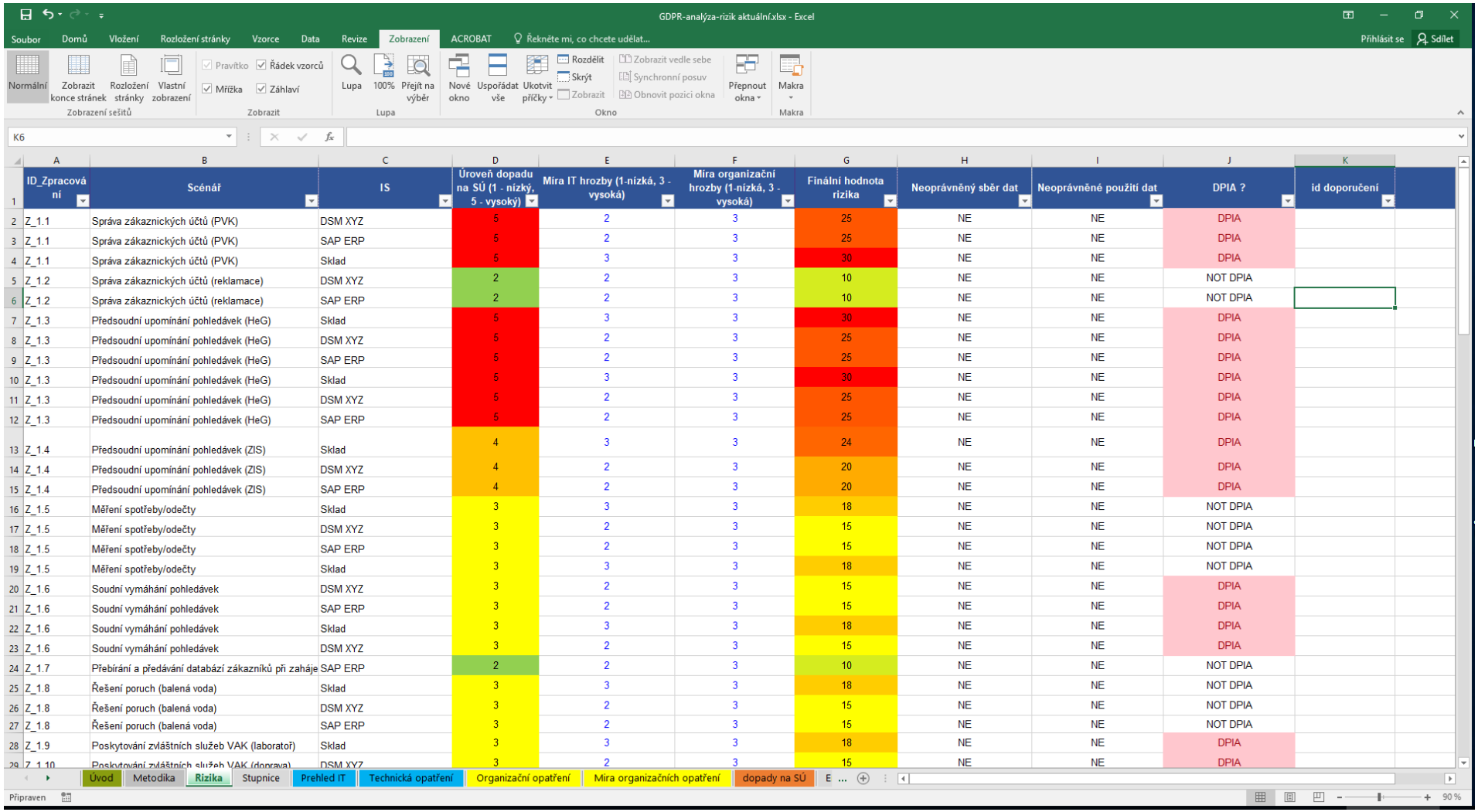
Interní odpovědnost za zpracování:	
/Uvést interní odpovědnost za toto zpracování – pozice/ 36.	/Uvést email na odpovědnou osobu/ 37.
Organizační útvar (y), které se seznamují s osobními údaji:	
38.	

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

Analýza Rizik



ID_Zpracování	Scénář	IS	Úroveň dopadu na SÚ (1 - nízký, 5 - vysoký)	Míra IT hrozby (1-nízká, 3 - vysoká)	Míra organizační hrozby (1-nízká, 3 - vysoká)	Finální hodnota rizika	Neoprávněný sběr dat	Neoprávněné použití dat	DPIA ?	id doporučení
Z_1.1	Správa zákaznických účtů (PVK)	DSM XYZ	5	2	3	25	NE	NE	DPIA	
Z_1.1	Správa zákaznických účtů (PVK)	SAP ERP	5	2	3	25	NE	NE	DPIA	
Z_1.1	Správa zákaznických účtů (PVK)	Sklad	5	3	3	30	NE	NE	DPIA	
Z_1.2	Správa zákaznických účtů (reklamace)	DSM XYZ	2	2	3	10	NE	NE	NOT DPIA	
Z_1.2	Správa zákaznických účtů (reklamace)	SAP ERP	2	2	3	10	NE	NE	NOT DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	Sklad	5	3	3	30	NE	NE	DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	DSM XYZ	5	2	3	25	NE	NE	DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	SAP ERP	5	2	3	25	NE	NE	DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	Sklad	5	3	3	30	NE	NE	DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	DSM XYZ	5	2	3	25	NE	NE	DPIA	
Z_1.3	Předsoudní upomínání pohledávek (HeG)	SAP ERP	5	2	3	25	NE	NE	DPIA	
Z_1.4	Předsoudní upomínání pohledávek (ZIS)	Sklad	4	3	3	24	NE	NE	DPIA	
Z_1.4	Předsoudní upomínání pohledávek (ZIS)	DSM XYZ	4	2	3	20	NE	NE	DPIA	
Z_1.4	Předsoudní upomínání pohledávek (ZIS)	SAP ERP	4	2	3	20	NE	NE	DPIA	
Z_1.5	Měření spotřeby/odečty	Sklad	3	3	3	18	NE	NE	NOT DPIA	
Z_1.5	Měření spotřeby/odečty	DSM XYZ	3	2	3	15	NE	NE	NOT DPIA	
Z_1.5	Měření spotřeby/odečty	SAP ERP	3	2	3	15	NE	NE	NOT DPIA	
Z_1.5	Měření spotřeby/odečty	Sklad	3	3	3	18	NE	NE	NOT DPIA	
Z_1.6	Soudní vymáhání pohledávek	DSM XYZ	3	2	3	15	NE	NE	DPIA	
Z_1.6	Soudní vymáhání pohledávek	SAP ERP	3	2	3	15	NE	NE	DPIA	
Z_1.6	Soudní vymáhání pohledávek	Sklad	3	3	3	18	NE	NE	DPIA	
Z_1.6	Soudní vymáhání pohledávek	DSM XYZ	3	2	3	15	NE	NE	DPIA	
Z_1.7	Přebírání a předávání databází zákazníků při zaháje	SAP ERP	2	2	3	10	NE	NE	NOT DPIA	
Z_1.8	Řešení poruch (balená voda)	Sklad	3	3	3	18	NE	NE	NOT DPIA	
Z_1.8	Řešení poruch (balená voda)	DSM XYZ	3	2	3	15	NE	NE	NOT DPIA	
Z_1.8	Řešení poruch (balená voda)	SAP ERP	3	2	3	15	NE	NE	NOT DPIA	
Z_1.9	Poskytování zvláštních služeb VAK (laboratoř)	Sklad	3	3	3	18	NE	NE	DPIA	
Z_1.10	Poskytování zvláštních služeb VAK (doprava)	DSM XYZ	3	2	3	15	NE	NE	DPIA	

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

Dokumentace k prokázání souladu s GDPR

Č.	Kód dokumentu	Název dokumentu	Odpovídající článek v GDPR	Mandatorní povinnost dle GDPR
	1	**Příprava projektu a analýza**		
1	1.1	Dotazníky z provedených šetření		
2	1.2	GAP analýza souladu s GDPR		
	2	**Rámec politiky osobních údajů**		
3	2.1	Zásady ochrany osobních údajů	Článek 24(2)	✓
4	2.2	Zásady ochrany osobních údajů zaměstnanců - směrnice	Článek 24(2)	
5	2.3	Ochrana osobních údajů - web	Články 12, 13 and 14	✓
6	2.4	Registrace oznámení o ochraně osobních údajů	GDPR Články 12, 13 and 14	
7	2.5	Zásady uchování dat	Články 5(1)(e), 13(1), 17, 30	✓
8	2.6	Příloha - Plán uchovávání dat	Článek 30	✓
9	2.7	Popis pracovního místa pověřence pro ochranu osobních údajů	Články 37, 38, 39	✓*
	3	**Mapování zpracovatelských činností**		
10	3.1	Pokyny pro mapování datových a zpracovatelských činností	Článek 30	
11	3.2	Příloha – Katalog (registr) zpracování	Článek 30	✓
	4	**Správa práv subjektu údajů**		
12	4.1	Formulář souhlasu se zpracováním údajů subjektu	Články 6(1)(a), 7(1), 9(2)	✓
13	4.2	Formulář pro odejmutí souhlasu se zpracováním údajů subjektu	Článek 7(3)	
14	4.3	Formulář rodičovského souhlasu	Článek 8	✓
15	4.4	Formulář pro odejmutí rodičovského souhlasu	Článek 8	✓
16	4.5	Postup žádosti o přístup k údajům subjektu	Články 7(3), 15, 16, 17, 18, 20, 21, 22	
17	4.6	Formulář žádosti o přístup k údajům subjektu	GDPR Článek 15	
18	4.7	Formulář pro zveřejnění údajů subjektu	GDPR Článek 15	
	5	**Posouzení dopadů na ochranu OÚ**		
19	5.1	Metodika hodnocení dopadů na ochranu osobních údajů	Článek 35	
20	5.2	Registr posouzení	Článek 35	✓
21	5.3	Analýza rizik z hlediska subjektů údajů	Článek 33	

Č.	Kód dokumentu	Název dokumentu	Odpovídající článek v GDPR	Mandatorní povinnost dle GDPR
	6	**Přenosy osobních dat**		
22	6.1	Přeshraniční postup pro přenos osobních údajů	Články 1(3), 44, 45, 46, 47, 49	
23	6.2	Příloha 1 - Standardní smluvní doložky pro předávání osobních údajů správcům	Článek 46(5)	✓
24	6.3	Příloha 2 - Standardní smluvní doložky pro předávání osobních údajů zpracovatelům	Článek 46(5)	✓
	7	**Shoda s třetími stranami**		
25	7.1	Procesní dotazník pro shodu s GDPR	GDPR Články 28, 32	
26	7.2	Smlouva o zpracování osobních údajů – role správce	Články 28, 32, 82	✓
27	7.3	Smlouva o zpracování osobních údajů – role zpracovatele	Články 28, 32, 82	✓
	8	**Bezpečnost osobních údajů**		
28	8.1	Zásady bezpečnosti IT	Článek 32	
29	8.2	Pravidla řízení přístupu	Článek 32	
30	8.3	Bezpečnostní postupy pro oddělení IT	Článek 32	
31	8.4	Zásady BYOD (přineste si vlastní zařízení)	Článek 32	
32	8.5	Zásady užití mobilních zařízení a teleworkingu	Článek 32	
33	8.6	Zásady čistého stolu a obrazovky	Článek 32	
34	8.7	Zásady klasifikace informací	Článek 32	
35	8.8	Zásady anonymizace a pseudonymizace	Článek 32	
36	8.9	Zásady užití kryptování	Článek 32	
37	8.10	Plán obnovy po havárii	Článek 32	
38	8.11	Postup interního auditu	Článek 32	
39	8.12	Dodatek - Kontrolní seznam interního auditu ISO 27001	Článek 32	
	9	**Porušení bezpečnosti osobních údajů**		
40	9.1	Postup při odhalení porušení a oznamování	Články 4(12), 33, 34	✓
41	9.2	Registrace porušení bezpečnosti údajů	Článek 33(5)	✓
42	9.3	Oznamovací formulář při porušení bezpečnosti údajů určený úřadu dohledu	Článek 33	✓
43	9.4	Oznamovací formulář porušení bezpečnosti údajů pro subjekty údajů	Článek 34	✓

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

Děkuji za pozornost!

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz